C.R. Math. Rep. Acad. Sci. Canada

Vol. IX, No. 6 **December 1987 decembre**

CONTENTS

C.R. Math. Rep. Acad. Sci. Canada - Vol. IX, No. 6, December 1987 décembre

Memoir

The Amalgamation Property in Lattice Theory

G. Grätzer FRSC

1. Introduction. The Amalgamation Property migrated to lattice theory from group theory *via* universal algebra. In this paper, I will try to introduce the general reader to the basic ideas related to the Amalgamation Property in lattices. I will not attempt to survey all the lattice theoretic results.

This paper is based on the invited address I gave on August 2, 1986 at the Universal Algebra and Lattice Theory Conference at the National Institute of Health in Bethesda, Maryland. Only the results with E. Fried concerning pasting are of more recent origin.

Special thanks are due to J. Berman, E. Fried, R. Padmanabhan, and G. H. Wenzel for their critical comments on the draft of this paper.

The research for this paper was supported by the NSERC of Canada.

2. Basic concepts. I shall assume that the reader is familiar with the basic concepts of lattice theory: lattices, diagrams, identities (equations), varieties (equational classes), see G. Grätzer [1] and [3].

In particular, we need two lattices: The lattice of Figure 1 will be denoted by N_5. It is closely related to the *modular identity*. A lattice L is called *modular* iff for all $x, y, z \in L$, $z \leq x$ implies that $x \wedge (y \vee z) = (x \wedge y) \vee z$. A lattice is modular iff it does not contain N_5 as a sublattice. The class of all modular lattices will be denoted by **M**.

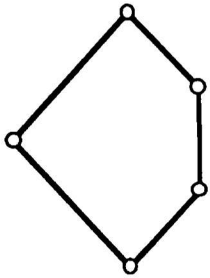


Figure 1

The lattice of Figure 2 will be denoted by M_3. It is closely related to the *distributive identity*. A lattice L is *distributive* iff for all $x, y, z \in L$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. The class of all distributive lattices will be denoted by **D**. M_3 is the smallest modular nondistributive lattice. A modular lattice L belongs to **D** iff it does not contain M_3 as a sublattice.

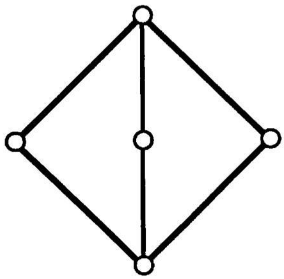


Figure 2

3. Definition. There are two ways to define the Amalgamation Property: informally with "potatoes" and formally with a categorical diagram.

Informal definition:

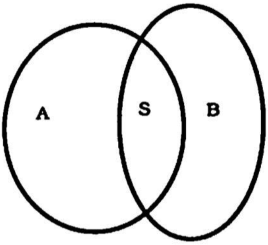


Figure 3

Let A and B be lattices, and let S be a common sublattice of A and B as shown on Figure 3 ($A \cap B = S$ can be assumed without loss of generality). The lattice L *amalgamates* A *and* B *over* S iff L contains sublattices A', B', and S' such that A is isomorphic to A', B to B', S to S', and S' holds the same position in A' (resp., B') as S in A (resp. B).

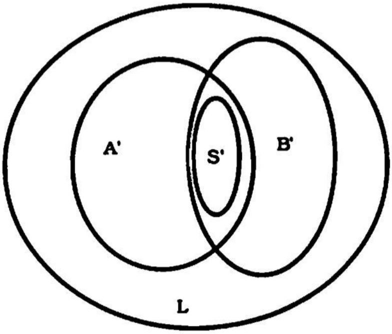


Figure 4 shows the lattice L as it amalgamates A and B over S; note that, in general, the intersection of A' and B' may be larger than S'. If there is no danger of confusion, A', B', S' will also be denoted by A, B, S.

Figure 4

The categorical definition follows:

$$\begin{tikzcd} S \arrow[r] \arrow[d] & A \\ B & \end{tikzcd}$$

Figure 5

We are given two embeddings of the lattice S into the lattices A and B, as in Figure 5.

$$\begin{tikzcd} S \arrow[r] \arrow[d] & A \arrow[d] \\ B \arrow[r] & L \end{tikzcd}$$

Figure 6

The lattice L amalgamates A and B over S iff there are embeddings of A and B into L such that the diagram of Figure 6 is commutative.

We say that a class **K** of lattices has the *Amalgamation Property* iff every pair of lattices can be amalgamated over a common sublattice. The class **L** of all lattices and the variety **D** have the Amalgamation Property, but as we shall see below, **M** does not.

The *Strong Amalgamation Property* requires that, in L, the sublattices A and B intersect in S. **L** has the Strong Amalgamation Property. **D** does not. Indeed, consider the lattice of Figure 7. Let this lattice be both A and B, and let S be the three element sublattice consisting of the elements marked by solid circles.

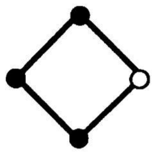


Figure 7

M_3 shows that there is a strong amalgamation of A and B over S in **L**. It is easily seen that there is none in **D**: the middle filled element must have more than one relative complement in any strong amalgamation, and this is impossible in a distributive lattice.

4. Gluing and pasting. If L amalgamates A and B over S, so does every lattice that contains L.

However, in general, there may be many lattices amalgamating A and B over S, none containing any of the other ones as sublattices. Consider the trivial example of Figure 8. Let A and B be the lattice of Figure 8. S is the two-element lattice of black-filled elements. There are four ways to amalgamate A and B over S, as shown in Figure 9.

Figure 8

Note that no lattice of Figure 9 can be embedded into another lattice of Figure 9 over S (a black-filled element has to be mapped into a black-filled element).

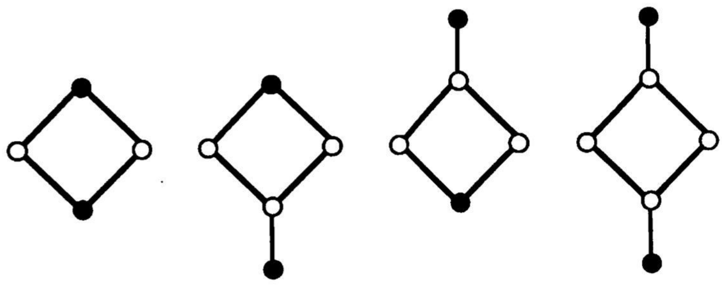


Figure 9

Using some well-known results (see Section VI.2 of G. Grätzer [3]), it is easy to show that there are finite lattices A and B, and a common sublattice S, such that there are countably infinite amalgamations of A and B over S, and no amalgamation can be embedded into another amalgamation preserving S.

Figure 10 illustrates *gluing*, one of the oldest forms of amalgamation (due to R. P. Dilworth): S is a *dual ideal* of A (if x, y $\in$ S, then $x \wedge y \in S$ and if $x \in S$, $y \in A$, and $x \leq y$, then $y \in S$) and S is an *ideal* of B (if x, y $\in$ S, then $x \vee y \in S$ and if $x \in S$, $y \in B$, and $y \leq x$, then $y \in S$); then $L = A \cup B$ amalgamates A and B over S. The partial order in L is the natural one: $\leq$ retains its meaning in A and B; for $a \in A$ and $b \in B$, $a \leq b$ iff $a \leq s$ in A and $s \leq b$ in B for some $s \in S$.

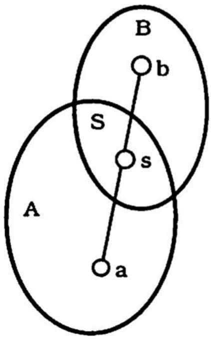


Figure 10

If L glues A and B over S, then L amalgamates A and B over S; in fact, if any other lattice K amalgamates A and B over S, then L is (isomorphic to) a sublattice of K. This is the "most uniqueness" one can get out of the Amalgamation Property.

There are other instances where we get this type of uniqueness. Let A and B be given as in Figure 11; in both lattices S is the two-element chain of solid elements. There is only one minimal way to amalgamate A and B over S, as shown in Figure 12.

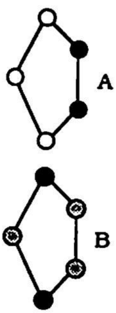


Figure 11

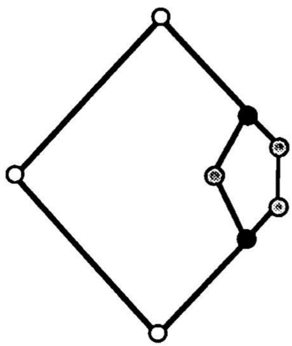


Figure 12

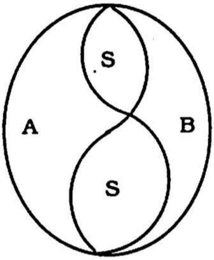


Figure 13

Again, any amalgamation contains the unique lattice we obtain from $L = A \cup B$. This last example illustrates another special type of amalgamation which we shall call *pasting*: Let L be a lattice. Let A, B, and S be sublattices of L, $A \cap B = S$, $A \cup B = L$, see Figure 13. Then L *pastes* A and B together over S, if every amalgamation of A and B over S contains L as a sublattice. This concept was investigated in A. Slavík [1]; see also G. Grätzer [3], Exercise 12 of Section V.4. (A. Slavík used the term "A-decomposable".)

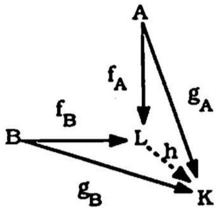


Figure 14

In a more categorical version: Let L be a lattice. Let A, B, S be sublattices of L, $A \cap B = S$, $A \cup B = L$. Let f_A and f_B be the embeddings of A and B, respectively, into L. Then L *pastes* A and B together over S if whenever g_A and g_B are embeddings of A and B into a lattice K satisfying $xg_A = xg_B$ for all $x \in S$, then there is an embedding) h of L into K satisfying $f_Ah = g_A$ and $f_Bh = g_B$, see Figure 14.

5. Varieties with the Amalgamation Property. When the Amalgamation Property was first introduced, three lattice varieties were known to have it: **T** (the trivial variety of one element lattices), **D** (the variety of all distributive lattices), and **L** (the variety of all lattices).

It is worth recalling why the Amalgamation Property holds for **L**. Let A and B be given with the common sublattice S as in Figure 3, $A \cap B = S$. By B. Jónsson [1], we can define on $P = A \cup B$ a partial ordering relation $\leq$ as follows:

(i) For $x, y \in A$ (and for $x, y \in B$), $x \leq y$ in P iff $x \leq y$ in A (resp., $x \leq y$ in B).

(ii) For $x \in A$ and $y \in B$, $x \leq y$ in P iff there exists an $s \in S$ with $x \leq s$ in A and $s \leq y$ in B; and dually, for $y \leq x$.

The MacNeille completion P^c of P (the lattice of all subsets X of P with the property that X contains all the elements that are lower bounds of the set of all upper bounds of X) is a lattice containing P as a subposet ($p \in P$ is identified with $\{x \mid x \in P \text{ and } x \leq p\}$) and all joins and meets that exist in P are preserved in P^c (see, e.g., G. Grätzer [3]). Thus P^c amalgamates A and B over S.

Since the early fifties, many attempts have been made to find lattice varieties having the Amalgamation Property, or to prove that there are none other than **T**, **D**, and **L**. In particular, there was great interest whether **M** (the variety of all modular lattices) has the Amalgamation Property. Lists of unsolved problems invariably included one or more problems relating to the Amalgamation Property (see, e.g., B. Jónsson [3] and G. Grätzer [3]).

The problem was finally resolved by the following

Theorem. <u>The only lattice varieties having the Amalgamation Property are **T**, **D**, and **L**.</u>

The solution came in two steps, in 1972 and 1983.

In 1972, G. Grätzer, B. Jónsson, and H. Lakser made the following simple observation: let **V** be a variety of modular lattices having the Amalgamation Property, $\mathbf{V} \supset \mathbf{D}$. Then any lattice, L, in **V** can be embedded into a projective geometry (that is, into the lattice of all subspaces of a projective space).

Indeed, to start with, we can assume that L has a zero and a unit. Now recall from Section 2 that M_3 must be in **V**. The crucial step is the following: We embed L into a lattice L' in **V** such that every $a \in L'$ is contained in a sublattice of L' isomorphic to M_3.

To accomplish this, take any $a \in L$ that is not contained in a sublattice isomorphic to M_3. Amalgamate M_3 with L over the three-element chain in **V** as shown in Figure 15 (this figure shows the A, B, and S of the amalgamation, not the resulting lattice of **V**. Proceed like this with all the elements of L; by forming a direct limit we obtain a lattice L_1 in **V** in which every element of L is contained in a sublattice isomorphic to M_3. Repeating this process ω times, and again forming a direct limit, we obtain the lattice L'.

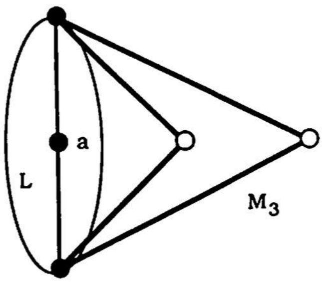


Figure 15

This L' is a simple complemented modular lattice, so by a result of O. Frink [1], L' can be embedded in a projective geometry. It now immediately follows that **M** does not have the Amalgamation Property: indeed, in this projective geometry, the lattice theoretic version of Desargues' Theorem, the *arguesian identity*, holds, while there are modular lattices L in which it does not.

It takes some more work to get our full result: **T** and **D** are the only varieties of modular lattices having the Amalgamation Property. For the complete proof, the reader is referred to our paper.

It took another dozen years or so for A. Day and J. Ježek to resolve the nonmodular case. They built on earlier attempts of J. Ježek and A. Slavík [1] and of A. Slavík [1] who proved that any nonmodular lattice variety having the Amalgamation Property has to contain a large class of lattices (the "primitive lattices"). They used the concept of pasting which proved to be crucial.

Their argument uses an earlier result of A. Day [1]. Let L be a lattice, and let $I = [a, b]$ be an interval of L. We split the interval I in the lattice L to obtain L[I]. The lattice L[I] consists of $L - I$ and $I \times C_2$ (C_2 is the two-element chain with elements 0 and 1) with the natural partial ordering.

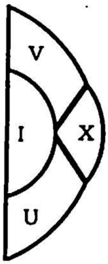


Figure 16

To visualize it, think of L split into four parts as in Figure 16: U is the set of elements in $L - I$ with an upper bound in I; V is the set of elements in $L - I$ with a lower bound in I; X is $L - (I \cup U \cup V)$. Then $L[I]$ is as depicted in Figure 17. I_0 is $\{\langle i, 0\rangle \mid i \in I\}$ and I_1 is $\{\langle i, 1\rangle \mid i \in I\}$. In $L[I]$, $x \leq \langle i, 0\rangle$ iff $x \leq i$ in L; $\langle i, 1\rangle \leq y$ iff $i \leq y$ in L.

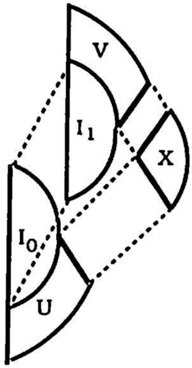


Figure 17

Now Day's result is the following: if we start with the free distributive lattice $F_D(3)$ on 3 generators and we keep splitting intervals so that every interval eventually gets split, the inverse limit of this sequence of lattices contains the free lattice $F_L(3)$ on 3 generators as a sublattice. So if **V** is a variety closed under the splitting of an interval, then **V** is generated by $F_L(3)$, and so **V** = **L**.

If Θ is a congruence relation of L under which I is a single congruence class, then obviously $L[I]$ is a subdirect product of L and $(L/\Theta)[I/\Theta]$, where I/Θ is a singleton. Thus if L is a lattice in a nonmodular lattice variety **V** and L/Θ is $C_2 \times C_2$, then $(L/\Theta)[I/\Theta]$ is N_5, so $L[I]$ is in **V**.

For the remainder of the argument: For a nonmodular lattice variety **V** having the Amalgamation Property, an ingenious induction on the number of elements in L concludes that $L[I]$ is in **V** without having to assume that I is a congruence class. The reader is referred to the paper of Day and Ježek for the details.

6. The Amalgamation Class. In G. Grätzer and H. Lakser [1], we investigate which varieties of pseudocomplemented distributive lattices have the Amalgamation Property. The result is rather disappointing: only the three smallest varieties and the largest one have the

Amalgamation Property. It seems more appropriate to investigate *to what extent* a variety has the Amalgamation Property. We do this by introducing the concept of the amalgamation class:

For a variety **V**, the *amalgamation class of* **V**, Amal(**V**), is the class of all those members S of **V** for which for any A, B $\in$ **V**, if S, A, B are as in Figure 3, then there is an amalgamation L of A and B over S in **V**, as in Figure 4.

Obviously, **V** has the Amalgamation Property iff Amal(**V**) = **V**. In G. Grätzer and H. Lakser [1], we have given a pretty effective description of the finite members of Amal(**V**) for any proper variety **V** of pseudocomplemented distributive lattices.

For lattice varieties, we have been much less successful in saying anything about Amal(**V**). In G. Grätzer, B. Jónsson, and H. Lakser [1], we have proved that the two-element chain, C_2, is not in Amal(**M**). The proof is very geometric: were $C_2 \in$ Amal(**M**), it would follow that every modular lattice L is a sublattice of a modular lattice L' in which L lies in an edge of an M_3 as shown in Figure 18. But then we would have the extra "two dimensions" to imitate the proof of Desargues' Theorem in L' in its lattice theoretic form (the arguesian identity), a contradiction.

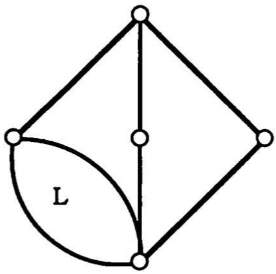


Figure 18

Obviously, the one-element lattice is in Amal(**V**) for any lattice variety **V**. We have been unable to find any other member of Amal(**M**). So it was a great surprise to us when M. Yasuhara [1] proved that for any variety **V**, Amal(**V**) is cofinal with **V** (that is, every lattice in **V** can be embedded into a lattice in Amal(**V**)). Unfortunately, the proof does not reveal how to find a member of Amal(**M**); we still have not seen any nontrivial member of Amal(**M**).

In general, not much is known about Amal(**V**). In G. Grätzer [2], I point out that if $C_2 \in$ Amal(**V**), then **V** is a join-irreducible element of the lattice of lattice varieties. J. Berman [1] constructs a nonmodular variety **V** with $C_2 \in$ Amal(**V**); **V** is generated by a sequence of lattices patterned after Figure 12. B. Jónsson [4] describes all finite members of Amal(**V**) for finitely generated lattice varieties; in particular, he obtains a nice description of all the finite members of Amal($\mathbf{N_5}$), where $\mathbf{N_5}$ is the variety generated by N_5.

7. Pasting. The concept of pasting (see Sections 4 and 5) has been investigated in A. Slavík [1], A. Day and J. Ježek [1], and in two papers by E. Fried and G. Grätzer ([3] and [4]). Here is the main characterization theorem of pasting (E. Fried and G. Grätzer [4]):

Theorem. Let L be a lattice. Let A, B, and S be sublattices of L, $A \cap B = S$, $A \cup B = L$. Then L pastes A and B together over S iff the following two conditions hold:

(i) For $a \in A$ and $b \in B$, if $a \leq b$, then there exists an $s \in S$ with $a \leq s$ in A and $s \leq b$ in B, and dually for $b \leq a$.

(ii) If X and Y are ideals of L satisfying $X - Y \subseteq A - B$ and $Y - X \subseteq B - A$, then $X \subseteq Y$ or $Y \subseteq X$; and dually, for dual ideals.

In the finite case, (ii) can be replaced by the condition (A. Day and J. Ježek [1]):

(ii') For $s \in S$, all the covers of s in L are in A or all are in B; and dually.

Check (i) and (ii') in the lattices of Figures 8 and 10.

The main application of the characterization is the result (E. Fried and G. Grätzer [4]): **M** and **D** are closed under pasting.

8. Concluding comments. There are some interesting connections between the Amalgamation Property and products of varieties.

If **V** and **W** are lattice varieties, their product, $\mathbf{V} \circ \mathbf{W}$ consists of all lattices L for which there is a congruence relation Θ satisfying: (i) all Θ-classes of L are in **V**; (ii) L/Θ is in **W**. In general, $\mathbf{V} \circ \mathbf{W}$ is not a variety; however, $\mathbf{H}(\mathbf{V} \circ \mathbf{W})$ (the class of all homomorphic images of members of $\mathbf{V} \circ \mathbf{W}$) always is.

In G. Grätzer and D. Kelly [2], we prove that if $\mathbf{V}$ is closed under gluing then $\mathbf{V} \circ \mathbf{D}$ is a variety. In fact, based on a result of R. Freese [1], we present continuumly many modular lattice varieties closed under gluing.

R. N. McKenzie (in R. McKenzie and D. Hobby [1]) proves that $\mathbf{D} \circ \mathbf{W}$ and $\mathbf{M} \circ \mathbf{W}$ are always varieties. A very deep result of T. Harrison [1] proves that there are no nonmodular varieties (other than $\mathbf{L}$) for which a similar result holds: if $\mathbf{V}$ is a nonmodular lattice variety such that $\mathbf{V} \circ \mathbf{D}$ is a variety, then $\mathbf{V} = \mathbf{L}$; in fact, he proves that if $\mathbf{V} \circ \mathbf{W}$ is a variety for some nontrivial modular lattice variety $\mathbf{W}$, then $\mathbf{V} = \mathbf{L}$;.

Since Harrison's result uses only that $\mathbf{V}$ is closed under finite gluing, by the result of Grätzer and Kelly, we obtain the following sharp form of the result of Day and Ježek: If $\mathbf{V}$ is a nonmodular lattice variety closed under finite gluing, then $\mathbf{V} = \mathbf{L}$.

If $\mathbf{V} \circ \mathbf{W}$ is not a variety, then $\mathbf{H}(\mathbf{V} \circ \mathbf{W})$ is; however, the members of $\mathbf{H}(\mathbf{V} \circ \mathbf{W})$ cannot be described by congruences so neatly. R. N. McKenzie conjectured that an "amalgamated" version of congruences, the so called tolerance relations, will serve to describe $\mathbf{H}(\mathbf{V} \circ \mathbf{W})$. A *tolerance relation* T on a lattice L is defined as a reflexive and symmetric binary relation having the substitution property. A maximal T-connected subset of L is a *T-block*. The quotient lattice L/T consists of the T-blocks with the natural ordering. R. N. McKenzie conjectured that a lattice K belongs to the variety generated by $\mathbf{V} \circ \mathbf{W}$ iff there is a tolerance relation T on K satisfying (i) all T-classes of L are in $\mathbf{V}$; (ii) L/T is in $\mathbf{W}$. The following result is proved in E. Fried and G. Grätzer [1]:

Theorem. Let $\mathbf{M}_3$ be the variety generated by the modular lattice M_3, and let F be the lattice of Figure 19. Then F is in $\mathbf{H}(\mathbf{M}_3 \circ \mathbf{D})$. However, there is no tolerance relation T on F such that all T-classes of F are in $\mathbf{M}_3$ and F/T is in $\mathbf{D}$.

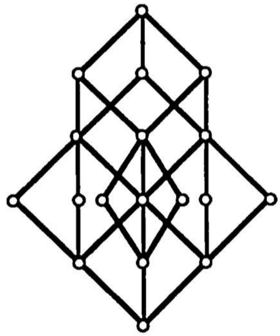


Figure 19

In E. Fried and G. Grätzer [2], we introduced a generalization of the concept of congruence relation, called *generalized congruence*. With this new concept, the analogue of McKenzie's conjecture can be proved.

Lattices form an important example of congruence distributive universal algebras; many results mentioned in this paper have analogues in the theory of congruence distributive varieties. Many valuable contributions have been made to this field by C. Bergman, B. M. Davey, B. Jónsson, and others. The interested reader may start with C. Bergman [1] as an introduction to this field.

Final note: I have just received two manuscripts containing results relevant to this survey. The first is by C. Bergman proving that Amal($\mathbf{M}_3$) is not axiomatizable. The second is by A. Day and Ch. Herrmann in which the last theorem of this section is proved for $\mathbf{N}_5 \circ \mathbf{D}$.

References

C. Bergman

[1] Amalgamation classes of some distributive varieties. *Algebra Universalis* **20** (1985), 143 - 146.

J. Berman

[1] Interval lattices and the amalgamation property. *Algebra Universalis* **12** (1981), 360 - 375.

A. Day

[1] Characterization of finite lattices that are bounded homomorphic images of sublattices of free lattices. *Canadian J. Math.* **31** (1979), 69 - 78.

A. Day and J. Ježek

[1] The amalgamation property for varieties of lattices. Mathematics Report #1 - 83, Lakehead University.

R. Freese

[1] Projective geometries as projective modular lattices. *Trans. Amer. Math. Soc.* **251** (1979), 329 - 342.

E. Fried and G. Grätzer

[1] Notes on Tolerance Relations of Lattices: A Conjecture of R. N. McKenzie. Manuscript submitted to *Festschrift. Journal of Pure and Applied Algebra.*.

[2] Generalized Congruences and Products of Lattice Varieties. Manuscript submitted to *Acta Sci. Math. (Szeged)*.

[3] Pasting and modular lattices. Abstract: *Notices Amer. Math. Soc.* 87T-06-209. Manuscript.

[4] Pasting infinite lattices. Abstract. *Notices Amer. Math. Soc.* 87T-06-193. Manuscript submitted to *Journal of Autralian Math. Soc.*

E. Fried, G. Grätzer, and H. Lakser

[1] Projective geometries as cover preserving sublattices. Manuscript submitted to *Algebra Universalis.*

O. Frink

[1] Complemented modular lattices and projective spaces of infinite dimension. *Trans. Amer. Math. Soc.* **60** (1946), 452 - 467.

G. Grätzer

[1] *Lattice Theory: First Concepts and Distributive Lattices.* W. H. Freeman and Company, San Francisco, Calif., 1971.

[2] On the Amalgamation Property. *Notices Amer. Math. Soc.* **23** (1976), A-268.

[3] *General Lattice Theory.* Pure and Applied Mathematics series, Academic Press, New York, N.Y., 1978; Birkhäuser Verlag, Matematische Reihe, Band 52, Basel, 1978.

G. Grätzer, B. Jónsson, and H. Lakser

[1] The amalgamation property in equational classes of modular lattices. *Pacific J. Math.* **45** (1973), 507 - 524.

G. Grätzer and D. Kelly

[1] A survey of products of lattice varieties. *Colloquia Mathematica Societatis János Bolyai* **33**. Universal Algebra, Esztergom (Hungary), 1980, 457 - 472.

[2] The lattice variety $\mathbf{D} \circ \mathbf{D}$. *Acta Sci. Math. (Szeged)*, **51** (1987).

[3] Products of lattice varieties. *Algebra Universalis* **21** (1985), 33 - 45.

G. Grätzer and H. Lakser

[1] The structure of pseudocomplemented distributive lattices. II. Congruence extension and amalgamation. *Trans. Amer. Math. Soc.* **156** (1971), 343 - 358.

G. Grätzer and G. H. Wenzel

[1] Notes on Tolerance Relations of Lattices: Some Basic Observations. Manuscript submitted to *Acta Sci. Math. (Szeged).*

T. A. Harrison

[1] **P** a nontrivial modular lattice variety and **V** a nonmodular lattice variety such that **V** ∘ **P** is a variety implies **V** is the variety of all lattices. Ph.D. Thesis, University of Hawaii, 1985.

J. Ježek and A. Slavík

[1] Primitive lattices. *Czech. Math. Journal* **29 (104)** (1979), 595 - 634.

B. Jónsson

[1] Universal relational systems. *Math. Scand.* **4** (1956), 193 - 208.

[2] Extensions of relational structures. *Theory of Models (Proceedings 1963 Internat. Sympos. Berkeley)*, 146 - 157. North Holland, Amsterdam, 1965.

[3] Varieties of lattices: Some open problems. *Colloquia Mathematica Societatis János Bólyai.* **29**. Universal Algebra, Esztergom (Hungary), 1977, 421 - 436.

[4] Amalgamation in small varieties of lattices. *Festschrift. Journal of Pure and Applied Algebra*, to appear.

R. McKenzie and D. Hobby

[1] The structure of finite algebras (tame congruence theory). Manuscript, 1985.

A. Slavík

[1] A note on the amalgamation property in lattice varieties. *Comm. Math. Univ. Carolinae* **21** (1980), 473 - 478.

M. Yasuhara

[1] The Amalgamation Property, the Universal-Homogeneous Models, and the Generic Models. *Math. Scand.* **34** (1974), 5 - 36.

Received Sept. 15, 1987

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba
R3T 2N2

THE SOLUTIONS TO SOME DIOPHANTINE EQUATIONS USING A RECURRENCE EQUATION

Vinko Mandekić-Botteri
Presented by J. Arthur, F.R.S.C.

ABSTRACT. This article shows that the unique sequence $\{a_n\}$ satisfying the inhomogeneous second-order linear recurrence

$$a_n = -3a_{n-1} - a_{n-2} - 2,$$

where $a_o = 0$, $a_1 = -1$, is the alternating sequence satisfying

$$a_n = (-1)^n F_n^2,$$

where F_n denotes the nth Fibonacci number.

On the basis of this fact, all the integral solutions of the Diophantine equations

$$X(X + 1) = Y(Y + X), \quad (X,Y \in \mathbb{Z})$$
$$(x - y + 1)(x - y + 2) = (x + 1)y, \quad (x,y \in \mathbb{Z})$$

are given, as well as all the solutions to the equation

$$\binom{n}{r} = \binom{n+1}{r-1}, \quad n,r \in \mathbb{N}, \ (n \geqslant r).$$

INTRODUCTION. We shall first prove that the unique sequence $\{a_n\}$ satisfying the inhomogeneous second-order linear recurrence

$$a_n + 3a_{n-1} + a_{n-2} = -2,$$

where $a_o = 0$, $a_1 = -1$, is the alternating sequence satisfying

$$a_n = (-1)^n F_n^2.$$

Two proofs of this fact are given: the first one uses the well-known facts concerning the Fibonacci sequence, while the second proof uses the theory of difference equations.

The main subject of this article is the solving of the Diophantine equations

$$X(X + 1) = Y(Y + X), \quad (X,Y \in \mathbb{Z})$$
$$(x - y + 1)(x - y + 2) = (x + 1)y, \quad (x,y \in \mathbb{Z})$$

and the solving of the equation

$$\binom{n}{r} = \binom{n+1}{r-1}, \quad n,r \in \mathbb{N}, \ (n \geqslant r)$$

using the solution to the above recurrence equation.

The equations

$$X(X + 1) = Y(Y + X), \quad (X,Y \in \mathbb{Z})$$
$$(x - y + 1)(x - y + 2) = (x + 1)y, \quad (x,y \in \mathbb{Z})$$

are specific cases of the general equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

solved by Lagrange (see [1], page 412). However, for these specific equations, we provide simpler proofs using second-order linear recurrences.

It is shown that all integral solutions for X to the first Diophantine equation are in the form of

$$X_m = a_m = (-1)^m F_m^2 ,$$

where F_m is the mth Fibonacci number.

The solutions to all these equations are expressed in the form of the couples (X,Y), (x,y) respectively (n,r), and can be simply represented by F_m.

One more equivalent definition of Fibonacci's sequence is given.

1. RECURRENCE EQUATION

LEMMA. The unique sequence $\{a_n\}$ satisfying the inhomogeneous second-order linear recurrence

$$a_n = -3a_{n-1} - a_{n-2} - 2 , \qquad (1)$$

where $a_0 = 0$, $a_1 = -1$, is the alternating sequence satisfying

$$a_n = (-1)^n F_n^2 , \qquad (2)$$

where F_n denotes the nth Fibonacci number.

FIRST PROOF: By identity I_{13} on page 57 of Fibonacci and Lucas Numbers by Verner E. Hoggatt , Jr. (Published by Houghton Mifflin, 1969),

$$F_{n-1} \cdot F_{n+1} - F_n^2 = (-1)^n . \qquad (3)$$

By identity I_{19} on page 59 of the same book,

$$F_{n-k} \cdot F_{n+k} - F_n^2 = (-1)^{n+k+1} F_k^2 . \qquad (4)$$

Now, by (3) and (4),

$$F_{n+2}^2 - 3F_{n+1}^2 + F_n^2 + 2(-1)^n = F_{n+2}^2 - 3(F_{n+2} - F_n)^2 + F_n^2 + 2(-1)^n$$

$$= -2F_{n+2}^2 - 2F_n^2 + 6F_{n+2}F_n + 2(-1)^n$$

$$= -2F_{n+2}^2 - 2F_n^2 + 6(F_{n+1}^2 + (-1)^{n+1}) + 2(-1)^n$$

$$= -2(F_{n+2}^2 - F_{n+1}^2) + 2(F_{n+1}^2 - F_n^2) + 2F_{n+1}^2 - 4(-1)^n$$

$$= -2(F_{n+2} + F_{n+1})(F_{n+2} - F_{n+1}) + 2(F_{n+1} + F_n)(F_{n+1} - F_n)$$

$$+ 2F_{n+1}^2 - 4(-1)^n = -2F_nF_{n+3} + 2F_{n-1}F_{n+2} + 2F_{n+1}^2 - 4(-1)^n$$

$$= -2F_n(F_{n+1} + F_{n+2}) + 2F_{n-1}F_{n+2} + 2F_{n+1}^2 - 4(-1)^n$$

$$= 2F_{n+1}(F_{n+1} - F_n) + 2F_{n+2}(F_{n-1} - F_n) - 4(-1)^n$$

$$= 2F_{n+1}F_{n-1} - 2F_{n+2}F_{n-2} - 4(-1)^n$$

$$= 2(F_n^2 + (-1)^{n+1+1}F_1^2) - 2(F_n^2 + (-1)^{n+2+1}F_2^2) - 4(-1)^n = 0.$$

Hence

$$F_{n+2}^2 - 3F_{n+1}^2 + F_n^2 + 2(-1)^n = 0. \qquad (5)$$

If we put (2) in (5), we obtain (1). □

<u>SECOND PROOF</u>: We wish to show that the solution to (1) is

$$a_n = (-1)^n F_n^2 .$$

From (1), we have

$$a_{n+3} + 3a_{n+2} + a_{n+1} = -2 \qquad (6)$$

and

$$a_{n+2} + 3a_{n+1} + a_n = -2 . \qquad (7)$$

Subtracting (7) from (6), we obtain the third-order homogeneous difference equation

$$a_{n+3} + 2a_{n+2} - 2a_{n+1} - a_n = 0$$

with characteristic polynomial

$$x^3 + 2x^2 - 2x - 1 = (x - 1)(x^2 + 3x + 1)$$

and characteristic roots 1, $(-3 + \sqrt{5})/2$, and $(-3 - \sqrt{5})/2$.
Using the initial conditions

$$a_0 = 0,\ a_1 = -1,\ a_2 = 1,$$

we see that

$$a_n = (-1)^n(1/5)[((1 + \sqrt{5})/2)^n - ((1 - \sqrt{5})/2)^n]^2 = (-1)^n F_n^2. \square$$

2. FIBONACCI SEQUENCE

<u>COROLLARY 1</u>. <u>The sequence given by</u>

$$a_0 = 0,\ a_1 = 1,\ a_{n+2}^2 = 3a_{n+1}^2 - a_n^2 - 2.(-1)^n,\ a_{n+2} > 0,\ n \geqslant 0, \quad (8)$$

<u>is Fibonacci's sequence.</u>

<u>PROOF</u>: This immediately follows from (1), (2) and (5). □

3. DIOPHANTINE EQUATIONS

THEOREM. The integral solutions for X in the Diophantine equation

$$X(X+1) = Y(Y+X)\ , \tag{9}$$

are $X_m = a_m = (-1)^m F_m^2$.

PROOF: The equation (9) can be written in two equivalent forms

$$(5X+2)^2 - 5(X+2Y)^2 = 4\ , \tag{10}$$

$$Y = \frac{-X \pm \sqrt{5X^2+4X}}{2}\ . \tag{11}$$

According to Landau ([2] , Theorem 111) the solutions to the Diophantine equation (10) are given by

$$\pm\varepsilon^m = \frac{\alpha_m + \sqrt{5}\beta_m}{2} = \frac{(5X_m+2) + (X_m+2Y_m)\sqrt{5}}{2}, \alpha_m, \beta_m, m \in \mathbb{Z}, \varepsilon = \frac{3+\sqrt{5}}{2}. \tag{12}$$

From (12) it follows that

$$\alpha_m \equiv 2 \pmod 5\ , \tag{13}$$

$$X_m = \frac{\alpha_m - 2}{5}\ , \ m \in \mathbb{Z}\ . \tag{14}$$

Because of $\varepsilon = (3+\sqrt{5})/2$, $\varepsilon^{-1} = (3-\sqrt{5})/2$, it follows that $\alpha_{-m} = \alpha_m$, and further on equation (12) will be taken for $m \in \mathbb{N} \cup \{0\}$. In the same way, the solutions α_m to the equation (12) will be taken for $m \in \mathbb{N} \cup \{0\}$.

Further, if the equation (12) has the solution $\alpha_m > 0 (\alpha_m < 0)$, $\alpha_m \equiv 2 \pmod 5$, then it has the solution $\alpha_{m+1} < 0 (\alpha_{m+1} > 0)$, $\alpha_{m+1} \equiv 2 \pmod 5$, for $m \in \mathbb{N} \cup \{0\}$.

It is sufficient, for this purpose, to observe ε^{m+1} and $-\varepsilon^{m+1}$:

$$\pm\varepsilon^{m+1} = \pm \frac{(3\alpha_m + 5\beta_m) + (\alpha_m + 3\beta_m)\sqrt{5}}{4} = \pm \frac{\alpha_{m+1} + \sqrt{5}\beta_{m+1}}{2}\ , \tag{15}$$

from which it follows that

$$\alpha_{m+1} = \pm \frac{3\alpha_m + 5\beta_m}{2}\ , \ \beta_{m+1} = \pm \frac{\alpha_m + 3\beta_m}{2}\ . \tag{16}$$

According to (13) we have

$$\alpha_{m+1} \equiv \pm 3 \pmod 5. \tag{17}$$

If $\alpha_m \equiv 2 \pmod 5$, then it will also be that $\alpha_{m+1} \equiv 2 \pmod 5$, iff it be

$$\operatorname{sgn}\alpha_{m+1} = -\operatorname{sgn}\alpha_m\ , \tag{18}$$

which follows from (15), (16) and (17). Hence, in (16) only the sign - can exist, and (16) becomes

$$\alpha_{m+1} = -\frac{3\alpha_m + 5\beta_m}{2}, \beta_{m+1} = -\frac{\alpha_m + 3\beta_m}{2}. \qquad (16')$$

As m = 0 and m = 1 satisfy us, according to (12) and (13), the values $\alpha_0 = 2$, $\alpha_1 = -3$, it follows from (14) that

$$X_0 = 0,\ X_1 = -1. \qquad (19)$$

According to (18) and $\alpha_1 = -3$ it will be: $\alpha_2 > 0, \alpha_3 < 0, \alpha_4 > 0, \ldots$, i.e.

$$\operatorname{sgn} \alpha_m = (-1)^m, \text{ for } m \in \mathbb{N} \cup \{0\}. \qquad (20)$$

According to (14), (for m, m+1 and m+2) and (16') (for m+1 and m+2) we obtain

$$X_{m+2} = -(3X_{m+1} + X_m + 2),\ m \geq 0. \qquad (21)$$

According to the Lemma, (19) and (21) it follows that the integral solutions for X to the Diophantine equation (9) are

$$X_m = a_m = (-1)^m F_m^2 \ . \square$$

All integer solutions to the Diophantine equation (9) are

$$\left.\begin{aligned} &(X_0,Y_0) = (0,0), \quad \text{for } m = 0, \\ &(X_m, Y_m^{(1,2)}) = ((-1)^m F_m^2, \frac{F_m((-1)^{m+1}F_m \pm \sqrt{5F_m^2 + 4(-1)^m})}{2}), \text{for } m \in \mathbb{N}, \end{aligned}\right\} \quad (22)$$

where F_m is the mth Fibonacci number.

REMARK. The fact that $X_m = (-1)^m a^2$, $a \in \mathbb{N} \cup \{0\}$ can be proved without reference to the Lemma. From (14) and (20) it follows

$$\operatorname{sgn} X_m = (-1)^m, \text{ for } m \in \mathbb{N}.$$

Let n be an integer, p be a prime, and let v(n) denote the number of times p divides n. We wish to show that if p is a prime,

$$X(X + 1) = Y(Y + X),$$

and $p | X$, then $v(X) = 2k$ for some integer $k \geq 1$. Then, it indeed follows that $|X|$ is a square. Suppose by way of contradiction that $v(X) = 2r + 1$, where $r \geq 0$. Then, clearly, $v(X + 1) = 0$, and by the theory valuations,

$$v(X(X + 1)) = v(X) + v(X + 1) = v(X) + 0 = 2r + 1.$$

We claim that for the right-hand side of equation (9), $v(Y(Y + X)) \neq 2r + 1$, which would be a contradiction. Suppose $v(Y) < v(X)$. Then $v(Y + X) = v(Y)$ and

$$v(Y(Y + X)) = v(Y) + v(Y + X) = v(Y) + v(Y) = 2v(Y) \neq 2r+1.$$

Now suppose $v(Y) \geq v(X) = 2r + 1$. Then $v(Y + X) \geq v(X)$ and

$$v(Y(Y + X)) = v(Y) + v(Y + X) \geq 2v(X) > 2r + 1.$$

Thus, we cannot have that $v(X) = 2r + 1$ and thus, $v(X) = 2k$. $\square$

<u>COROLLARY 2</u>. <u>All the integer solutions to the Diophantine equation</u>

$$(x - y + 1)(x - y + 2) = (x + 1)y, (x,y \in \mathbb{Z}) \qquad (23)$$

<u>are</u>

$$\left(\frac{F_m(\pm\sqrt{5F_m^2 + 4(-1)^m} + (-1)^m F_m)}{2} - 1, \frac{F_m(\pm\sqrt{5F_m^2 + 4(-1)^m} - (-1)^m F_m)}{2}\right),$$

$$m \in \mathbb{N} \cup \{0\}. \qquad (24)$$

PROOF: If we put $X = x-y+1$, $Y = y$, then the Diophantine equation (9) becomes the Diophantine equation (23) and the corresponding solutions (22) become (24).□

The solutions (22) and (24) to the Diophantine equations (9) and (23) are obtained in a relatively simple manner. (See [1], pages 412-417.)

4. THE EQUATION $\binom{n}{r} = \binom{n+1}{r-1}$

COROLLARY 3. All the solutions (n_k, r_k), $k \in N$, to the equation

$$\binom{n}{r} = \binom{n+1}{r-1}, \quad n,r \in N, \quad (n \geq r) \tag{25}$$

are

$$(n_k, r_k) = \left(\frac{\sqrt{5d_k^2 + 4d_k} + d_k}{2} - 1, \frac{\sqrt{5d_k^2 + d_k} - d_k}{2}\right), \text{ where}$$

$$d_k = n_k - r_k + 1 = F_{2k}^2, \ k \in N.$$

PROOF: The equation (25) for $d = n - r + 1$ becomes the equation

$$d(d+1) = r(r+d),$$

which has the form of (9), and, further, the Theorem is applied.□

These solutions can be obtained in a similar way- which has been done in the following Corollary 4. Thus the problem set in [3] i.e. "determine all solutions to the equation (25)", has been completely solved.

COROLLARY 4. All the solutions to the equation (25) are as follows

$$\left.\begin{aligned} &(n_k, r_k) = \left(\frac{a_k(b_k + a_k)}{2} - 1, \frac{a_k(b_k - a_k)}{2}\right), \\ &\text{where} \\ &b_k = \sqrt{5a_k^2 + 4}, \ a_k = \sqrt{d_k} = F_{2k}, \ d_k = n_k - r_k + 1, k \in N. \end{aligned}\right\} \tag{26}$$

PROOF: The solutions (26) to the equation (25) follow immediately from the Corollary 3.□

5. ACKNOWLEDGMENT

I wish to thank the referee for his suggestions concerning the two proofs of the Lemma and the proof using valuations in the Remark.

R E F E R E N C E S :

[1] L.E.Dickson: History of the Theory of Numbers, Vol.II, Diophantine Analysis, New York, Chelsea, 1971.

[2] Edmund Landau: Elementary number theory, New York, Chelsea Publishing Company, 1966.

[3] Dragoslav S.Mitrinović: Zbornik Matematičkih problema I, Beograd, Nolit, 1958.

Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Boškovićeva bb, 58000 Split, Yugoslavia.

Received January 7, 1987

C.R. Math. Rep. Acad. Sci. Canada - Vol. IX, No. 6, December 1987 décembre

INFORMATION CELLS: CLASSIFICATION AND REALIZATIONS

Walter Schempp

Presented by G. de B. Robinson, F.R.S.C.

Abstract. The classical sampling theorem due to E.T. Whittaker, Nyquist, Shannon, and Kotel'nikov, is concerned with the reconstruction of band-limited signals from a sequence of samples [2]. In view of the fact that voice and video are band-limited signals and the convergence of their representing cardinal series can be improved by the oversampling procedure, the sampling theorem is of paramount interest for digital signal processing and digital image processing. From the physical point of view, however, the concept of separating the time and the frequency domains of analog and digital signals which is inherent to the classical sampling theorem is completely artificial. A new approach based on the analog and digital ambiguity functions has led to a simultaneous treatment both of the time and the frequency domains via non-commutative harmonic analysis [7]. In the case of a radial digital ambiguity function, this approach leads to a Poisson-Plancherel type summation identity [6] which on its part implies a series of remarkable identities for theta-null values [7]. Its invariants are completely classified by the cyclic groups $\mathbf{Z}/p\mathbf{Z}$ satisfying the crystallographic restriction $p \in \{1,2,3,4,6\}$. The crystal symmetries result in a classification of the information (or Nyquist) cells.

1. Invariants of the Ambiguity Functions

Let ψ, φ denote wave functions belonging to the standard complex Hilbert space $L^2(\mathbf{R})$ and let $H(\psi,\varphi;.,.)$ be the associated analog cross-ambiguity function. Then we have the identity (see [6], [7])

$$H(\psi,\varphi;x,y) = \langle U_1(x,y,0)\psi|\varphi\rangle$$

for all pairs $(x,y) \in \mathbf{R} \oplus \mathbf{R}$, where U_1 denotes the linear

Schrödinger representation of the real Heisenberg nilpotent Lie group $\widetilde{A}(\mathbf{R})$ unitarily induced by the central character $z \longrightarrow e^{2\pi i z}$. Since U_1 is a square integrable representation modulo the center $\mathbf{R}$ of $\widetilde{A}(\mathbf{R})$, we have $H(\psi,\varphi;.,.) \in L^2(\mathbf{R} \oplus \mathbf{R})$. Let $H(\psi;.,.) = H(\psi,\psi;.,.)$ denote the analog auto-ambiguity function associated with the wave function $\psi \in L^2(\mathbf{R})$. A mapping

$$\sigma : \mathbf{R} \oplus \mathbf{R} \longrightarrow \mathbf{R} \oplus \mathbf{R}$$

is called an invariant of the analog auto-ambiguity H if the identity

$$H(\psi;x,y) = H(\psi_\sigma;\sigma(x,y))$$

holds for all pairs $(x,y) \in \mathbf{R} \oplus \mathbf{R}$ and all wave functions $\psi \in L^2(\mathbf{R})$ in such a way that the assignment

$$\psi \longrightarrow \psi_\sigma$$

defines a unitary operator in the Hilbert space $L^2(\mathbf{R})$. Then $H(\psi,\varphi;x,y) = H(\psi_\sigma,\varphi_\sigma;\sigma(x,y))$. By virtue of the identity $\mathbf{Sp}(1,\mathbf{R}) = \mathbf{SL}(2,\mathbf{R})$ an application of the oscillator representation [9] of the metaplectic group $\mathbf{Mp}(1,\mathbf{R})$ yields the following

Theorem 1. An arbitrary mapping σ: $\mathbf{R} \oplus \mathbf{R} \longrightarrow \mathbf{R} \oplus \mathbf{R}$ forms an invariant of the analog auto-ambiguity function H if and only if σ is $\mathbf{R}$-linear and $\det \sigma = 1$, i.e., $\sigma \in \mathbf{SL}(2,\mathbf{R})$.

2. The Poisson Plancherel Type Summation Identity

Let the wave function $\psi \in L^2(\mathbf{R})$ be normalized by $\|\psi\| = 1$. Recall that the analog auto-ambiguity function $H(\psi;.,.) \in L^2(\mathbf{R} \oplus \mathbf{R})$ is radial, i.e., $\mathbf{SO}(2,\mathbf{R})$-invariant, if and only if

$$\psi = \xi_n H_n$$

where $H_n \in L^2(\mathbf{R})$ denotes the Hermite (harmonic oscillator wave) function of degree $n \geq 0$. For holography and fiber optics [9] it is important to determine the phase factor $\xi_n \in \mathbf{T}$.

Identify the real plane $\mathbf{R} \oplus \mathbf{R}$ with the complex plane $\mathbf{C}$ in the usual way and let $L_n^{(\alpha)}$ denote the Laguerre function of degree $n \geq 0$ and order α. In the case of order $\alpha = 0$ write simply L_n. Observe that the associated analog cross-ambiguity function

$$H(H_m,H_n;x,y) = \sqrt{\frac{n!}{m!}}(\sqrt{\pi}(x+iy))^{m-n}L_n^{(m-n)}(\pi(x^2+y^2)) \quad (m \geqq n \geqq 0)$$

is a radial function on the complex plane **C** if and only if $m=n$. Cutting down the coefficient functions $\langle U_1(x,y,0)H_m|H_n\rangle$ to the compact Heisenberg nilmanifold (a principal circle bundle over the two-dimensional compact torus $\mathbf{T}^2$) yields the following Poisson-Plancherel type summation identity ([6], [7], and Borwein [1]) for digital cross-ambiguity functions

$$\sum_{(\mu_1,\mu_2)\in \mathbf{Z}\times\mathbf{Z}} L_m(\pi(\mu_1^2+\mu_2^2))L_n(\pi(\mu_1^2+\mu_2^2)) =$$

$$\frac{n!}{m!}\pi^{m-n} \sum_{(\mu_1,\mu_2)\in \mathbf{Z}\times\mathbf{Z}} (\mu_1^2+\mu_2^2)^{m-n}(L_n^{(m-n)}(\pi(\mu_1^2+\mu_2^2)))^2$$

where $m \geqq n$. It should be noticed that the terms occurring on both sides are radial functions on the quadratic lattice $\mathbf{Z}\times\mathbf{Z}$.

Theorem 2. <u>The invariants of the preceding Poisson-Plancherel type summation identity for digital cross-ambiguity functions are formed by the cyclic groups $\mathbf{Z}/p\mathbf{Z}$ where the order p satisfies the crystallographic restriction</u>

$$p \in \{1,2,3,4,6\}.$$

The proof depends upon the fact that by Theorem 1 supra an invariant $\sigma \neq \pm \mathrm{id}_{\mathbf{R}^2}$ of the equivalent identity (see [6], [7])

$$\sum_{(\mu_1,\mu_2)\in \mathbf{Z}\times\mathbf{Z}} H(H_m;\mu_1,\mu_2).H(H_n;\mu_1,\mu_2) = \sum_{(\mu_1,\mu_2)\in \mathbf{Z}\times\mathbf{Z}} |H(H_m,H_n;\mu_1,\mu_2)|^2$$

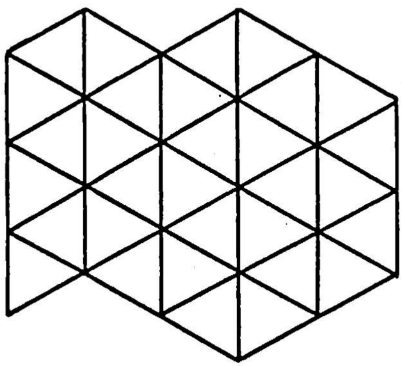
defines an elliptic Möbius transformation of **C**. Consequently it follows for the trace

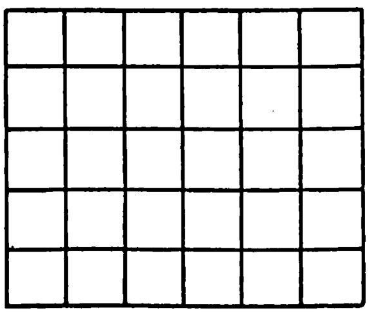
$$\mathrm{tr}\,\sigma \in \mathbf{Z}, \quad |\mathrm{tr}\,\sigma| < 2.$$

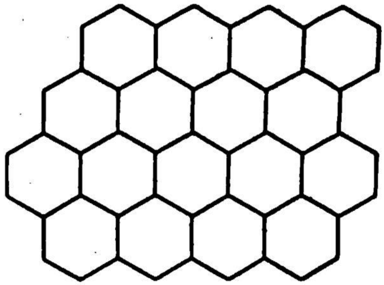
Notice that rotations of order $p = 5$ (quasi-crystals!) are excluded in the classification of Theorem 2 (cf. Weyl [10]).

3. Information Cells

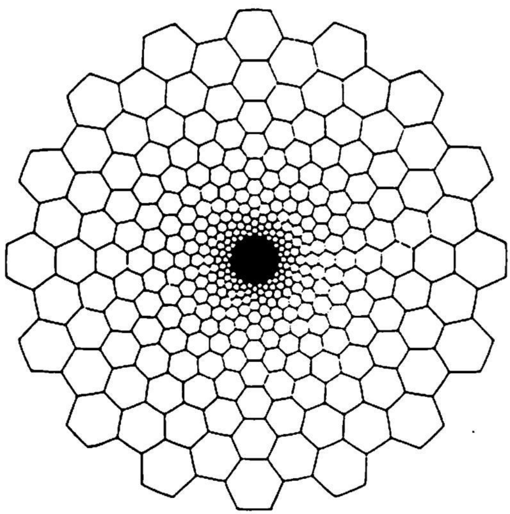
The realizations of the plane crystallographic groups $\mathbb{Z}/p\mathbb{Z}$, $p \in \{1,2,3,4,6\}$ by fundamental domains of planar lattices are called information cells or Nyquist cells. Their symmetry groups are isomorphic to the corresponding dihedral groups D_p of order $2p$. The figures displayed below show the regular patterns of spatially coded information cells in the cases $p = 3,4,6$.







The subsequent figure shows the information density extracted by the extra-foveal retina. Each of the hexagonal information cells represents the same number of sample points and contains about 200 ganglion cells in macaque monkey (see Koenderink and van Doorn [3], Kronauer and Zeevi [4], Porat and Zeevi [5]). Logarithmic scaling along the radial coordinate axis results in the regular honeycomb lattice (p = 6) displayed above corresponding to the fact well known from neuroanatomy that the transformation from visual field to the cortex is logarithmic.



As a final realization (p = 4) we refer to the higher order harmonic generation by laser radiation operating on a uniaxial crystal belonging to the tetragonal system like KDP or ADP. The irreducible linear representation of degree 2 of the dihedral group D_4 of order 8 explains the phenomenon of optical phase conjugation. For more details, see the paper [8].

References

1. Borwein, J.: Theta inversion, Heisenberg uncertainty, and radar. Amer. Math. Monthly **93**, 822-823 (1986)
2. Higgins, J.R.: Five short stories about the cardinal series. Bull. (New Series) Amer. Math. Soc. **12**, 45-89 (1985)
3. Koenderink, J.J., van Doorn, A.J.: Visual detection of spatial contrast; influence of location in the visual field, target extent and illuminance level. Biol. Cybernetics **30**, 157-167 (1978)
4. Kronauer, R.E., Zeevi, Y.Y.: Reorganization and diversification of signals in vision. IEEE Trans. Syst. Man Cybernetics, Vol. **SMC-15**, 91-101 (1985)
5. Porat, M., Zeevi, Y.Y.: The generalized Gabor scheme of image representation in biological and machine vision. IEEE Trans. 1987 (in press)
6. Schempp, W.: Radar ambiguity functions, the Heisenberg group, and holomorphic theta series. Proc. Amer. Math. Soc. **92**, 103-110 (1984)
7. Schempp, W.: Harmonic analysis on the Heisenberg nilpotent Lie group, with applications to signal theory. Pitman Research Notes in Math., Vol. **147**. Harlow, Essex: Longman. New York: J. Wiley & Sons 1986
8. Schempp, W.: Nonlinear laser optics I: Duality of semisimple rings and phase matching (to appear)
9. Schempp, W.: The oscillator representation of the metaplectic group applied to quantum electronics and computerized tomography (in print)
10. Weyl, H.: Symmetry. J. Washington Acad. Sciences **28**, 253-271 (1938). Also in: Collected papers, Vol. III, pp. 592-610. Berlin-Heidelberg-New York: Springer 1968

Received July 8, 1987

Lehrstuhl fuer Mathematik I
University of Siegen
D-5900 Siegen
Federal Republic of Germany

C.R. Math. Rep. Acad. Sci. Canada - Vol. IX, No. 6, December 1987 décembre

ON THE TRACE OF SYMMETRIC BI-DERIVATIONS

Gy. Maksa

Presented by J. *Aczél*, F.R.S.C.

Abstract. In this note we give a functional equation for the trace of symmetric bi-derivations and we characterize its non-negative solutions.

Let E be a real linear space. A function $d : R \to E$ is a derivation if d satisfies both equations

$$d(x+y)=d(x)+d(y) \qquad \text{and} \qquad d(xy)=xd(y)+yd(x)$$

for all $x,y \in R$. In the case $E=R$ d is called real derivation. The description of real derivations can be found in the book [3] and this can be applied in the case of real linear space-valued derivations, too. It is clear from this description that there are non identically zero real derivations. This fact plays an important role in the discussions in connection with some functional equations of information theory. For example, if d is a non identically zero real derivation then the function $f : [0,1] \to R$ defined by

$$f(0)=f(1)=0, \qquad f(x)=\frac{d(x)^2}{x(1-x)}, \quad 0<x<1$$

is a non-negative discontinuous solution of the fundamental equation of information (see [2]) and the function $g : [0,1] \to R$ given by

$$g(0)=g(1)=0, \qquad g(x)=\frac{d(x)^2}{x}, \quad 0<x<1$$

is a non-negative discontinuous solution of the additivity equation of Shannon entropy (see [6]). On the other hand the solutions bounded on a set of positive measure of these equations are continuous (see [5,6]). The function d^2 in the examples above can be considered as the trace (or diagonalization) of the function $D : R^2 \to R$ given by

$$D(x,y)=d(x)d(y) \qquad x,y \in R.$$

If d is a real derivation then D obviously satisfies the following conditions : D is symmetric and bi-additive, that is,

(1) $$D(x,y)=D(y,x) \qquad x,y \in R$$

(2) $$D(x+y,z)=D(x,z)+D(y,z) \qquad x,y,z \in R$$

and, in addition

(3) $$D(xy,z)=xD(y,z)+yD(x,z) \qquad x,y,z \in R.$$

In the following a function $D : R^2 \to R$ satisfying (1),(2) and (3) will be called a <u>symmetric bi-derivation</u>. The purpose of this paper is to find a functional equation for the trace of symmetric bi-derivations and to characterize its non-negative solutions.

Let D be a symmetric bi-derivation and f be its trace, that is,

(4) $$f(x)=D(x,x) \qquad x \in R$$

Then, by (1), (2) and (3), we have

$$f(xy)=D(xy,xy)=xD(y,xy)+yD(x,xy)=x^2D(y,y)+y^2D(x,x)+2xyD(x,y)=$$
$$=x^2D(y,y)+y^2D(x,x)+xy[D(x+y,x+y)-D(x,x)-D(y,y)]=$$
$$=x^2f(y)+y^2f(x)+xy[f(x+y)-f(x)-f(y)]$$

for all $x,y \in R$. This computation shows that f satisfies the functional equation

(5) $$f(xy)=(y^2-xy)f(x)+(x^2-xy)f(y)+xyf(x+y)$$

for all $x,y \in R$. Our main result is contained in the following

THEOREM. <u>If</u> $f : R \to R$ <u>is a solution of</u> (5) <u>then there exists a symmetric bi-derivation</u> D <u>such that</u> (4) <u>holds. If, in addition,</u> f <u>is non-negative then there exist a real Hilbert space</u> $(E,<,>)$ <u>and a derivation</u> $d : R \to E$ <u>such that</u> $f(x)=<d(x),d(x)>$ <u>for all</u> $x \in R$.

Proof. Let $y=x$ in (5). Then

$$f(x^2)=x^2 f(2x) \qquad x \in R \tag{6}$$

which shows that $f(0)=0$ and f is an even function. Write $-y$ instead of y in (5), use that f is even and substract the equation so obtained from (5). Thus we have

$$f(x+y)+f(x-y)=2f(x)+2f(y) \qquad x,y \in R$$

that is, f is a quadratic function. It is known from [1] that there exists a symmetric bi-additive function $D : R^2 \to R$ such that (4) holds. In what follows we prove that D satisfies (3), too. Since f is quadratic (6) implies that

$$f(x^2)=4x^2 f(x) \qquad x \in R, \tag{7}$$

in particular

$$f(1)=D(1,1)=0 \tag{8}$$

and it follows from (5) that

$$f(xy)-y^2 f(x)-x^2 f(y)=2xyD(x,y) \qquad x,y \in R \tag{9}$$

Because of (8) this implies that

$$D(x,1)=0 \qquad x \in R \tag{10}$$

Now write x^2 and y^2 instead of x and y, respectively in (9) and use (7) and (9). Thus

$$2x^2y^2D(x^2,y^2)=f(x^2y^2)-(y^2)^2f(x^2)-(x^2)^2f(y^2)=4x^2y^2[f(xy)-y^2f(x)-x^2f(y)]=$$
$$=8x^3y^3D(x,y)$$

which implies (since $D(x,0)=D(0,y)=0$)

$$D(x^2,y^2)=4xyD(x,y) \qquad x,y \in R \tag{11}$$

Write $x+y$ and z instead of x and y, respectively in (11). Since D is symmetric and bi-additive we get

$$D(x^2,z^2)+2D(xy,z^2)+D(y^2,z^2)=4(x+y)zD(x,z)+4(x+y)zD(y,z) \qquad x,y,z \in R.$$

This equation and (11) imply

$$D(xy,z^2)=2z[yD(x,z)+xD(y,z)] \qquad x,y,z \in R \tag{12}$$

Finally, write $z+1$ instead of z in (12). Then by (12) and (10) we obtain (3).

The second statement of our theorem is an obvious consequence of the result just proved and Corollary 1 in [4].

We remark that the solutions of (5) bounded on a set of positive measure are identically zero because they are quadratic functions and their value is 0 at the point 1.

References

[1] Aczel, J., The general solution of two functional equations by reduction to functions additive in two variables and with the aid of Hamel bases, Glasnik Mat.-Fiz. Astr. 20 (1965), 65-73.

[2] Daroczy, Z., Maksa, Gy., Nonnegative information functions, Analytic Function Methods in Probability and Statistics, Coll. Math. Soc. J. Bolyai, 21 (1979), 65-76.

[3] Kuczma, M., An Introduction to the Theory of Functional Equations and Inequalities, Cauchy's Equation and Jensen's Inequality, Panstwowe Wydawnictwo Naukowe, Warszawa-Krakow, 1985.

[4] Maksa, Gy., A remark on symmetric biadditive functions having nonnegative diagonalization, Glasnik Mat., 15(35) (1980), 279-282.

[5] Maksa, Gy., Bounded symmetric information functions, C.R. Math. Rep. Acad. Sci. Canada, Vol. II., No 5., (1980), 247-252.

[6] Maksa, Gy., On the bounded solutions of a functional equation, Acta Math. Acad. Sci. Hungar., 37(4), (1981), 445-450.

Department of Mathematics
L. Kossuth University
H-4010 Debrecen
Pf. 12, Hungary

Received July 17, 1987

ON Γ-EXTENSIONS OF TOTALLY REAL AND COMPLEX MULTIPLICATION FIELDS

I. Kersten and J. Michaliček

Presented by P. Ribenboim, F.R.S.C.

INTRODUCTION. Suppose K is a number field with ring of integers $\mathfrak{O}$, and p is an odd prime. Letting $R = \mathfrak{O}[p^{-1}]$ the set of isomorphism classes of Γ-extensions of R form a $\mathbb{Z}_p$-module $H^1(R,\Gamma)$, where Γ is a topological group isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. There is a $\mathbb{Z}_p$-submodule $H(R,\Gamma)$ consisting of those classes of Γ-extensions which, in some sense, have a normal basis over R.

The purpose of this paper is to announce the following result: If K is totally real or has complex multiplication then there is a $\mathbb{Z}_p$-module isomorphism $H(R,\Gamma) \cong \mathbb{Z}_p^{r_2+1}$ where r_2 denotes the number of complex places of K.

Proofs will appear elsewhere. Throughout p is an odd prime and K is a number field, i.e. a finite field extension of $\mathbb{Q}$.

1. Γ-EXTENSIONS.

A Γ-field extension of K is a field extension K_∞ of K with Galois group Γ isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. One may regard a Γ-field extension as a sequence of fields

$$K = K_0 \subset K_1 \subset \ldots \subset K_\infty = \bigcup_{n\geq 0} K_n$$

where each K_n is a Galois extension of K with group $\Gamma_n := \Gamma/p^n\Gamma \cong \mathbb{Z}/p^n\mathbb{Z}$. Each Γ-field extension is unramified at all primes not lying above p, ([6], Prop. 13.2.) Thus letting $\mathfrak{O}_n$ be the ring of integers in K_n for $n \geq 0$ and setting $R_n = \mathfrak{O}_n[p^{-1}]$ one obtains a connected Γ-ring extension $R = \bigcup_n R_n$ of $R = R_0$. An arbitrary Γ-extension of R is a sequence of rings $R = R_0 \subset R_1 \subset \ldots \subset R_\infty = \bigcup_n R_n$, where each R_n is a Γ_n-extension of R, i.e. a Galois ring extension of R with group Γ_n as defined in [1]. Given two Γ-extensions $R_\infty = \bigcup R_n$ and $S_\infty = \bigcup S_n$ of R one can show: If there is an isomorphism of Γ_n-extensions $R_n \cong S_n$ for all n, then there is an isomorphism $f_n : R_n \to S_n$ for all n such that $f_n(x) = f_m(x)$ whenever $x \in R_m$ and $m \le n$. There is a product $R_n \cdot S_n$ of Γ_n-extensions of R inducing an abelian group structure on the set $H^1(R,\Gamma_n)$ of isomorphism classes of Γ_n-extensions of R. The group $H^1(R,\Gamma_n)$ is a $(\mathbb{Z}/p^n\mathbb{Z})$-module as follows from [3], Theorem 4. Let $H^1(R,\Gamma) = \varprojlim H^1(R,\Gamma_n)$ with respect to the homomorphisms $\pi_{m,n}: H^1(R,\Gamma_n) \to H^1(R,\Gamma_m)$, $[R_n] \to [R_n^u]$, where u is the subgroup of order p^{n-m} of Γ_n for $m \le n$.

For each $n > 0$ there is a subgroup $H(R,\Gamma_n)$ of $H^1(R,\Gamma_n)$ consisting of those classes of Γ_n-extensions which have a normal basis over R, and $\pi_{m,n}$ induces a group homomorphism $H(R,\Gamma_n) \to H(R,\Gamma_m)$ for $m \le n$ [5],1. Let $H(R,\Gamma)$ be the subset of $H^1(R,\Gamma)$ consisting of those classes of Γ-extensions $R_\infty = \bigcup R_n$ such that each R_n has a normal basis over R. Then $H(R,\Gamma)$ is a $\mathbb{Z}_p$-submodule of $H^1(R,\Gamma)$ since the projective limit is left exact.

There is a canonical isomorphism $H^1(R,\Gamma) \cong H^1(K,\Gamma)$, and it is known that $H^1(K,\Gamma)$ is isomorphic to $\mathbb{Z}_p^{r_2+1+\delta}$ for some integer $\delta = \delta(K) \ge 0$. The conjecture $\delta(K) = 0$ is called Leopoldt's conjecture, [6], §5.5 and Theorem 13.4.

2. Γ_n-EXTENSIONS WITH NORMAL BASIS. Assume τ is a generator of Γ_n, and R_n is a Γ_n-extension of R having a normal basis $(X_i = \tau^i(X_0) \mid i = 0,\ldots,p^n-1)$. Then $X = \sum_i X_i \tau^{-i}$ is a unit in the group ring $R_n[\Gamma_n]$ and $\tau(X) = \tau \cdot X$ with $\tau(X) = \sum \tau(X_i)\tau^{-i}$, [4], Lemma 1.1.

Thus we may regard a normal basis of a Γ_n-extension R_n of R as a unit X in $R_n[\Gamma_n]$ satisfying $\tau(X) = \tau\cdot X$. Defining for $i \in \mathbb{Z}$ an R-algebra homomorphism ν_i from $R_n[\Gamma_n]$ to $R_n[\Gamma_n]$ via $\nu_i(\tau) = \tau^i$, then each Γ_n-extension with normal basis has a normal basis X satisfying $\nu_0(X) = 1$ and $X^{-1} = \nu_{-1}(X)$, [4], Prop. 1.1. We call such a normal basis normalized.

Let ζ_n be a primitive p^n-th root of unity in $\mathbb{C}$. Defining for $i \in \mathbb{Z}$ an R-algebra homomorphism χ_i from $R[\Gamma_n]$ into $R(\zeta_n)$ via $\chi_i(\tau) = \zeta_n^i$, then $\chi_i(x)$ is the i-th Fourier coefficient of $x \in R[\Gamma_n]$.

Because of the following theorem we may regard the cyclotomic Γ-field extension of K, defined in [6], §7.3, as an element of $H(R,\Gamma)$.

2.1 THEOREM. *Let $K = \bigcup_n K_n$ be the cyclotomic Γ-field extension of K and $Z_n = \mathfrak{O}_n[p^{-1}]$ for $n \geq 0$. Then each Z_n has a normalized normal basis over Z_0 such that all its Fourier coefficients are p-power roots of unity.*

3. $H(R,\Gamma)$ FOR A TOTALLY REAL FIELD.

Let K be totally real, i.e. all embeddings of K into $\mathbb{C}$ lie in $\mathbb{R}$. As before set $R = R_0 = \mathfrak{O}[p^{-1}]$.

3.1 THEOREM. *Let $R_\infty = \bigcup_n R_n$ be a connected Γ-extension of R such that R_n has a normal basis over R for all n. Then there is an R-algebra isomorphism $R_n \cong Z_n$ for all $n > 0$, where Z_n is defined as in 2.1.*

Assume that there is N such that R_N is not isomorphic to Z_N. Let $X \in R_n[\Gamma_n]$ be a normalized normal basis of R_n over R and $n > N$. Letting $q = (X\,\nu_r(X^{-1}))^{p^n}$, where $r = p^c + 1$ and $c > 1$ is an integer, then q, being a p^n-th power in $R_n[\Gamma_n]$, lies in $R[\Gamma_n]$. Since all coefficients of q are in a totally real field, the equation $X^{-1} = \nu_{-1}(X)$

implies that the Fourier coefficients $\chi_i(q)$ have absolute value 1 for $i = 0,\dots,p^n-1$. Choosing c and n big enough one can show that all $\chi_i(q)$ are algebraic integers. Since $K(\zeta_n)$ is a complex multiplication field this implies that all $\chi_i(q)$ are roots of unity ([6], Lemma 1.6), contradicting the above assumption. The details will appear elsewhere. From 2.1 and 3.1 we get the following Corollary.

3.2 COROLLARY. *Suppose* $R_\infty = \bigcup R_n$ *is a nontrivial* Γ-*extension of* R, *and each* R_n *has a normal basis over* R. *Then, setting* $Z_\infty = \bigcup Z_n$, *there is an isomorphism of* Γ-*extensions* $R_\infty \cong Z_\infty^\omega$ *for some* $\omega \in \mathbf{Z}_p$. *The correspondence* $\omega \to Z_\infty^\omega$ *induces a* $\mathbf{Z}_p$-*module isomorphism* $\mathbf{Z}_p \xrightarrow{\sim} H(R,\Gamma)$.

It is proved in [2] that $|H(R,\Gamma_n)| = p^{n(r_2+1)}\cdot O(1)$ for an arbitrary number field K. This result combined with 2.1 also implies the existence of an isomorphism $H(R,\Gamma) \cong \mathbf{Z}_p$ if K is totally real.

4. H(R,Γ) FOR A COMPLEX MULTIPLICATION FIELD.

Let K be a complex multiplication field, i.e. K is a totally imaginary quadratic field extension of a totally real field, denoted by K^+. There is an automorphism ι of K which for each embedding from K into $\mathbb{C}$ coincides with complex conjugation. Write $\iota(\lambda) = \bar\lambda$ for $\lambda \in K$. Let $R = \mathfrak{O}[p^{-1}]$ and $R^+ = \mathfrak{O}^+[p^{-1}]$. For any R-module M define the R-module $\bar M$ to be the additive group M equipped with a new R-structure $\lambda.x = \bar\lambda x$ for $\lambda \in R$ and $x \in M$.

4.1 THEOREM. *Let* $R_\infty = \bigcup R_n$ *be a* Γ-*extension of* R. *If* $R_n \cdot \bar R_n$ *has a normal basis over* R *for all* n *there is* $s \geq 0$ *such that* $R_n^{p^s}$ *has a normal basis over* R *for all* n.

The isomorphism classes of Γ-extensions $R_\infty = \bigcup R_n$ with $R_n \cong \dot{R}_n$ for all n form a $\mathbb{Z}_p$-submodule of $H^1(R,\Gamma)$ which we call $\mathfrak{C}$. If R_∞ is connected and $R_n \cong \dot{R}_n$ for all n then $\iota : R \to R$ can be extended to a ring automorphism from R_n to R_n. Passing to the fixed rings of ι for all n one obtains a Γ-extension $R_\infty^+ = \bigcup R_n^+$ of R^+. This implies

$$\mathbb{Z}_p\text{-rank } \mathfrak{C} = 1 + \delta(K^+)$$

since the class of the cyclotomic Γ-extension Z_∞ of R is in $\mathfrak{C}$. The isomorphism classes of Γ-extensions $R_\infty = \bigcup R_n$ with $[R_n \cdot \dot{R}_n] = 1$ for all n form a $\mathbb{Z}_p$-submodule of $H^1(R,\Gamma)$ which we call $\mathfrak{N}$. One has

$$H^1(R,\Gamma) = \mathfrak{C} \oplus \mathfrak{N} .$$

Since $\delta(K) = \delta(K^+)$ and $\mathbb{Z}_p$-rank $H^1(R,\Gamma) = 1 + r_2 + \delta(K)$ we obtain

$$\mathbb{Z}_p\text{-rank } \mathfrak{N} = r_2 .$$

It follows from 3.2 that $H(R,\Gamma) \subset \langle Z_\infty \rangle \oplus \mathfrak{N}$. Theorem 4.1 implies that there is $t \geq 0$ such that $\langle Z_\infty \rangle \oplus \mathfrak{N}^{p^t} \subset H(R,\Gamma)$. Thus $\mathbb{Z}_p$-rank $H(R,\Gamma) = r_2 + 1$. We now obtain:

4.2 COROLLARY. *There is a $\mathbb{Z}_p$-module isomorphism* $\mathbb{Z}_p^{r_2+1} \cong H(R,\Gamma)$.

4.3 COROLLARY. *Leopoldt's conjecture holds for K if and only if the cyclotomic Γ-field extension is the only Γ-extension $K_\infty = \bigcup K_n$ of K such that each K_n is a complex multiplication field.*

REFERENCES.

[1] S. U. Chase, D.K. Harrison and A. Rosenberg. Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. 52 (1965), 15-33.

[2] C. Greither. On Galois extensions of commutative rings with Galois group $\mathbb{Z}/p^n\mathbb{Z}$, Preprint.

[3] D.K. Harrison. Abelian extensions of commutative rings, Mem. Amer. Math. Soc. 52 (1965), 1-14.

[4] I. Kersten and J. Michaliček. Kummer theory without roots of unity, to appear in J. Pure Appl. Algebra 1988.

[5] M. Orzech. A cohomological description of ablian Galois extensions, Trans. Amer. Math. Soc. 137 (1969), 481-499.

[6] L.C. Washington, Introduction to cyclotomic fields, Springer-Verlag New York, Heidelberg, Berlin 1982.

FB Mathematik
Gaußstr.20
D-5600 Wuppertal 1

Mathematisches Seminar
Bundesstr.55
D-2000 Hamburg 13

W. Germany

Received October 6, 1987

C.R. Math. Rep. Acad. Sci. Canada - Vol. IX, No. 6, December 1987 décembre

A REMARK ON A FUNCTIONAL EQUATION CHARACTERIZING THE JACOBIAN ELLIPTIC FUNCTIONS

STEFANIA PAGANONI MARZEGALLI

Presented by J. Aczél, F.R.S.C.

SUMMARY. It is proved in a direct and simple way that the only non constant analytic solutions of

$$(1)\qquad f(z_1+z_2+z_3)\,[f(z_1+z_3)f(z_2) - f(z_2+z_3)f(z_1)] = f(z_3)\,[f(z_2+z_3)f(z_2) - f(z_1+z_3)f(z_1)]$$

are the Jacobi elliptic functions *sn* .

In [3] the authors considered the functional equation (1) and proved that the only non constant analytic solutions of (1), defined in a neigbourhood of the origin, are the elliptic Jacobi functions $sn(z,k)$. In order to obtain this result the study of (1) was reduced to that of the functional equation

$$(2)\qquad g(z_1+z_2) - g(z_1) - g(z_2) = f(z_1)f(z_2)f(z_1+z_2)\ .$$

It was proved that (2) must have analytic solutions (f,g) and the form of the solutions f of (1) was deduced from the solution (f,g) of (2) (see [2]).

The aim of this paper is to show in a more simple and direct way that every non constant analytic solution of (1) has to satisfy the differential equation

$$(3)\qquad ff'' - 2f'^2 + f'''(0)f^2 + 2 = 0 \quad , \quad f(0)=0\ ,\ f'(0)=1.$$

By [4], the only non constant analytic solutions of (1) have the form

$$f(z) = \alpha\, \mathrm{sn}(z/\alpha;k) \qquad (\alpha,k\in\mathbb{C}\ ,\ \alpha\neq 0).$$

Theorem. *Consider the functional equation (1). A non constant analytic function, defined in a neighbourhood of the origin, is a solution of (1) if and only if it is of the form*

(4) $$f(z) = \beta\, \mathrm{sn}(z/\alpha;k) \qquad (\alpha,\beta,k\in\mathbb{C}\ ,\ \alpha,\beta\neq 0).$$

Proof. Let f be a non constant analytic solution of (1) defined in a neighbourhood of the origin. By putting $z_3=0$ into (1) we obtain

$$f(0)\,[f(z_2)^2 - f(z_1)^2] = 0\ .$$

Therefore, as $f\not\equiv c$, $f(0)=0$.

Differentiating (1) with respect to z_1 we get

(5) $$f'(z_1+z_2+z_3)\,[f(z_1+z_3)f(z_2) - f(z_2+z_3)f(z_1)] +$$
$$+ f(z_1+z_2+z_3)\,[f'(z_1+z_3)f(z_2) - f(z_2+z_3)f'(z_1)] =$$
$$= - f(z_3)\,[f'(z_1+z_3)f(z_1) + f(z_1+z_3)f'(z_1)].$$

Putting $z_1 = 0$ and $z = z_3 = -z_2$ in (5) gives

$$f'(0)\,[f(z)f(-z)] = -f'(0)f(z)^2,$$

that is,

(6) $$f'(0)\, f(z)\,[f(z) + f(-z)] = 0\ .$$

It is easy to see that $f'(0)\neq 0$ (otherwise, putting $z_2 = -(z_1+z_3)$ in (5), we should have $f(z_3)\dfrac{d}{dz_1}\Big[f(z_1+z_3)f(z_1)\Big] = 0$; therefore either $f(z)\equiv 0$ or $f(z+z_3)f(z) = c(z_3)$, but putting $z = 0$ we have $c(z_3) = 0$ and then again $f(z)\equiv 0$, contrary to our supposition).

So from (6) we have $f(-z) = -f(z)$.

From now on we assume, without loss of generality,

$$(7) \qquad f'(0) = 1.$$

(Indeed f is a solution of (1) if and only if γf is a solution of (1) with $\gamma \in \mathbb{C}\setminus\{0\}$).

Differentiating (5) twice with respect to z_2 we get

$$
\begin{aligned}
(8) \qquad & f'''(z_1+z_2+z_3)\,[f(z_1+z_3)f(z_2) - f(z_2+z_3)f(z_1)] + \\
& + 2f''(z_1+z_2+z_3)\,[f(z_1+z_3)f'(z_2) - f'(z_2+z_3)f(z_1)] + \\
& + f'(z_1+z_2+z_3)\,[f(z_1+z_3)f''(z_2) - f''(z_2+z_3)f(z_1)] + \\
& + f''(z_1+z_2+z_3)\,[f'(z_1+z_3)f(z_2) - f(z_2+z_3)f'(z_1)] + \\
& + 2f'(z_1+z_2+z_3)\,[f'(z_1+z_3)f'(z_2) - f'(z_2+z_3)f'(z_1)] + \\
& + f(z_1+z_2+z_3)\,[f'(z_1+z_3)f''(z_2) - f''(z_2+z_3)f'(z_1)] \quad = \quad 0.
\end{aligned}
$$

Putting $z_2 = 0$, $z = z_1 = -z_3$ in (8), we deduce that every non constant analytic solution of (1) has to satisfy (3).

In [4] it has been proved that f is a solution of (3) if and only if it satisfies a differential equation of the form

$$(9) \qquad (f')^2 = [1 - (1/\alpha^2)f^2]\,[1 - (k^2/\alpha^2)f^2] \quad , \quad f(0)=0, f'(0)=1$$

with suitable constants $\alpha, k \in \mathbb{C}$, $\alpha \neq 0$.

Now, it is well known that f satisfies (9) if and only if

$$f(z) = \alpha\, \mathrm{sn}(z/\alpha; k) \qquad (\alpha, k \in \mathbb{C}\ ,\ \alpha \neq 0).$$

If we drop the condition (7), (4) follows immediately.

By the addition formulae of the Jacobi's elliptic functions (see [1]) it is easy to verify that every function of the form (4) is a solution of (1).

REFERENCES

[1] Copson, E. T., *An Introduction to the Theory of Functions of a Complex Variable*, Oxford Univ. Press., 1970.

[2] Fenyö, I. -Paganoni, L., *Su una equazione funzionale proveniente dalla teoria delle funzioni ellitticche jacobiane*, to appear in Rend. Mat. Appl.

[3] Fenyö, I. -Paganoni, L., *A Functional Equation which characterizes the Jacobian sn(z;k) Functions*, to appear in Rend. Mat. Appl.

[4] Fenyö, I. -Paganoni, L., *Sur la connexion entre une équation fonctionnelle et l'équation différentielle des fonctions elliptiques Jacobiennes*, C. R. Math. Rep. Acad. Sci. Canada 7 (1985), 195-199.

Dipartimento di Matematica
Università degli Studi di Milano
via C. Saldini 50
I-20133 Milano, Italy

Received October 9, 1987

Mailing Addresses

1. G. Grätzer — Department of Mathematics
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

2. I. Kersten — F.B. Mathematik
Gaußstr. 20
D-5600 Wuppertal 1, W. Germany

3. Gy. Maksa — Department of Mathematics
L. Kossuth University
H-4010 Debrecen, Pf. 12, Hungary

4. V. Mandekić-Botteri — Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture
University of Split
Boškovićeva bb, 5800 Split, Yugoslavia

5. S.P. Mazegalli — Dipartimento di Matematica
Universita degli Studi di Milano
via C. Saldini 50
1-20133 Milano, Italy

6. J. Michaliček — Mathematisches Seminar
Bundesstr. 55
D-2000 Hamburg 13

7. W. Schempp — Lehrstuhl fuer mathematik I
University of Siegen
D-5900 Siegen
Federal Republic of Germany

Index - Volume IX

MEMOIRS - MEMOIRES

ARTICLES

Paging of Vol. IX

(1) 1-76	(2) 77-132	(3) 133-175
(4) 177-205	(5) 207-272	(6) 273-321