Jaroslav Ježek; Tomáš Kepka

Varieties of abelian quasigroups

Czechoslovak Mathematical Journal, Vol. 27 (1977), No. 3, 473–503

Persistent URL: http://dml.cz/dmlcz/101484

Czechoslovak Mathematical Journal, 27 (102) 1977, Praha

VARIETIES OF ABELIAN QUASIGROUPS

JAROSLAV JEŽEK and TOMÁŠ KEPKA, Praha

(Received August 5, 1975)

Abelian quasigroups were studied by many authors, but the universal-algebraic approach to their study was a fallow. Only few results of this kind can be cited, e.g. [4] and [5]. This paper represents an attempt of systematic study concerning varieties of abelian quasigroups. It would be very pleasant (for us) to find a complete description of the lattice of varieties. Although the lattice is countable, the task seems to be (at least for us) very difficult. However, we succeeded in describing several special sublattices, in finding all minimal subvarieties and in characterizing subvarieties with some prescribed properties. The authors were delighted that several branches of classical algebra proved to be useful in this non-associative case.

1. UNIVERSAL-ALGEBRAIC BACKGROUND

Although the aim of this paper is to study quasigroups, the methods employed will involve various other algebraic structures and thus we start with a survey of necessary facts from universal algebra.

Let $\mathcal{K}$ be a class of algebras $A(f_1, f_2, \ldots)$ of a given similarity type Δ. We denote by Δ^* the type obtained from Δ by adding a new nullary operation symbol. The class of all algebras $A(f_1, f_2, \ldots, h)$ of the type Δ^* such that $A(f_1, f_2, \ldots) \in \mathcal{K}$ (here h is the new nullary operation, i.e. an arbitrary element of A) will be denoted by $\mathcal{K}^*$ and the algebras from $\mathcal{K}^*$ will be called pointed $\mathcal{K}$-algebras. Evidently, if $A(f_1, f_2, \ldots$ $\ldots, h) \in \mathcal{K}^*$, then the algebras $A(f_1, f_2, \ldots, h)$ and $A(f_1, f_2, \ldots)$ have the same congruence lattices and thus if one of them is simple or subdirectly irreducible, then the other has the same property. However, $A(f_1, f_2, \ldots)$ has more subalgebras than $A(f_1, f_2, \ldots, h)$.

Let $\mathcal{K}_1$ be a class of algebras of type Δ_1 and $\mathcal{K}_2$ a class of algebras of type Δ_2. A one-to-one mapping ε of $\mathcal{K}_1$ onto $\mathcal{K}_2$ is called an equivalence between $\mathcal{K}_1$ and $\mathcal{K}_2$ if the following two conditions are satisfied:

(i) If $A \in \mathscr{K}_1$, then the algebras A and $\varepsilon(A)$ have the same underlying sets.
(ii) If $A, B \in \mathscr{K}_1$, then a mapping of A into B is a homomorphism of A into B iff it is a homomorphism of $\varepsilon(A)$ into $\varepsilon(B)$.

If such an equivalence exists, the classes $\mathscr{K}_1$ and $\mathscr{K}_2$ are called equivalent.

Varieties are equationally definable classes of algebras. If $\mathscr{V}$ is a variety, then $\mathscr{L}(\mathscr{V})$ denotes the lattice of its subvarieties.

Let $\mathscr{V}$ be a variety. Let us call a subvariety $\mathscr{K}$ of $\mathscr{V}^*$ reducible if $\mathscr{K} = \mathscr{H}^*$ for a subvariety $\mathscr{H}$ of $\mathscr{V}$, i.e. if $A(f_1, f_2, \dots, h) \in \mathscr{K}$ implies $A(f_1, f_2, \dots, k) \in \mathscr{K}$ for all $k \in A$.

The proofs of the following five lemmas are easy and some of them can be found in [9].

1.1. Lemma. *Let $\mathscr{K}$ be a class of algebras of a given type. Then $\mathscr{K}^*$ is a variety iff $\mathscr{K}$ is a variety.*

1.2. Lemma. *If $\mathscr{V}$ is a variety, then the lattice $\mathscr{L}(\mathscr{V})$ is isomorphic to the lattice of reducible subvarieties of $\mathscr{V}^*$.*

1.3. Lemma. *Let $\mathscr{V}$ be a variety, $A(f_1, f_2, \dots, h) \in \mathscr{V}^*$ and $X \subseteq A$. Then $A(f_1, f_2, \dots$ $\dots, h)$ is free in $\mathscr{V}^*$, with free basis X, iff the algebra $A(f_1, f_2, \dots)$ is free in $\mathscr{V}$, with free basis $X \cup \{h\}$.*

1.4. Lemma. *Let a class $\mathscr{K}$ of algebras be equivalent to a variety. Then $\mathscr{K}$ is a variety iff it is closed with respect to subalgebras.*

1.5. Lemma. *Let ε be an equivalence between two varieties $\mathscr{V}_1$ and $\mathscr{V}_2$.*

(i) *If $A, B \in \mathscr{V}_1$, then A is a subalgebra of B iff $\varepsilon(A)$ is a subalgebra of $\varepsilon(B)$.*
(ii) *If $A \in \mathscr{V}_1$ and $X \subseteq A$ is a subset, then X is closed in A iff it is closed in $\varepsilon(A)$.*
(iii) *If $A \in \mathscr{V}_1$ and $X \subseteq A$, then X generates A iff it generates $\varepsilon(A)$.*
(iv) *If $A \in \mathscr{V}_1$ and r is an equivalence on A, then r is a congruence of A iff it is a congruence of $\varepsilon(A)$.*
(v) *If $A \in \mathscr{V}_1$ and $(B_i)_{i \in I}$ is a family of algebras from $\mathscr{V}_1$, then $A = XB_i$ iff $\varepsilon(A) = X\varepsilon(A_i)$.*
(vi) *If A is a free $\mathscr{V}_1$-algebra with free basis X, then $\varepsilon(A)$ is a free $\mathscr{V}_2$-algebra with free basis X.*
(vii) *A class $\mathscr{K} \subseteq \mathscr{V}_1$ is a variety iff the class $\{\varepsilon(A); A \in \mathscr{K}\}$ is a variety.*
(viii) *$\mathscr{L}(\mathscr{V}_1) \simeq \mathscr{L}(\mathscr{V}_2)$.*

A variety $\mathscr{V}$ is called a Schreier variety if every subalgebra of any $\mathscr{V}$-free algebra is $\mathscr{V}$-free.

A variety $\mathscr{V}$ is called extensive ([6]) if every algebra from $\mathscr{V}$ can be embedded into an algebra from $\mathscr{V}$ which has a one-element subalgebra. A variety $\mathscr{V}$ is extensive iff every two algebras from $\mathscr{V}$ have a common extension in $\mathscr{V}$.

A variety $\mathscr{V}$ is said to have the strong amalgamation property if the following holds for any triple $A, B, C \in \mathscr{V}$: if A is a subalgebra of both B and C and $A = B \cap C$, then there exists an algebra $D \in \mathscr{V}$ such that both B and C are subalgebras of D. An equivalent formulation: for any triple $A, B, C \in \mathscr{V}$ and any pair of injective homomorphisms $f : A \to B$, $g : A \to C$ there exists an algebra $D \in \mathscr{V}$ and two injective homomorphisms $h : B \to D$, $k : C \to D$ such that $h \circ f = k \circ g$ and $h(B) \cap k(C) = h(f(A))$.

Quasigroups are algebras $Q(\cdot, /, \backslash)$ with three binary operations satisfying the following four identies:

$$(xy)/y = x\,, \quad x\backslash(xy) = y\,, \quad (x/y)\,y = x\,, \quad x(x\backslash y) = y\,.$$

The class of all quasigroups is thus a variety. It is equivalent to the class of all groupoids with unique division, which is not a variety.

2. AUXILIARY RESULTS CONCERNING RINGS AND MODULES

By a ring we mean an associative ring with unit. An ideal is always a two-sided ideal. Let R be a ring. The set of all ideals of R is a complete modular lattice with respect to inclusion; it will be denoted by $\mathscr{I}(R)$. Further, by an R-module we mean always a unital left R-module. The class of all R-modules will be denoted by $R\mathscr{M}$. Every ring R (and every its left ideal, as well) can be considered an R-module. Let $M \in R\mathscr{M}$, let $N \subseteq M$ be a submodule and $S \subseteq M$ a subset. Then the set $(N : S) = \{r \in R;\ rS \subseteq N\}$ is a left ideal of R. Throughout this paper, the symbol Z will be used for the ring of integers. Finally, all the results concerning rings and modules which we shall use can be found in [11], [12] and [3].

2.1. Lemma. *Let R be a left noetherian ring and let $I \subseteq R$ be a non-zero left ideal which is a free R-module. Then I is as a module isomorphic to R.*

Proof. The assertion follows from the fact that R contains no infinite direct sums of left ideals. ∎

2.2. Lemma. *Let R be a commutative noetherian ring such that $I \times R$ is a free module for every ideal I of R. Then R is a principal ideal domain.*

Proof. First we show that R is directly indecomposable. Indeed, let $e \in R$ be a non-trivial idempotent and $M = Re \times R$. Then M is a free module and $M/eM \simeq R(1 - e)$. On the other hand, if $M \simeq R \times R \times \ldots$, then $M/eM \simeq R(1 - e) \times R(1 - e) \times \ldots$, a contradiction, since $R(1 - e)$ is noetherian. Thus M is isomorphic to R, again a contradiction, since R contains no infinite direct sums of ideals.

Further, it is obvious that R is hereditary. However, every hereditary commutative noetherian ring is a direct sum of dedekind domains. Consequently, R is a dedekind domain. Finally, let A be an arbitrary finitely generated torsion-free R-module. Then A is projective, it is isomorphic to a finite direct sum of ideals and we see that $A \times F$ is a free module for finitely generated free module F. Clearly, $A \times F$ is finitely genetated and A possesses a finite free resolution, namely $0 \to F \to A \times F \to A \to 0$. According to [3, VII. § 4, Corollary 3], R is a unique factorization domain. Thus R is a principal ideal domain. ∎

2.3. Lemma. *Let R be a commutative ring, let K be an ideal with $(0 : K) = 0$ (in R) and I an ideal such that $I \times R/K$ is isomorphic to $F \times R/K$ for a free module F. Then I is isomorphic to F.*

Proof. Let M be a module and $N = \{x \in M; Kx = 0\}$. Then N is a submodule of M and we can put $M_1 = M/N$. Now we have $I \simeq (I \times R/K)_1 \simeq (F \times R/K)_1 \simeq F$. ∎

Let R be a ring. A module M is called cocyclic if it is isomorphic to a submodule of an injective hull of a simple module.

2.4. Lemma. *The following conditions are equivalent for a module M:*

(i) *M is cocyclic;*
(ii) *M contains an essential simple submodule;*
(iii) *M is subdirectly irreducible.*

Proof. Easy. ∎

2.5. Lemma. *Given a ring R, there is up to isomorphism only a set of subdirectly irreducible R-modules.*

Proof. Apply 2.4. ∎

2.6. Lemma. *Let R be a commutative noetherian domain such that the lattice $\mathscr{I}(R)$ is distributive. Then R is a Dedekind domain.*

Proof. This is a well known result (see [3]). ∎

2.7. Lemma. *Let K be a commutative field which is (as a ring) finitely generated. Then K is finite.*

Proof. It follows from Noether normalization lemma (Theorem X.6 of [12]) and from Cohen-Seidenberg theorem (Proposition IX. 9 of [12]) that K is an algebraic extension of its prime subfied P. If P is finite, then K is finite, too, since K is an algebraic extension of a finite degree over P. Suppose that P is the field of rational numbers. By the theorem on primitive elements (Theorem VII.14 of [12]) there exists an element $e \in K$ such that the ring K is generated by $P \cup \{e\}$. Since e is algebraic over P, there exists an irreducible polynomial φ with rational coefficients such that e is its root; moreover, we may suppose

$$\varphi(x) = x^n + r_{n-1}x^{n-1} + \ldots + r_1x + r_0$$

where $r_{n-1}, \ldots, r_0 \in P$. As is well-known, K is isomorphic to the field $P[x]/\varphi\, P[x]$ where $\varphi\, P[x]$ is the ideal generated by φ. Let $f_1/\varphi\, P[x], \ldots, f_m/\varphi\, P[x]$ be a finite generating set of the ring $P[x]/\varphi\, P[x]$. Denote by M the (finite) set of all numbers appearing as coefficients in one of the polynomials $f_1, \ldots, f_m, \varphi$. Since evidently the ring P is not finitely generated, there exists a rational number q not belonging to the subring R of P generated by M. Since $q/\varphi\, P[x] \in P[x]/\varphi\, P[x]$, we have

$$q = F(f_1, \ldots, f_m) + \varphi g$$

for a polynomial F in m indeterminates with integral coefficients and a polynomial

$$g = a_kx^k + \ldots + a_0$$

with coefficients $a_i \in P$. Put

$$F(f_1, \ldots, f_m) = c_0 + c_1x + c_2x^2 + \ldots$$

We may suppose $n \geqq 1$, since otherwise $K = P$ and everything is evident. Comparing the coefficients at x^{n+k} we get $0 = c_{n+k} + a_k$, so that $a_k \in R$. Comparing the coefficients at x^{n+k-1} we get $0 = c_{n+k-1} + a_{k-1} + a_kr_{n-1}$, so that $a_{k-1} \in R$. Comparing the coefficients at $x^{n+k}, x^{n+k-1}, \ldots, x^n$ we get $a_k, a_{k-1}, \ldots\ a_0 \in R$ so that $g \in R[x]$ and $q = F(f_1, \ldots, f_m) + \varphi g \in R[x]$, a contradiction with $q \notin R$. ∎

3. VARIETIES OF POINTED R-MODULES

Let R be a ring. R-modules can be viewed as algebras $M(+, rx)$ with one binary operation $+$ and a family of unary operations rx $(r \in R)$. In this case $R\mathcal{M}$ is a variety. Pointed R-modules are algebras $M(+, rx, h)$ such that $M(+, rx)$ is an R-module and h is a nullary operation, i.e. an element of M. The class $R\mathcal{M}^*$ of all pointed R-modules is a variety, too.

As is well known, the lattice $\mathcal{L}(R\mathcal{M})$ is isomorphic to the dual of the lattice $\mathcal{I}(R)$. If $\mathcal{V} \subseteq R\mathcal{M}$ is a subvariety and I is the corresponding element of $\mathcal{I}(R)$, then $I = \bigcap(0 : M)$, $M \in \mathcal{V}$ and $\mathcal{V}$ is just the class of all R-modules M with $IM = 0$ (i.e. the class of all R-modules which can be considered R/I-modules). Now we shall describe the lattice $\mathcal{L}(R\mathcal{M}^*)$ of varieties of pointed R-modules.

We denote by $\mathcal{K}(R)$ the lattice of all ordered pairs $\langle I, K\rangle$ such that $I \in \mathcal{I}(R)$ and K is a left ideal containing I; the lattice ordering is defined by $\langle I_1, K_1\rangle \leqq \langle I_2, K_2\rangle$ iff $I_2 \subseteq I_1$ and $K_2 \subseteq K_1$.

For every $\langle I, K\rangle \in \mathcal{K}(R)$ we denote by $\mu(\langle I, K\rangle)$ the class of all pointed R-modules $M(+, rx, h)$ such that $IM = 0$ and $Kh = 0$.

3.1. Lemma. *Let* $\langle I, K\rangle \in \mathscr{K}(R)$ *and* $\mathscr{V} = \mu(\langle I, K\rangle)$. *Then* $\mathscr{V}$ *is a subvariety of* $R\mathscr{M}^*$. *Furthermore, if* F *is a free* R/I*-module with a free basis* X *and* $M = F \times R/K$, *then* $M(+, rx, \langle 0, 1 + K\rangle)$ *is a free algebra in* $\mathscr{V}$ *and the set* $\{\langle x, 0\rangle; x \in X\}$ *is its free basis.*

Proof. Easy. ∎

3.2. Lemma. *Let* $\langle I, K\rangle \in \mathscr{K}(R)$, $\mathscr{V} = \mu(\langle I, K\rangle)$ *and let* $M(+, rx, h)$ *be the free algebra of rank* 1 *in* $\mathscr{V}$. *Then* $\mathscr{V}$ *is generated by this algebra,* $I = (0 : M)$ *and* $K = (0 : h)$.

Proof. Apply 3.1. ∎

If $\mathscr{V} \in \mathscr{L}(R\mathscr{M}^*)$, we put $\nu(\mathscr{V}) = \langle I, K\rangle$, where $I = \bigcap(0 : M)$ and $K = \bigcap(0 : h)$, $M(+, rx, h) \in \mathscr{V}$.

3.3. Lemma. (i) μ *is a mapping of* $\mathscr{K}(R)$ *into* $\mathscr{L}(R\mathscr{M}^*)$.
(ii) *If* $\langle I_1, K_1\rangle \leqq \langle I_2, K_2\rangle$ *then* $\mu(\langle I_1, K_1\rangle) \subseteq \mu(\langle I_2, K_2\rangle)$.
(iii) ν *is a mapping of* $\mathscr{L}(R\mathscr{M}^*)$ *into* $\mathscr{K}(R)$.
(iv) *If* $\mathscr{V}_1 \subseteq \mathscr{V}_2$ *then* $\nu(\mathscr{V}_1) \leqq \nu(\mathscr{V}_2)$.

Proof. Obvious. ∎

3.4. Proposition. *The lattice* $\mathscr{L}(R\mathscr{M}^*)$ *is isomorphic to the lattice* $\mathscr{K}(R)$. *The mapping* ν *is an isomorphism of* $\mathscr{L}(R\mathscr{M}^*)$ *onto* $\mathscr{K}(R)$ *and* μ *is the inverse isomorphism.*

Proof. It follows from 3.2 that $\nu(\mu(\langle I, K\rangle)) = \langle I, K\rangle$ for every $\langle I, K\rangle \in \mathscr{K}(R)$. By 3.3 it remains to prove $\mu(\nu(\mathscr{V})) = \mathscr{V}$ for every $\mathscr{V} \in \mathscr{L}(R\mathscr{M}^*)$. The inclusion $\mathscr{V} \subseteq \mu(\nu(\mathscr{V}))$ is clear. Let $\nu(\mathscr{V}) = \langle I, K\rangle$ and $M = R \times R$. Then $M(+, rx, \langle 0, 1\rangle)$ is a free pointed R-module of rank 1. There is a fully invariant congruence ϱ of M such that the corresponding factor M/ϱ is free of rank 1 in $\mathscr{V}$. Put $A = \{x \in R; \langle x, 0\rangle \mathrel{\varrho} \langle 0, 0\rangle\}$ and $B = \{y \in R; \langle 0, 0\rangle \mathrel{\varrho} \langle 0, y\rangle\}$. As one may check easily, A is an ideal, B is a left ideal and $A \subseteq B$ (e.g., the endomorphism $\langle x, y\rangle \mapsto \langle 0, x + y\rangle$ yields $A \subseteq B$). Since $A \,.\, M/\varrho = 0$, $B \,.\, \langle 0, 1\rangle/\varrho = 0$ and $M/\varrho \in \mathscr{V}$, $I \subseteq A$ and $K \subseteq B$. On the other hand, it is easy to see that $AN = 0$ for every free algebra N from $\mathscr{V}$ (and then for every algebra from $\mathscr{V}$). Thus $A \subseteq I$ and $A = I$. Similarly, $B = K$. Taking 3.1 into account, we see that M/ϱ is a free algebra of rank 1 in $\mu(\nu(\mathscr{V}))$. By 3.2, $\mu(\nu(\mathscr{V})) \subseteq \mathscr{V}$. ∎

3.5. Proposition. *Every variety of pointed R-modules has the strong amalgamation property.*

Proof. Let $B = B(+, rx, h)$, $C = C(+, rx, k)$ and $A = A(+, rx, t)$ be three pointed R-modules and let $\varphi : A \to B$, $\psi : A \to C$ be monomorphisms. Put $D = B \times C/E$ where $E = \{\langle \varphi(a), -\psi(a)\rangle; a \in A\}$. The mapping ξ defined by $\xi(b) =$

$= \langle b, 0\rangle + E$ is a monomorphism of the pointed R-module B into the pointed R-module $D(+, rx, \langle h, 0\rangle + E)$. Similarly, $\eta : C \to D$ is a monomorphism, where $\eta(c) = \langle 0, c\rangle + E$. Clearly, $\xi\varphi = \eta\psi$ (use the equality $\langle h, 0\rangle + E = \langle \varphi(t), 0\rangle + + E = \langle 0, \psi(t)\rangle + E = \langle 0, k\rangle + E$). Finally, $\xi(B) \cap \eta(C) = \xi\, \varphi(A)$. The rest is clear. ■

4. RINGS WITH *i*-GENERATORS

Let a ring R and two elements $\alpha, \beta \in R$ be given. We shall say that α, β are *i*-generators of R if they are invertible and R is generated as a ring by $\alpha, \beta, \alpha^{-1}, \beta^{-1}$.

Given a group G, the group-ring ZG consists of formal sums $c_1x_1 + \ldots + c_nx_n$ such that $n \geqq 0$, x_i are pairwise distinct elements from G and c_i are non-zero integers. If the group G is generated by two elements α, β, then α, β are at the same time *i*-generators of the ring ZG. In what follows we fix the following symbols:

G_2 for the free group with two free generators g_1, g_2;
A_2 for the free abelian group with two free generators a_1, a_2;
A_1 for the free abelian group with one free generator a_1.

4.1. Lemma. *Let α, β be i-generators of a ring R. Then there exists a unique ring homomorphism $\varkappa$ of ZG_2 onto R such that $\varkappa(g_1) = \alpha$ and $\varkappa(g_2) = \beta$.*

Proof. Obvious. ■

4.2. Lemma. *The lattice $\mathscr{I}(ZG_2)$ is not countable.*

Proof. Let H be a normal subgroup of G_2 and I the ideal of ZG_2 generated by all $1 - h$, $h \in H$. As is easy to see, we obtain a one-to-one mapping of the set of all normal subgroups of G_2 into $\mathscr{I}(ZG_2)$. The rest follows from the well known fact that there exists an uncountable set of pairwise non-isomorphic groups with two generators. ■

4.3. Lemma. *The ring ZA_2 is noetherian. Hence every commutative ring R with i-generators α, β is noetherian.*

Proof. The ring ZA_2 is a homomorphic image of the polynomial ring $Z[x, y, u, v]$ in four indeterminates over Z. However, the last ring is noetherian by the well known Hilbert "basis" theorem. ■

4.4. Lemma. *Let $R = ZA_1$ and $I = R(a_1 - 1)$. Then the ring R/I is isomorphic to Z and the ring R/I^2 is not a principal ideal ring. In particular, R is not a dedekind domain.*

Proof. The isomorphism $Z \simeq R/I$ is clear. Hence I is a non-zero prime ideal of R which is not maximal. Therefore R cannot be a dedekind domain. Further, let R/I^2 be a principal ideal ring. Then R/I^2 is a direct sum of principal ideal domains and local artinian rings. On the other hand, $(I/I^2)^2 = 0$ and it is easy to see that R/I^2 contains no non-trivial idempotent. Finally, $I \neq I^2$ and R/I^2 is neither artinian nor a principal ideal domain, a contradiction. ∎

4.5. Lemma. *The lattices $\mathscr{I}(ZG_2)$, $\mathscr{I}(ZA_2)$ and $\mathscr{I}(ZA_1)$ are not distributive.*

Proof. Apply 2.6 and 4.4. ∎

Let W denote the set of all formal expressions which can be obtained by a finite number of the following rules:

(i) $0 \in W$; $1 \in W$;
(ii) if $t, w \in W$, then the inscriptions $t + w$, $-t$, αt, βt, $\alpha^{-1}t$, $\beta^{-1}t$ belong to W, too.

For every $t \in W$ define a quasigroup term $\tau(t)$ as follows:

$$\tau(1) = x\,; \qquad \tau(\alpha t) = \tau(t)(y \setminus y)\,;$$
$$\tau(0) = y\,; \qquad \tau(\beta t) = (y / y)\,\tau(t)\,;$$
$$\tau(t + w) = (\tau(t) / y)\,((y / y) \setminus \tau(w))\,; \qquad \tau(\alpha^{-1}t) = \tau(t) / (y \setminus y)\,;$$
$$\tau(-t) = (y / y)\,((\tau(t) / y) \setminus y)\,; \qquad \tau(\beta^{-1}t) = (y / y) \setminus \tau(t)\,.$$

Let us note that the term $\tau(t)$ contains at most two variables, namely x and y. The term obtained from $\tau(t)$ by substituting yy for x will be denoted by $\vartheta(t)$. Clearly, $\vartheta(t)$ contains only one variable, namely y.

Given a ring R with i-generators α, β, every element of W can be considered an element of R. Conversely, every element of R can be expressed many times as an element of W. For every $r \in R$ fix arbitrarily one such $t_r \in W$ and put $\tau(r) = \tau(t_r)$ and $\vartheta(r) = \vartheta(t_r)$.

5. (R, α, β)-QUASIGROUPS

Let a ring R with i-generators α, β be given. A quasigroup $Q(\cdot, /, \setminus)$ is called an (R, α, β)-quasigroup if there exists a pointed R-module $Q(+, rx, h)$ with $ab = \alpha a + \beta b + h$ for all $a, b \in Q$. In this case $a / b = \alpha^{-1}(a - \beta b - h)$ and $a \setminus b = \beta^{-1}(b - \alpha a - h)$ for all $a, b \in Q$. The pointed R-module $Q(+, rx, h)$ will be called an arithmetical pointed R-module of $Q(\cdot, /, \setminus)$. The class of all (R, α, β)-quasigroups will be denoted by $\mathscr{P}(R, \alpha, \beta)$.

Let $M = M(+, rx, h)$ be a pointed R-module. Then we define a pointed (R, α, β)-quasigroup $\varepsilon(M) = Q(\cdot, /, \setminus, u)$ in this way:

$$Q = M\,,$$
$$ab = \alpha a + \beta b + h\,, \quad a / b = \alpha^{-1}(a - \beta b - h)\,, \quad a \setminus b = \beta^{-1}(b - \alpha a - h)\,,$$
$$u = 0\,.$$

Further we put $\omega(M) = Q(\cdot, /, \setminus)$.

5.1. Lemma. *Let $Q(+, rx, h)$ be a pointed R-module and $\varepsilon(Q) = Q(\cdot, /, \backslash, u)$. Then*

$$a + b = (a / u)((u / u) \backslash b),$$

$$\alpha a = a(u \backslash u), \quad \beta a = (u / u) a,$$

$$\alpha^{-1} a = a / (u \backslash u), \quad \beta^{-1} a = (u / u) \backslash a,$$

$$h = uu.$$

If $r \in R$ and $a \in Q$, then ra is the element of Q which is obtained from $\tau(r)$ if x is replaced by a and y by u.

Proof. Easy. ∎

5.2. Lemma. *Let $Q = Q(+, rx, h)$ and $P = P(+, rx, k)$ be two pointed R-modules. A mapping of Q into P is a homomorphism of these pointed R-modules iff it is a homomorphism of the pointed (R, α, β)-quasigroups $\varepsilon(Q)$ and $\varepsilon(P)$.*

Proof. Apply 5.1. ∎

5.3. Lemma. *Two arithmetical pointed R-modules of an (R, α, β)-quasigroup are equal iff their additive groups have the same zero elements.*

Proof. Apply 5.1 with $u = 0$. ∎

Let $M = M(+, rx, h)$ be a pointed R-module and $u \in M$. We shall define new operations on M by

$$a \oplus b = a + b - u, \quad r * a = ra + u - ru, \quad k = \alpha u + \beta u + h.$$

It is easy to see that $M_u = M(\oplus, r * x, k)$ is a pointed R-module and u is its zero element. Moreover, $\omega(M_u) = \omega(M)$. In particular, we have proved the following lemma.

5.4. Lemma. *For every pointed (R, α, β)-quasigroup $Q(\cdot, /, \backslash, u)$ there exists a uniquely determined pointed R-module $Q(+, rx, h)$ such that $Q(\cdot, /, \backslash, u) = \varepsilon(Q(+, rx, h))$.* ∎

5.5. Proposition. *The class $\mathscr{P}(R, \alpha, \beta)$ is a variety and ε is an equivalence between $R\mathscr{M}^*$ and $\mathscr{P}(R, \alpha, \beta)^*$.*

Proof. By 5.3 and 5.4, ε is a biunique mapping. The rest follows from 5.2, 1.3 and 1.4. ∎

5.6. Lemma. *Let $Q(+, rx, h)$ and $Q(\oplus, r * x, k)$ be two arithmetical pointed R-modules of an (R, α, β)-quasigroup. Then the modules $Q(+, rx)$ and $Q(\oplus, r * x)$ are isomorphic.*

Proof. Easy. ∎

6. VARIETIES OF (R, α, β)-QUASIGROUPS

Similarly as in Section 5, let R be a ring with i-generators α, β. Further put $\gamma = \alpha + \beta - 1$.

6.1. Proposition. *Let $\langle I, K\rangle \in \mathscr{K}(R)$ and $\mathscr{V} = \varepsilon(\mu(\langle I, K\rangle))$. Then*

(i) *$\mathscr{V}$ is a variety of pointed (R, α, β)-quasigroups.*
(ii) *$\mathscr{V}$ is reducible iff $K \subseteq (I : \gamma)$.*

Proof. (i) is evident. (ii) First, let $\mathscr{V}$ be reducible and $M = R/I \times R/K$. Then $M = M(+, rx, \langle 0, 1 + K\rangle)$ is a pointed R-module from $\mu(\langle I, K\rangle)$. Put $\omega(M) = M(\cdot, /, \backslash)$ and take $u \in M$ arbitrarily. According to the hypothesis, the pointed (R, α, β)-quasigroup $M(\cdot, /, \backslash, u)$ belongs to $\mathscr{V}$. Then $\varepsilon^{-1}(M(\cdot, /, \backslash, u)) = M(\oplus, r * x, k)$ is contained in $\mu(\langle I, K\rangle)$ and $s * k = u$ for all $s \in K$. By Section 5, $k = \alpha u + \beta u + \langle 0, 1 + K\rangle$ and $s * k = s\alpha u + s\beta u + \langle 0, s + K\rangle + u - su = u$. Hence $s\gamma u = 0$ and we have proved $K\gamma M = 0$. Thus $K\gamma \subseteq (0 : M) = I$. The converse assertion can be proved similarly. ∎

We denote by $\mathscr{S}(R, \alpha, \beta)$ the subset of $\mathscr{K}(R)$ consisting of all pairs $\langle I, K\rangle$ such that $K \subseteq (I : \gamma)$. Clearly, $\mathscr{S}(R, \alpha, \beta)$ is a sublattice of $\mathscr{K}(R)$.

6.2. Corollary. *The lattice $\mathscr{S}(R, \alpha, \beta)$ is isomorphic to the lattice $\mathscr{L}(\mathscr{P}(R, \alpha, \beta))$. The isomorphism is given by $\langle I, K\rangle \mapsto \mathscr{V}$, where $\mathscr{V}^* = \varepsilon(\mu(\langle I, K\rangle))$.*

Proof. Apply 3.4, 6.1 and 1.2. ∎

6.3. Proposition. *Let $\langle I, K\rangle \in \mathscr{S}(R, \alpha, \beta)$ and let $\mathscr{V}$ be the corresponding variety of (R, α, β)-quasigroups. Let $X \subseteq I$ and $Y \subseteq K$ be subsets such that I is the ideal generated by X and K is the left ideal generated by $I \cup Y$. Then $\mathscr{V}$ is just the class of all (R, α, β)-quasigroups satisfying the identities $\tau(r) = y$, $r \in X$ and $\vartheta(s) = y$, $s \in Y$.*

Proof. We have $\mathscr{V}^* = \varepsilon(\mu(\langle I, K\rangle))$. Clearly, $\mu(\langle I, K\rangle)$ is just the variety of pointed R-modules $M(+, rx, h)$ satisfying $IM = 0$ and $Kh = 0$. However, these equalities are equivalent to $XM = 0$ and $Yh = 0$. Further, $Q(\cdot, /, \backslash) \in \mathscr{V}$ iff $Q(\cdot, /, \backslash, u) \in \mathscr{V}^*$ for all $u \in Q$, i.e., iff for every $u \in Q$ the pointed R-module $Q_u = Q(+, rx, uu) = \varepsilon^{-1}(Q(\cdot, /, \backslash, u)$ satisfies $u = XQ_u$ and $u = Y . uu$. It follows from 5.1 that this is equivalent to the validity of the identities $\tau(r) = y$, $r \in X$ and $\vartheta(s) = y$, $s \in Y$. ∎

6.4. Corollary. *Every variety $\mathscr{V}$ of (R, α, β)-quasigroups is determined in $\mathscr{P}(R, \alpha, \beta)$ by identities containing no more than two variables. In particular, $\mathscr{V}$ is generated by its free quasigroup of rank 2.* ∎

6.5. Corollary. *Let R be left noetherian. Then the lattice $\mathscr{L}(\mathscr{P}(R, \alpha, \beta))$ is countable and every variety of (R, α, β)-quasigroups is determined in $\mathscr{P}(R, \alpha, \beta)$ by a finite number of identities in at most two variables.* ∎

6.6. Proposition. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element from $\mathscr{S}(R, \alpha, \beta)$. Then I is just the set of all $r \in R$ such that $\tau(r) = y$ holds in $\mathscr{V}$ and K is the set of all $s \in R$ such that $\vartheta(s) = y$ holds in $\mathscr{V}$.*

Proof. Easy. ∎

6.7. Example. Let $\mathscr{V}$ be the variety of all (R, α, β)-quasigroups satisfying $x(x / y) = yx \,.\, x$ and let $\langle I, K\rangle$ be the corresponding element from $\mathscr{S}(R, \alpha, \beta)$. Clearly, an (R, α, β)-quasigroup $Q(\cdot, /, \backslash)$ with an arithmetical pointed R-module $Q(+, rx, h)$ satisfies this identity iff

$$\alpha a + \beta\alpha^{-1}a - \beta\alpha^{-1}\beta b - \beta\alpha^{-1}h + h = \alpha^2 b + \alpha\beta a + \alpha h + \alpha a + h$$

for all $a, b \in Q$. Now we can easily see that

$$I = R(\alpha + \beta\alpha^{-1} - \alpha\beta - \beta)\, R + R(\alpha^2 + \beta\alpha^{-1}\beta)\, R$$

and

$$K = R(\alpha + \beta\alpha^{-1}) + I\,.$$

6.8. Lemma. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element from $\mathscr{S}(R, \alpha, \beta)$. Then $\mathscr{V}$ is just the variety of $(R/I, \alpha + I$ $\beta + I)$-quasigroups corresponding to $\langle 0, K/I\rangle$.*

Proof. Easy. ∎

6.9. Lemma. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element from $\mathscr{S}(R, \alpha, \beta)$. Then $I = \bigcap(0 : M)$ and $K = \bigcap(0 : h)$ where $M = M(+, rx, h)$ is such that $\varepsilon(M) \in \mathscr{V}^*$ (i.e. $\omega(M) \in \mathscr{V}$).*

Proof. Obvious. ∎

6.10. Lemma. *The lattice $\mathscr{I}(R)$ is antiisomorphic to a sublattice of $\mathscr{L}(\mathscr{P}(R, \alpha, \beta))$*

Proof. Obvious. ∎

Let R be a ring with i-generators α, β and $\gamma = \alpha + \beta - 1$.

7.1. Proposition. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element of $\mathscr{S}(R, \alpha, \beta)$. Let F be a free R/I-module with a free basis X. Define $M \in R\mathscr{M}^*$ by $M = (F \times R/K)(+, rx, \langle 0, 1 + K\rangle)$. Then $\omega(M)$ is a free quasigroup in $\mathscr{V}$ and the set $\{\langle x, 0\rangle; x \in X \cup \{0\}\}$ is its free basis.*

Proof. By 3.1 the pointed R-module M is free in the variety $\mu(\langle I, K\rangle)$ and $\{\langle x, 0\rangle; x \in X\}$ is its free basis. Now it is enough to apply 1.5 and 1.3. ∎

7.2. Lemma. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element from $\mathscr{S}(R, \alpha, \beta)$. Suppose that $I \subseteq L \subseteq K$ for an ideal L and denote by $\mathscr{W}$ the variety corresponding to $\langle L, K\rangle$. Then $\mathscr{W} \subseteq \mathscr{V}$ and these varieties have the same quasigroups of rank 1.*

Proof. Apply 7.1. ∎

7.3. Lemma. *Let t be an arbitrary and s an invertible element of R. Then the (R, α, β)-quasigroup $\omega(R(+, rx, \gamma t + s))$ is free of rank 1 in the variety $\mathscr{P}(R, \alpha, \beta)$.*

Proof. Define $\varphi : R \to R$ by $\varphi(x) = xs - t$. Then φ is a biunique mapping and

$$\varphi(\alpha x + \beta y + 1) = \alpha xs + \beta ys + s - t = \alpha xs - \alpha t + \beta ys - \beta t + \gamma t + s =$$
$$= \alpha\, \varphi(x) + \beta\, \varphi(y) + \gamma t + s\,.$$

The rest is clear. ∎

7.4. Lemma. *Let R be commutative and suppose that every subquasigroup of the free (R, α, β)-quasigroup of rank 1 is free. Let t be an arbitrary and s an invertible element of R. Then every non-zero ideal containing $\gamma t + s$ is principal and isomorphic to R as a module.*

Proof. Let I be a non-zero ideal containing $\gamma t + s$. As one may check easily, I is a subquasigroup of the quasigroup $Q = \omega(R(+, rx, \gamma t + s))$. By 7.3, Q is free of rank 1 in $\mathscr{P}(R, \alpha, \beta)$, and hence the quasigroup I is free. Now it follows by 1.3, 1.5 and 5.6 that I is a free R-module. By 2.1 and 4.3, I is isomorphic to R. ∎

7.5. Proposition. *Let R be commutative, let $\mathscr{V}$ be a Schreier variety of (R, α, β)-quasigroups and $\langle I, K\rangle$ the corresponding element of $\mathscr{S}(R, \alpha, \beta)$. Then R/I is a principal ideal domain and either $K = I$ or $\gamma \in I$.*

Proof. According to 6.8, we can assume $I = 0$. First let $K \neq 0$ and let A be an ideal of R. Clearly, $(A \times R/K)(+, rx, \langle 0, 1 + K\rangle)$ is a subalgebra of $(R \times R/K)$ $(+, rx, \langle 0, 1 + K\rangle)$. Now, taking into account 7.1 and the fact that $\mathscr{V}$ is a Schreier variety, we see that $A \times R/K$ is isomorphic to $F \times R/K$ for a free module F. Put $M = (0 : K) \times R/K$. Then $KM = 0$, so that $M \simeq R/K$. However, R/K is noetherian, $(0 : K)$ is an R/K-module, and consequently either $0 = (0 : K)$ or $K = R$. In both cases we have $0 = (0 : K)$ and R is a principal ideal domain by 2.3 and 2.1.

Further, let $K = 0$. Similarly as above, we can show that the assumptions of 2.2 are satisfied, and so R/I is a principal ideal domain. ∎

7.6. Proposition. *Let R be commutative, let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups such that every quasigroup from $\mathscr{V}$ contains an idempotent and let $\langle I, K\rangle$ be the corresponding element of $\mathscr{S}(R, \alpha, \beta)$. Then $\mathscr{V}$ is a Schreier variety iff R/I is a principal ideal and either $I = K$ or $K = R$.*

Proof. The proof is left to the reader as an easy exercise. ∎

7.7. Proposition. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element of $\mathscr{S}(R, \alpha, \beta)$. Then every quasigroup from $\mathscr{V}$ contains an idempotent iff $\gamma s - 1 \in K$ for some $s \in R$.*

Proof. Easy. ∎

8. FURTHER PROPERTIES OF (R, α, β)-QUASIGROUPS

As before, R is a ring with i-generators α, β and $\gamma = \alpha + \beta - 1$.

8.1. Proposition. *Every variety of (R, α, β)-quasigroups has the strong amalgamation property.*

Proof. It is easy to see that a variety $\mathscr{V}$ has the strong amalgamation property iff $\mathscr{V}^*$ has the strong amalgamation property and that the strong amalgamation property is preserved by the equivalence of varieties. Now it remains to apply 3.5. ∎

8.2. Proposition. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element of $\mathscr{S}(R, \alpha, \beta)$. Then $\mathscr{V}$ is extensive iff $K = (I : \gamma)$.*

Proof. With respect to 6.8, we can assume that $I = 0$. First let $\mathscr{V}$ be extensive. Let $Q(\cdot, /, \backslash) \in \mathscr{V}$, $u \in Q$ be arbitrary and $Q(+, rx, h) = \varepsilon^{-1}(Q(\cdot, /, \backslash, u))$. There exists an extension $P(\cdot, /, \backslash)$ of $Q(\cdot, /, \backslash)$ belonging to $\mathscr{V}$ and an element $e \in P$ with $ee = e$. Since ε is an equivalence, the pointed R-module $P(+, rx, h) = \varepsilon^{-1}(P(\cdot, /, \backslash, u))$ is an extension of $Q(+, rx, h)$. We have $e = ee = \alpha e + \beta e + h$, so that $h = \gamma(-e)$. Consequently, $(0 : \gamma)\, h = (0 : \gamma)\, \gamma(-e) = 0$. By 6.9, $K = (0 : \gamma)$.

Conversely, let $K = (0 : \gamma)$. Let $Q(\cdot, /, \backslash) \in \mathscr{V}$ and let u be an arbitrary element of Q. Put $Q(+, rx, h) = \varepsilon^{-1}(Q(\cdot, /, \backslash, u))$ and denote by $H(+, rx)$ the injective hull of $Q(+, rx)$. Evidently $H(+, rx, h) \in \mu(\langle 0, (0 : \gamma)\rangle)$, so that the pointed quasigroup $H(\cdot, /, \backslash, u) = \varepsilon(H(+, rx, h))$ belongs to $\mathscr{V}^*$ and the quasigroup $H(\cdot, /, \backslash)$ belongs to $\mathscr{V}$. Moreover, $H(\cdot, /, \backslash)$ is an extension of $Q(\cdot, /, \backslash)$. Define a mapping φ of $R\gamma$ into H by $\varphi(r\gamma) = rh$. It is easy to verify that φ is a homomorphism of the R-module $R\gamma$ into $H(+, rx)$. Since $R\gamma$ is a submodule of R and H is injective, φ can be extended to a module homomorphism $\psi : R \to H$. Put $e = \psi(1)$. We have

$$\gamma e = \gamma\, \psi(1) = \psi(\gamma 1) = \psi(\gamma) = \varphi(\gamma) = \varphi(1\gamma) = 1h = h\,.$$

Hence in $H(\cdot, /, \backslash)$ we can write

$$(-e)(-e) = -\alpha e - \beta e + h = -\gamma e - e + h = -e\,.$$

Thus $-e$ is an idempotent element of $H(\cdot, /, \backslash)$. ■

8.3. Corollary. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element of $\mathscr{S}(R, \alpha, \beta)$. Suppose that $\gamma \notin I$ and that R/I is a ring without zero divisors. Then $K = I$ and $\mathscr{V}$ is extensive.* ■

8.4. Lemma. *Let $Q(\cdot, /, \backslash)$ be an (R, α, β)-quasigroup. Let $u \in Q$ be an arbitrary element and put $Q(+, rx, h) = \varepsilon^{-1}(Q(\cdot, /, \backslash, u))$. The quasigroup $Q(\cdot, /, \backslash)$ is subdirectly irreducible iff the module $Q(+, rx)$ is cocyclic. $Q(\cdot, /, \backslash)$ is simple iff $Q(+, rx)$ is simple.*

Proof. Clearly, $Q(\cdot, /, \backslash)$ and $Q(\cdot, /, \backslash, u)$ have the same congruences. Similarly, $Q(+, rx, h)$ and $Q(+, rx)$ have the same congruences. Finally, $Q(\cdot, /, \backslash, u)$ and $Q(+, rx, h)$ have the same congruences because of the equivalence ε. Now we can use 2.4. ■

A variety is called residually small if the class $\mathscr{K}$ of all its subdirectly irreducible members contains a representative subset, i.e. a subset M such that every $A \in \mathscr{K}$ s isomorphic to some $B \in M$.

8.5. Corollary. *The variety of all (R, α, β)-quasigroups is residually small.* ■

8.6. Proposition. *Let $\mathscr{V}$ be a variety of (R, α, β)-quasigroups and let $\langle I, K\rangle$ be the corresponding element of $\mathscr{S}(R, \alpha, \beta)$. Let $Q(\cdot, /, \backslash) \in \mathscr{V}$, $u \in Q$ and $Q(+, rx, h) = \varepsilon^{-1}(Q(\cdot, /, \backslash, u))$. The quasigroup $Q(\cdot, /, \backslash)$ is injective in $\mathscr{V}$ iff the R/I-module $Q(+, rx)$ is injective.*

Proof. An easy exercise. ■

A quasigroup $Q(\cdot, /, \backslash)$ is called a T-quasigroup (see [13], [10] and [9]) if there exist an abelian group $Q(+)$, two automorphisms α, β of $Q(+)$ and an element $h \in Q$ such that $ab = \alpha a + \beta b + h$ for all $a, b \in Q$. Denote by $R(Q)$ the subring generated by $\alpha, \beta, \alpha^{-1}, \beta^{-1}$ in the endomorphism ring of $Q(+)$. It is not difficult to see that $R(Q)$ is a ring with i-generators α, β and Q is an $(R(Q), \alpha, \beta)$-quasigroup. Moreover, the ring $R(Q)$ is determined uniquely up to ring isomorphism.

The class of all T-quasigroups will be denoted by $\mathscr{T}$.

9.1. Proposition. *The following conditions are equivalent for any quasigroup Q:*

(i) *Q is a T-quasigroup.*
(ii) *Q is an (R, α, β)-quasigroup for a ring R with i-generators α, β.*
(iii) *Q is a (ZG_2, g_1, g_2)-quasigroup.*

Proof. Easy. ∎

9.2. Theorem. *The lattice $\mathscr{L}(\mathscr{T})$ is isomorphic to $\mathscr{S}(ZG_2, g_1, g_2)$. Further, $\mathscr{L}(\mathscr{T})$ is modular, uncountable and not distributive.*

Proof. Apply 9.1, 6.2, 6.10, 4.2 and 4.5. ∎

9.3. Theorem. (i) *Every variety of T-quasigroups has the strong amalgamation property.*

(ii) *Every variety of T-quasigroups is residually small.*
(iii) *Every variety of T-quasigroups is determined in $\mathscr{T}$ by a set of identities in at most two variables.*
(iv) *The variety $\mathscr{T}$ is extensive.*

Proof. Apply 8.1, 8.3, 8.5 and 6.4. ∎

9.4. Proposition. *Let $\mathscr{V}$ be a variety of T-quasigroups. Then $\mathscr{V}$ contains a subvariety $\mathscr{W}$ such that:*

(i) *$\mathscr{W}$ is the largest extensive subvariety contained in $\mathscr{V}$.*
(ii) *Every quasigroup from $\mathscr{V}$ is isotopic to a quasigroup from $\mathscr{W}$ having an idempotent.*
(iii) *Every quasigroup from $\mathscr{V}$ possessing an idempotent belongs to $\mathscr{W}$.*

Proof. Easy (use 8.2). ∎

9.5. Corollary. *Every minimal variety of T-quasigroups is extensive.* ∎

We do not know the answers to the following two problems.

9.6. Problem. Find the number of minimal varieties of T-quasigroups.

9.7. Problem. It can be shown that the variety of quasigroups satisfying the identity $xy \,.\, uv = vy \,.\, ux$ is contained in the variety of T-quasigroups. Find the number of subvarieties of this variety.

10. ABELIAN QUASIGROUPS

A quasigroup $Q(\cdot, /, \backslash)$ is called abelian if it satisfies the identity $xy \,.\, uv = xu \,.\, yv$. The variety of abelian quasigroups will be denoted by $\mathscr{A}$ and the variety of commutative abelian quasigroups by $\mathscr{B}$.

10.1. Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) *Q is abelian.*
(ii) *Q is an (R, α, β)-quasigroup for a commutative ring R with i-generators α, β.*
(iii) *Q is a (ZA_2, a_1, a_2)-quasigroup.*

Proof. By the well known Toyoda's theorem (see [1]), every abelian quasigroup is a T-quasigroup. The rest is easy. ■

10.2. Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) *Q is commutative and abelian.*
(ii) *Q is a commutative T-quasigroup.*
(iii) *Q satisfies the identity $xy \,.\, uv = xu \,.\, vy$.*
(iv) *Q is an (R, α, α)-quasigroup for a ring R with an i-generator α.*
(v) *Q is a (ZA_1, a_1, a_1)-quasigroup.*

Proof. Easy. ■

10.3. Theorem. (i) *The lattice $\mathscr{L}(\mathscr{A})$ is isomorphic to $\mathscr{S}(ZA_2, a_1, a_2)$ and $\mathscr{L}(\mathscr{B})$ is isomorphic to $\mathscr{S}(ZA_1, a_1, a_1)$.*

(ii) *The lattices $\mathscr{L}(A)$ and $\mathscr{L}(\mathscr{B})$ are infinite, countable and modular.*
(iii) *The lattices $\mathscr{L}(\mathscr{A})$ and $\mathscr{L}(\mathscr{B})$ are not distributive.*

Proof. Apply 10.1, 10.2, 6.10, 6.2, 6.5 and 4.5. ■

10.4. Theorem. (i) *Every variety of abelian quasigroups has the strong amalgamation property and is residually small.*

(ii) *Every variety of abelian quasigroups is determined as a variety of algebras with three binary operations by the identity $xy \,.\, uv = xu \,.\, yv$ together with a finite set of identities containing at most two variables.*
(iii) *Every descending chain of varieties of abelian quasigroups is finite.*
(iv) *Free quasigroups from $\mathscr{A}$ (from $\mathscr{B}$) of rank 1 contain subquasigroups which are not free.*
(v) *The varieties $\mathscr{A}$ and $\mathscr{B}$ are extensive.*

Proof. (i), (ii) and (iii) follow from 8.1, 8.5, 6.5 and 4.3. (iv) Suppose, on the contrary, that every subquasigroup of a free quasigroup from $\mathscr{B}$ of rank 1 is free. Put $R = ZA_1$ and $I = R(a_1 - 1)^2$. We have $(a_1 - 1)^2 = -(2a_1 - 1) + a_1^2$ and R/I is a principal ideal ring by 7.4, a contradiction with 4.4. Similarly for $\mathscr{A}$. (v) follows from 8.3. ■

In spite of the countability of $\mathscr{L}(\mathscr{B})$ the problem of describing this lattice completely seems to be difficult. The situation is analogous to that of varieties of commutative semigroups. There are only countably many varieties of commutative semigroups but again the lattice has not yet been described.

Let us call a lattice completely describable if it is either finite or isomorphic to a countable lattice in which both lattice operations are recursive. We do not know the answers to the following two problems.

10.5. Problem. Determine whether the lattices $\mathscr{L}(\mathscr{A})$ and $\mathscr{L}(\mathscr{B})$ are completely describable.

10.6. Problem. Characterize Schreier varieties of abelian quasigroups.

11. SIMPLE ABELIAN QUASIGROUPS

For every prime power p^n we denote by $\mathrm{GF}(p^n)$ the finite field with p^n elements. By an admissible triple of elements of $\mathrm{GF}(p^n)$ we shall mean a triple α, β, g such that α, β are i-generators of $\mathrm{GF}(p^n)$ and the following implications hold: if $\alpha + \beta \neq 1$, then $g = 0$; if $\alpha + \beta = 1$, then $g \in \{0, 1\}$. Let us remark that since $\mathrm{GF}(p^n)$ is a finite field, elements α, β are i-generators iff they are non-zero elements generating $\mathrm{GF}(p^n)$ as a field.

Let α, β, g be an admissible triple of elements of $\mathrm{GF}(p^n)$. Then we define an abelian guasigroup $H(p^n, \alpha, \beta, g)$ as follows: its underlying set is the set $\mathrm{GF}(p^n)$; the binary operation (which will be denoted by $\circ$) is defined by $a \circ b = \alpha a + \beta b + g$.

11.1. Theorem. *Let p^n be a prime power and let α, β, g be an admissible triple of elements of* $\mathrm{GF}(p^n)$. *Then*:

(i) *Th abelian quasigroup $H = H(p^n, \alpha, \beta, g)$ is finite and simple.*
(ii) *The quasigroup H is simple as a groupoid.*
(iii) *H contains an idempotent iff $g = 0$.*
(iv) *H contains no other subgroupoids than the idempotents and H.*

Proof. As is easy to see, H is a $(\mathrm{GF}(p^n), \alpha, \beta)$-quasigroup. However, the $\mathrm{GF}(p^n)$-module $\mathrm{GF}(p^n)$ is simple and we can use 8.4. The rest is clear. ■

11.2. Theorem. *Let p^n and q^m be two prime powers and let α, β, g and γ, δ, h be two admissible triples of elements of* $\mathrm{GF}(p^n)$ *and* $\mathrm{GF}(q^m)$, *respectively. Then the quasigroups* $\mathrm{H}(p^n, \alpha, \beta, g)$ *and $H(q^m, \gamma, \delta, h)$ are isomorphic iff $p = q$, $n = m$, $g = h$ and $\lambda(\alpha) = \gamma$ and $\lambda(\beta) = \delta$ for an automorphism λ of the field* $\mathrm{GF}(p^n)$.

Proof. The converse implication is evident. Suppose that the quasigroups $H(p^n, \alpha, \beta, g)$ and $H(q^m, \gamma, \delta, h)$ are isomorphic. Then clearly $p = q$, $n = m$ and there exists a permutation φ of $\mathrm{GF}(p^n)$ such that $\varphi(\alpha x + \beta y + g) = \gamma\,\varphi(x) + \delta\varphi(y) + h$ for all $x, y \in \mathrm{GF}(p^n)$.

Suppose $g = 0$ and $h = 1$. Then $\gamma + \delta = 1$ and thus the substitution $x = y = 0$ gives $\varphi(0) = (\gamma + \delta)\,\varphi(0) + 1 = \varphi(0) + 1$, a contradiction. Similarly, if $g = 1$ and $h = 0$ we get a contradiction. Thus $g = h$.

Let $\alpha + \beta \neq 1$. Then $g = h = 0$ and $H(p^n, \alpha, \beta, 0)$ is not idempotent. Consequently, $H(p^n, \gamma, \delta, 0)$ is not idempotent either and thus $\gamma + \delta \neq 1$. We have

$$\begin{aligned}
&\varphi(\alpha x + \beta y) = \gamma\,\varphi(x) + \delta\,\varphi(y)\,,\\
&\varphi(0) = (\gamma + \delta)\,\varphi(0)\,, \quad \varphi(0) = 0\,,\\
&\varphi(\alpha x) = \gamma\,\varphi(x)\,, \quad \varphi(\beta x) = \delta\,\varphi(x)\,,\\
&\varphi(x + y) = \varphi(\alpha\alpha^{-1}x + \beta\beta^{-1}y) = \gamma\,\varphi(\alpha^{-1}x) + \delta\,\varphi(\beta^{-1}y) =\\
&\qquad = \varphi(\alpha\alpha^{-1}x) + \varphi(\beta\beta^{-1}y) = \varphi(x) + \varphi(y)\,.
\end{aligned}$$

Put $\lambda(x) = \varphi(x)\,.\,(\varphi(1))^{-1}$. Then

$$\begin{aligned}
&\lambda(x + y) = \lambda(x) + \lambda(y)\,,\\
&\lambda(\alpha) = \gamma\,, \quad \lambda(\beta) = \delta\,, \quad \lambda(1) = 1\,,\\
&\lambda(\alpha x) = \varphi(\alpha x)\,.\,(\varphi(1))^{-1} = \gamma\,\varphi(x)\,(\varphi(1))^{-1} = \lambda(\alpha)\,\lambda(x)\,,\\
&\lambda(\beta x) = \lambda(\beta)\,\lambda(x)\,.
\end{aligned}$$

The set of all $r \in \mathrm{GF}(p^n)$ such that $\lambda(rx) = \lambda(r)\,\lambda(x)$ for all $x \in \mathrm{GF}(p^n)$ is evidently a subring containing the generators α, β. This implies that λ is an automorphism of $\mathrm{GF}(p^n)$.

Now let $\alpha + \beta = 1$, so that $\gamma + \delta = 1$, too. Put $\psi(x) = \varphi(x) - \varphi(0)$. We have

$$\begin{aligned}
&\psi(\alpha x + \beta y + g) = \varphi(\alpha x + \beta y + g) - \varphi(0) = \gamma\,\varphi(x) + \delta\,\varphi(y) + h - \varphi(0) =\\
&\qquad = \gamma\,\varphi(x) + \delta\,\varphi(y) + h - (\gamma + \delta)\,\varphi(0) = \gamma\,\psi(x) + \delta\,\psi(y) + h\,,\\
&\psi(0) = 0\,,\\
&\psi(x + g) = \psi(\alpha x + \beta x + g) = \gamma\,\psi(x) + \delta\,\psi(x) + h = \psi(x) + h\,,\\
&\psi(\alpha x + \beta y) + h = \psi(\alpha x + \beta y + g) = \gamma\,\psi(x) + \delta\,\psi(y) + h\,,\\
&\psi(\alpha x + \beta y) = \gamma\,\psi(x) + \delta\,\psi(y)\,,\\
&\psi(\alpha x) = \gamma\,\psi(x)\,,\\
&\psi(\beta x) = \delta\,\psi(x)\,,\\
&\psi(x + y) = \psi(\alpha\alpha^{-1}x + \beta\beta^{-1}y) = \gamma\,\psi(\alpha^{-1}x) + \delta\,\psi(\beta^{-1}y) =\\
&\qquad = \psi(\alpha\alpha^{-1}x) + \psi(\beta\beta^{-1}y) = \psi(x) + \psi(y)\,.
\end{aligned}$$

Put $\lambda(x) = \psi(x)(\psi(1))^{-1}$. Similarly as above, λ is an automorphism, $\lambda(\alpha) = \gamma$ and $\lambda(\beta) = \delta$. ∎

11.3. Theorem. *Every non-trivial simple abelian quasigroup is isomorphic to $H(p^n, \alpha, \beta, g)$ for a prime power p^n and an admissible triple α, β, g of elements of* $\mathrm{GF}(p^n)$.

Proof. Let $Q(\circ, /, \backslash)$ be a simple abelian quasigroup. Take $u \in Q$ and consider $Q(+, rx, h) = \varepsilon^{-1}(Q(\circ, /, \backslash, u))$. Then $Q(+, rx)$ is a simple ZA_2-module (by 8.4). Hence $Q(+, rx)$ is isomorphic to ZA_2/I for a maximal ideal I of ZA_2. Let $\varphi : Q(+, rx) \simeq ZA_2/I(+, rx)$ be an isomorphism. Clearly, φ is an isomorphism of $Q(\circ, /, \backslash)$ onto $\omega(ZA_2/I(+, rx, \varphi(h)))$. On the other hand, ZA_2/I is a field generated as a ring by $a_1 + I$, $a_1^{-1} + I$, $a_2 + I$, $a_2^{-1} + I$. By 2.7, $ZA_2/I = \mathrm{GF}(p^n)$ for a prime power p^n. Hence we can assume that $Q = \mathrm{GF}(p^n)$ and $x \circ y = \alpha x + \beta y + h$ for some non-zero elements α, β generating $\mathrm{GF}(p^n)$ and some $h \in \mathrm{GF}(p^n)$. If $\alpha + \beta \neq 1$ then the mapping $x \mapsto x + (\alpha + \beta - 1)^{-1} h$ is an isomorphism of $Q(\circ)$ onto $H(p^n, \alpha, \beta, 0)$. If $\alpha + \beta = 1$ and $h \neq 0$ then the mapping $x \mapsto xh^{-1}$ is an isomorphism of $Q(\circ)$ onto $H(p^n, \alpha, \beta, 1)$. ∎

11.4. Corollary. *Every simple abelian quasigroup is finite and simple as a groupoid.* ∎

12. MINIMAL VARIETIES OF ABELIAN QUASIGROUPS

Let p^n be a prime power and let α, β be two non-zero elements of $\mathrm{GF}(p^n)$ generating $\mathrm{GF}(p^n)$. Then we denote by $\mathscr{H}(p^n, \alpha, \beta)$ the variety of quasigroups generated by $H(p^n, \alpha, \beta, 0)$.

12.1. Theorem. *Let p^n be a prime power and let α, β be two non-zero elements of* $\mathrm{GF}(p^n)$ *such that α, β generate* $\mathrm{GF}(p^n)$ *and $\alpha + \beta \neq 1$. Then*

(i) *$\mathscr{H}(p^n, \alpha, \beta)$ is a minimal variety of abelian quasigroups.*
(ii) *$\mathscr{H}(p^n, \alpha, \beta) = \mathscr{P}(\mathrm{GF}(p^n), \alpha, \beta)$.*
(iii) *$H(p^n, \alpha, \beta, 0)$ is free of rank 1 in $\mathscr{H}(p^n, \alpha, \beta)$.*
(iv) *If $Q \in \mathscr{H}(p^n, \alpha, \beta)$ then $Q = \omega(V(+, rx, 0))$ for a vector space $V(+, rx)$ over* $\mathrm{GF}(p^n)$.
(v) *Every non-trivial quasigroup from $\mathscr{H}(p^n, \alpha, \beta)$ contains an idempotent and is free in $\mathscr{H}(p^n, \alpha, \beta)$.*

Proof. Let $\varkappa : ZA_2 \to \mathrm{GF}(p^n)$ be the ring homomorphism with $\varkappa(a_1) = \alpha$ and $\varkappa(a_2) = \beta$. Put $I = \operatorname{Ker} \varkappa$. Then I is a maximal ideal of ZA_2. Since $\alpha + \beta \neq 1$, $a_1 + a_2 - 1 \notin I$ and $(I : a_1 + a_2 - 1) = I$ (I is a prime ideal). Now it is obvious that $\mathscr{P}(\mathrm{GF}(p^n), \alpha, \beta)$ is just the variety of abelian quasigroups corresponding to $\langle I, I \rangle \in \mathscr{S}(ZA_2, a_1, a_2)$ and that this variety is minimal (iii) follows from 7.1 and 7.2 and the rest is easy. ∎

12.2. Theorem. *Let p^n be a prime power and let α, β be two non-zero elements of* $\mathrm{GF}(p^n)$ *such that α, β generate* $\mathrm{GF}(p^n)$ *and $\alpha + \beta = 1$. Then*

(i) *$\mathscr{H}(p^n, \alpha, \beta)$ is a minimal variety of abelian quasigroups.*

(ii) *$\mathscr{H}(p^n, \alpha, \beta)$ is just the only non-trivial subvariety of $\mathscr{P}(\mathrm{GF}(p^n), \alpha, \beta)$; a quasigroup from $\mathscr{P}(\mathrm{GF}(p^n), \alpha, \beta)$ belongs to $\mathscr{H}(p^n, \alpha, \beta)$ iff it is idempotent.*

(iii) *$H(p^n, \alpha, \beta, 0)$ is free of rank 2 in $\mathscr{H}(p^n, \alpha, \beta)$.*

(iv) *If $Q \in \mathscr{H}(p^n, \alpha, \beta)$ then $Q = \omega(V(+, rx, 0))$ for a vector space $V(+, rx)$ over* $\mathrm{GF}(p^n)$.

(v) *Every quasigroup from $\mathscr{H}(p^n, \alpha, \beta)$ is free in $\mathscr{H}(p^n, \alpha, \beta)$.*

Proof. Let $\varkappa$ and I be as in the proof of 12.1. Then I is a maximal ideal and $a_1 + a_2 - 1 \in I$. It is easy to see that the variety of idempotent quasigroups from $\mathscr{P}(\mathrm{GF}(p^n), \alpha, \beta)$ is just the variety of abelian quasigroups corresponding to $\langle I, ZA_2 \rangle$. The rest is clear. ∎

12.3. Theorem. *Let $\mathscr{V}$ be a minimal variety of abelian quasigroups. Then there exist a prime power p^n and two non-zero elements α, β of* $\mathrm{GF}(p^n)$ *generating* $\mathrm{GF}(p^n)$ *such that $\mathscr{V} = \mathscr{H}(p^n, \alpha, \beta)$. Moreover, $\mathscr{H}(p^n, \alpha, \beta) = \mathscr{H}(q^m, \gamma, \delta)$ iff $p = q$, $n = m$ and $\lambda(\alpha) = \gamma$ and $\lambda(\beta) = \delta$ for an automorphism λ of* $\mathrm{GF}(p^n)$.

Proof. Let $\langle I, K \rangle$ be the element of $\mathscr{S}(ZA_2, a_1, a_2)$ corresponding to $\mathscr{V}$. Then I is a maximal ideal and either $I = K$ or $K = ZA_2$. By 2.7, $ZA_2/I = \mathrm{GF}(p^n)$ for a prime power p^n. Now it is clear that $\mathscr{V} = \mathscr{H}(ZA_2/I, a_1 + I, a_2 + I)$. The rest follows from 12.1, 12.2 and 11.2. ∎

Remark. Let p^n be a prime power, and let α, β be two non-zero elements of $\mathrm{GF}(p^n)$ such that α, β generate $\mathrm{GF}(p^n)$ and $\alpha + \beta = 1$. Put $\mathscr{V} = \mathscr{P}(\mathrm{GF}(p^n), \alpha, \beta)$. The variety $\mathscr{V}$ has several interesting properties. The lattice $\mathscr{L}(\mathscr{V})$ has exactly three elements and $\mathscr{H}(p^n, \alpha, \beta)$ is the only non-trivial subvariety of $\mathscr{V}$. Every quasigroup from $\mathscr{V}$ is either idempotent or has no idempotent element. Every quasigroup from $\mathscr{V}$ is either free (and then has no idempotent element) or belongs to $\mathscr{H}(p^n, \alpha, \beta)$ (and then it is idempotent). $\mathscr{V}$ is a Schreier variety but it is not extensive. Every quasigroup from $\mathscr{V}$ is injective in $\mathscr{V}$. The free quasigroup of rank 1 in $\mathscr{V}$ is just the quasigroup $H(p^n, \alpha, \beta, 1)$.

Minimal varieties of idempotent abelian groupoids were described in [8].

13. THE LATTICE OF VARIETIES OF COMMUTATIVE ABELIAN IP-QUASIGROUPS

Let N denote the set of non-negative integers. If $n, m \in N$, then we shall write $n \lhd m$ iff $m = xn$ for some $x \in N$. If $n \neq 0$, then x is determined uniquely and we put $x = m/n$. If $n = 0$ and $n \lhd m$, then $m = 0$ and we put $0/0 = 0$. As is easy to see, $\lhd$ is an ordering of N and N becomes a complete lattice with the least element 1 and with the largest element 0.

In what follows we shall deal with subgroups of the additive group $Z \times Z$. Let $G \subseteq Z \times Z$ be a subgroup. We define

$$G_D = \{\langle a + b, a + b\rangle; \langle a, b\rangle \in G\},$$
$$G_E = \{\langle a - b, b - a\rangle; \langle a, b\rangle \in G\}.$$

Further we put

$$D = \{\langle a, a\rangle; a \in Z\}, \quad E = \{\langle a, -a\rangle; a \in Z\}.$$

As is easy to see, there are uniquely determined numbers $n, m \in N$ such that $G \cap D = nD = Z. \langle n, n\rangle$ and $G \cap E = mE = Z . \langle m, -m\rangle$. We put $n = \alpha(G)$ and $m = \beta(G)$.

The following two lemmas are obvious.

13.1. Lemma. *Let $G \subseteq Z \times Z$ be a subgroup. Then G_D is a subgroup of D and G_E is a subgroup of E.* ■

13.2. Lemma. *Let $H \subseteq G$ be two subgroups of $Z \times Z$. Then $\alpha(G) \lhd \alpha(H)$ and $\beta(G) \lhd \beta(H)$.* ■

13.3. Lemma. *The following conditions are equivalent for a subgroup G of $Z \times Z$:*

(i) $G_D \subseteq G$.
(ii) $G_E \subseteq G$.
(iii) *If $\langle a, b\rangle \in G$ then $\langle b, a\rangle \in G$.*

Proof. (i) implies (iii). Let $\langle a, b\rangle \in G$. Then $\langle -a, -b\rangle \in G$ and $\langle a + b, a + b\rangle \in G_D \subseteq G$ and thus $\langle b, a\rangle \in G$.

(iii) implies (ii). Let $\langle a, b\rangle \in G$. Then $\langle -a, -b\rangle$ and $\langle -b, -a\rangle$ belong to G. Hence $\langle a - b, b - a\rangle \in G$.

(ii) implies (i). Let $\langle a, b\rangle \in G$. Then $\langle -a, -b\rangle$ and $\langle b - a, a - b\rangle$ are contained in G. Consequently, $\langle b, a\rangle$ and $\langle b, a\rangle + \langle a, b\rangle = \langle a + b, a + b\rangle$ are elements of G. ■

Any subgroup G of $Z \times Z$ satisfying the equivalent conditions of 13.3 will be called admissible. As is easy to see, the set $\mathcal{G}$ of all admissible subgroups is a complete lattice with respect to the ordering $G \leqq H$ iff $H \subseteq G$. It is a sublattice in the dual of the lattice of all subgroups of $Z \times Z$.

Let $G \in \mathcal{G}$. Then we put $\gamma(G) = 0$ if $G \neq 0$, $G_D = G \cap D$ and $G_E = G \cap E$. In the other cases, $\gamma(G) = 1$.

13.4. Lemma. *Let $G \in \mathcal{G}$, let $\alpha(G)$ (resp. $\beta(G)$) be even and $G_E = G \cap E$ (resp. $G_D = G \cap D$). Then $\beta(G)$ (resp. $\alpha(G)$) is even.*

Proof. Let $\langle a, b\rangle \in G$. Then $\langle a + b, a + b\rangle \in G_D \subseteq \alpha(G) . D$, and so $a + b = 2z$ for some $z \in Z$. Now $a - b = 2a - 2z$ is even. The rest and the second case are clear. ■

13.5. Lemma. *Let $G \in \mathcal{G}$ be such that $\gamma(G) = 0$. Then $\alpha(G)$ is even iff $\beta(G)$ is even.*

Proof. Apply 13.4. ■

13.6. Lemma. *Let $G \in \mathcal{G}$. Then either $G_D = G \cap D$ or $G_D = 2\,\alpha(G)\,D = 2(G \cap D)$.*

Proof. We have $G_D = mD$ for some $m \in N$. However, $2(G \cap D) \subseteq (G \cap D)_D \subseteq$ $\subseteq G_D \subseteq G \cap D$, and consequently $2\,\alpha(G) = xm$ and $m = y\,\alpha(G)$ for some $x, y \in Z$. Thus either $x = 1$ and $y = 2$ or $x = 2$ and $y = 1$. ■

13.7. Lemma. *Let $G \in \mathcal{G}$. Then either $G_E = G \cap E$ or $G_E = 2\,\beta(G)\,E = 2(G \cap E)$.*

Proof. Similar to that of 13.6. ■

Let $n, m \in N$. Then we define $A(n, m) = Z\langle n, n\rangle + Z\langle m, -m\rangle = nD + mE$.

13.8. Lemma. *Let $n, m \in N$. Then*

(i) $A(n, m) \in \mathcal{G}$,
(ii) $\alpha(A(n, m)) = n$ *and* $(A(n, m))_D = 2nD$,
(iii) $A(n, m) \cap D = (A(n, m))_D$ *iff* $n = 0$
(iv) $\beta(A(n, m)) = m$ *and* $(A(n, m))_E = 2mE$
(v) $A(n, m) \cap E = (A(n, m))_E$ *iff* $m = 0$.
(vi) $\gamma(A(n, m)) = 1$.

Proof. Obvious. ■

Let $n, m \in N$ be non-zero elements such that $2 \lhd n + m$ (i.e. either both n, m are even or both n, m are odd). Then we put $B(n, m) = Z\langle n, n\rangle + Z\langle (n + m)/2, (n - m)/2\rangle$.

13.9. Lemma. *Let $n, m \in N$ be non-zero elements such that $2 \lhd n + m$. Then*

(i) $B(n, m) \in \mathcal{G}$,
(ii) $\alpha(B(n, m)) = n$ *and* $(B(n, m))_D = B(n, m) \cap D$,
(iii) $\beta(B(n, m)) = m$ *and* $(B(n, m))_E = B(n, m) \cap E$,
(iv) $\gamma(B(n, m)) = 0$,
(v) $B(n, m) = Z\langle m, -m\rangle + Z\langle (n + m)/2, (n - m)/2\rangle$.

Proof. Obvious. ■

13.10. Lemma. *Let $G \in \mathcal{G}$ be such that $\gamma(G) = 0$. Then both $\alpha(G)$ and $\beta(G)$ are non-zero.*

Proof. Let $\alpha(G) = 0$. Then clearly $G \subseteq E$ (since $G_D \subseteq G$), and so $G_E = 2G$. Thus $\beta(G) = 0$ and $G = 0$. The case $\beta(G) = 0$ is similar. ■

13.11. Lemma. *Let $G \in \mathcal{G}$ be such that $\gamma(G) = 0$. Then $G = B(\alpha(G), \beta(G))$.*

Proof. First take into account 13.5 and 13.10 and put $n = \alpha(G)$, $m = \beta(G)$. Then $nD = G_D = G \cap D$ and $mE = G_E = G \cap E$. There is $\langle a, b \rangle \in G$ such that $a - b = m$. Further, $a + b = xn$ for some $x \in Z$, $a = (xn + m)/2$ and $b = (xn - m)/2$. Suppose that x is even. Then $\langle xn/2, xn/2 \rangle \in nD \subseteq G$, so that $\langle m/2, -m/2 \rangle \in G \cap E = G_E$, a contradiction with $m \neq 0$. Thus x is odd, $\langle (1 - x)\, n/2, \ (1 - x)\, n/2 \rangle \in G$ and $\langle (n + m)/2, \ (n - m)/2 \rangle = \langle a, b \rangle + \langle (1 - x)\, n/2, (1 - x)\, n/2 \rangle \in G$. We have proved $B(n, m) \subseteq G$.

As for the converse inclusion, let $\langle a, b \rangle \in G$. Then $a + b = xn$ and $a - b = ym$ for some $x, y \in Z$ and $\langle a, b \rangle = \langle (xn + ym)/2, \ (xn - ym)/2 \rangle$. However $-y\langle (n + m)/2, \ (n - m)/2 \rangle \in B(n, m) \subseteq G$ and $\langle a, b \rangle - y\langle (n + m)/2, (n - m)/2 \rangle = \langle (x - y)\, n/2, \ (x - y)\, n/2 \rangle \in G \cap D = G_D = nD \subseteq B(n, m)$. There fore $\langle a, b \rangle \in B(n, m)$ and the proof is complete. ∎

13.12. Lemma. *Let $G \in \mathcal{G}$ be such that $\gamma(G) = 1$. Then $G = A(\alpha(G), \beta(G))$.*

Proof. Put $\alpha(G) = n$, $\beta(G) = m$. Then $nD = G \cap D$ and $mE = G \cap E$. Hence $A(n, m) = nD + mE \subseteq G$. If $n = 0$ then $G \subseteq E$ and the situation is clear. Similarly if $m = 0$. So we can assume $n, m \neq 0$. First let $G \cap D \neq G_D$. Then $G_D = 2nD$ by 13.6. Take $\langle a, b \rangle \in G$. We have $a + b = 2xn$ and $a - b = ym$ for some $x, y \in Z$. Clearly, $\langle a, b \rangle = \langle (2xn + ym)/2, (2xn - ym)/2 \rangle$. Since $nD \subseteq G$, $\langle ym/2, -ym/2 \rangle \in G \cap E = mE$ and y is even. Now it is obvious that $\langle a, b \rangle \in A(n, m)$. If $G \cap D = G_D$ then $G \cap E \neq G_E$ and we can proceed similarly. ∎

13.13. Lemma. *Let $n, m, p, q \in N$. Then $A(p, q) \subseteq A(n, m)$ iff $n \lhd p$ and $m \lhd q$.*

Proof. The lemma follows easily from 13.2, 13.8 and from the definition of $A(n, m)$. ∎

13.14. Lemma. *Let $p, q \in N$ and let $n, m \in N$ be non-zero elements such that $2 \lhd n + m$. Then*

(i) *$A(p, q) \subseteq B(n, m)$ iff $n \lhd p$ and $m \lhd q$.*
(ii) *$B(n, m) \subseteq A(p, q)$ iff $p \lhd n$, $q \lhd m$ and n/p and m/q are even.*

Proof. (i) This is an easy consequence of 13.2, 13.8 and 13.9.

(ii) Let $B(n, m) \subseteq A(p, q)$. Then $n = xp$ and $m = yq$ for some $x, y \in N$. Since n, m are non-zero, $0 \neq x, y, p, q$. Further, $\langle (n + m)/2, (n - m)/2 \rangle = \langle (xp + yq)/2, (xp - yq)/2 \rangle \in A(p, q)$. Hence $\langle xp, xp \rangle \in (A(p, q))_D$ and x is even due to 13.8(ii). Similarly we can show that y is even. The converse implication is easy. ∎

13.15. Lemma. *Let n, m, p, q be non-zero elements of N such that $2 \lhd n + m$ and $2 \lhd p + q$. Then $B(p, q) \subseteq B(n, m)$ iff $n \lhd p$, $m \lhd q$ and $2 \lhd (p/n + q/m)$.*

Proof. Let $B(p, q) \subseteq B(n, m)$. Obviously, $p = xn$ and $q = ym$ for some $x, y \in N$. Further, $\langle (xn + ym)/2, (xn - ym)/2 \rangle \in B(n, m)$. If x is even, then $\langle ym/2, -ym/2 \rangle \in \in B(n, m) \cap E$, and so y is even. If x is odd, $\langle (1 - x) n/2, (1 - x) n/2 \rangle \in B(n, m)$ and $\langle (n + ym)/2, (n - ym)/2 \rangle \in B(n, m)$. In this case $\langle (y - 1) m/2, (1 - y) m/2 \rangle \in \in B(n, m) \cap E = mE$. Consequently y is odd. The converse implication is easy. ∎

Let $G \in \mathcal{G}$. Then we denote by $\varrho(G)$ the set $\{\langle a, b \rangle; \langle 2b - a, 2a - b \rangle \in G\}$.

13.16. Lemma. *Let* $G \in \mathcal{G}$. *Then*

(i) $\varrho(G)$ *is a subgroup of* $Z \times Z$, $G \subseteq \varrho(G)$ *and* $\varrho(G) \in \mathcal{G}$;
(ii) $\alpha(\varrho(G)) = \alpha(G)$ *and* $(\varrho(G))_D = G_D$, $G \cap D = \varrho(G) \cap D$;
(iii) *either* $\beta(\varrho(G)) = \beta(G)$ *or* $3\, \beta(\varrho(G)) = \beta(G)$.

Proof. (i) and (ii) are clear and $\langle a, -a \rangle \in \varrho(G)$ iff $\langle 3a, -3a \rangle \in G$. ∎

13.17. Lemma. *Let* $n, m \in N$. *Then*

(i) $\varrho(A(n, m)) = A(n, m)$ *if either* $m = 0$ *or* m *is not divisible by* 3.
(ii) $\varrho(A(n, m)) = A(n, m/3)$ *if* $m \neq 0$ *and* m *is divisible by* 3.

Proof. First let $0 \neq m = 3x$. As is easy to see, $A(n, x) \subseteq \varrho(A(n, m)) = G$. On the other hand, $\alpha(G) = n$ and $\beta(G) = x$ by 13.16. Hence either $G = A(n, x)$ or $G = = B(n, x)$. However, the latter case is not possible, since $G_D = (A(n, m))_D \neq nD = = (B(n, x))_D$ provided $n \neq 0$. Similarly for the second case. ∎

13.18. Lemma. *Let* $n, m \in N$ *be non-zero and* $2 \lhd n + m$. *Then*

(i) $\varrho(B(n, m)) = B(n, m)$ *if* m *is not divisible by* 3;
(ii) $\varrho(B(n, m)) = B(n, m/3)$ *if* m *is divisible by* 3.

Proof. Similar to that of 13.17. ∎

13.19. Lemma. *Let* $G \in \mathcal{G}$. *Then there is no other admissible subgroup between* G *and* $\varrho(G)$.

Proof. Easy. ∎

Consider the following ring R: Its underlying abelian group is $Z \times Z$ and the multiplication is defined by

$$\langle a, b \rangle . \langle c, d \rangle = \langle ac + bd, ad + bc \rangle .$$

The ring R is commutative and the element $t = \langle 0, 1 \rangle$ is its i-generator. Further put $s = \langle -1, 2 \rangle = \langle 0, 1 \rangle + \langle 0, 1 \rangle - \langle 1, 0 \rangle$. The element $\langle 1, 0 \rangle$ is obviously the unit of R.

13.20. Lemma. (i) *The lattice $\mathscr{I}(R)$ is just the dual of $\mathscr{G}$.* (ii) *If $G \in \mathscr{I}(R)$ then* $(G : s) = \varrho(G)$.

Proof. Easy (observe $\langle a, b\rangle . \langle 0, 1\rangle = \langle b, a\rangle$). ∎

Let $\mathscr{R} \subseteq N \times N \times \{0, 1\}$ be the subset defined as follows:

(i) $\langle n, m, 1\rangle \in \mathscr{R}$ *whenever* $n, m \in N$;
(ii) $\langle n, m, 0\rangle \in \mathscr{R}$ *whenever* $n, m \in N$, *n, m are non-zero and* $2 \lhd n + m$.

We shall define a relation $\leqq$ on $\mathscr{R}$ in this way: $\langle a, b, c\rangle \leqq \langle x, y, z\rangle$ iff $a \lhd x$, $b \lhd y$ and at least one of the following three cases takes place:

(i) $z = 1$;
(ii) x/a and y/b are even;
(iii) $c = z$ and $x/a + y/b$ is even.

Further, let $\mathscr{N} \subseteq N \times N \times \{0, 1\} \times \{0, 1\}$ be the following subset: $\langle a, b, c, d\rangle \in \in \mathscr{N}$ iff $\langle a, b, c\rangle \in \mathscr{R}$ and either $d = 1$ or $3 \lhd b \neq 0 = d$. We define $\leqq$ on $\mathscr{N}$ as follows: $\langle a, b, c, d\rangle \leqq \langle x, y, z, v\rangle$ iff $\langle a, b, c\rangle \leqq \langle x, y, z\rangle$ in $\mathscr{R}$ and either $d \leqq v$ or $3 \lhd y/b$.

Define the following mappings:

(i) $\eta : \mathscr{I}(R) \to N \times N \times \{0, 1\}$ by $\eta(G) = \langle \alpha(G), \beta(G), \gamma(G)\rangle$.
(ii) $\lambda : \mathscr{S}(R, t, t) \to N \times N \times \{0, 1\} \times \{0, 1\}$ by $\lambda(\langle G, H\rangle) = \langle \alpha(G), \beta(G), \gamma(G), 1\rangle$ if $G = H$ and $\lambda(\langle G, H\rangle) = \langle \alpha(G), \beta(G), \gamma(G), 0\rangle$ if $G \neq H$.
(iii) $\sigma : \mathscr{R} \to \mathscr{I}(R)$ by $\sigma(\langle n, m, 1\rangle) = A(n, m)$ and $\sigma(\langle n, m, 0\rangle) = B(n, m)$.
(iv) $\gamma : \mathscr{N} \to \mathscr{I}(R) \times \mathscr{I}(R)$ by $\gamma(\langle a, b, c, 1\rangle) = \langle \sigma(\langle a, b, c\rangle), \sigma(\langle a, b, c\rangle)\rangle$ and $\gamma(\langle a, b, c, 0\rangle) = \langle \sigma(\langle a, b, c\rangle), \varrho(\sigma(\langle a, b, c\rangle))\rangle$.

13.21. Proposition. (i) *The set $\mathscr{R}$ with $\leqq$ is a lattice and η is an isomorphism of the dual of $\mathscr{I}(R)$ onto $\mathscr{R}$. Moreover, $\eta^{-1} = \sigma$.*

(ii) *The set $\mathscr{N}$ with $\leqq$ is a lattice and λ is an isomorphism of the lattice $\mathscr{S}(R, t, t)$ onto $\mathscr{N}$. Moreover, $\lambda^{-1} = \gamma$.*

Proof. Apply the preceding theory. ∎

13.22. Lemma. (i) *Let $n, m \in N$. Then the ideal $A(n, m)$ of R is generated by $\langle n, n\rangle$ and $\langle m, -m\rangle$.*

(ii) *Let $n, m \in N$ be non-zero such that $2 \lhd n + m$. Then the ideal $B(n, m)$ of R is principal and is generated by $\langle (n + m)/2, (n - m)/2\rangle$.*

Proof. Easy. ∎

13.23. Lemma. *Let $C(2)$ be the two-element cyclic group with elements $\{1, \alpha\}$. Then there is a ring isomorphism φ of the group ring $ZC(2)$ onto R such that $\varphi(\alpha) = t = \langle 0, 1\rangle$.*

Proof. Obvious. ∎

13.24. Lemma. *Let Q be a commutative groupoid and let $x \mapsto x^{-1}$ be a mapping of Q into Q. Then the following assertions are equivalent:*

(i) $x^{-1} . xy = y$ *for all* $x, y \in Q$.

(ii) $x . x^{-1}y = y$ *for all* $x, y \in Q$.

In this case, Q is a cancellation and divisison groupoid and $(x^{-1})^{-1} = x$ *for all* $x \in Q$.

Proof. First let $x^{-1} . xy = y$ for all $x, y \in Q$. It is clear that Q is a cancellation groupoid. Further, $x^{-1} . xx^{-1} = x^{-1}$ and $(x^{-1})^{-1} x^{-1} = (x^{-1})^{-1} (x^{-1}(xx^{-1})) = xx^{-1}$. Hence $(x^{-1})^{-1} = x$ and $x . x^{-1}y = y$ for all $x, y \in Q$.

Next let $x . x^{-1}y = y$ for all $x, y \in Q$. Obviously, Q is a division groupoid. Further, $x^{-1}(x^{-1}(x^{-1})^{-1}) = x^{-1}$ and $xx^{-1} = x(x^{-1}(x^{-1}(x^{-1})^{-1})) = x^{-1}(x^{-1})^{-1}$. Finally, $x = x . xx^{-1} = x . x^{-1}(x^{-1})^{-1} = (x^{-1})^{-1}$ and the proof is complete. ∎

A commutative groupoid Q with a unary operation $x \mapsto x^{-1}$ satisfying the equivalent conditions of 13.24 is called an IP-groupoid. Let $\mathscr{D}$ denote the variety of all commutative abelian IP-groupoids. That is, $\mathscr{D}$ is the variety of algebras with one binary and one unary operation satisfying the identites $xy = yx$, $xy . uv = xu . yv$ and $x^{-1} . xy = y$. Let $Q(\cdot, {}^{-1})$ be a commutative IP-groupoid. Then Q can be considered in a unique way a quasigroup $Q(\cdot, /, \backslash)$. In this case, $x^{-1} = x / xx$ for every $x \in Q$. Conversely, if $Q(\cdot, /, \backslash)$ is a commutative quasigroup satisfying $(x / xx)(xy) = y$ for all $x, y \in Q$ and $x^{-1} = x / xx$, then $Q(\cdot, {}^{-1})$ is a commutative IP-groupoid. Now is easy to see that the variety $\mathscr{D}$ and the variety of all commutative abelian quasigroups $Q(\cdot, /, \backslash)$ satisfying $(x / xx)(xy) = y$ are equivalent. The last variety will be denoted by $\mathscr{D}$, too.

13.25. Lemma. *The following conditions are equivalent for any quasigroup* $Q(\cdot, /, \backslash)$:

(i) $Q(\cdot, /, \backslash)$ *is a commutative abelian IP-quasigroup.*

(ii) $Q(\cdot, /, \backslash)$ *satisfies the identity* $x(y . uv) = u(y . vx)$.

(iii) *There is an abelian group* $Q(+)$, *its automorphism* φ *and an element* $g \in Q$ *such that* $\varphi^2 = 1$ *and* $ab = \varphi(a) + \varphi(b) + g$ *for all* $a, b \in Q$.

(iv) $Q(\cdot, /, \backslash)$ *is a* $(ZC(2), \alpha, \alpha)$*-quasigroup.*

Proof. The equivalence of (i) and (ii) is easy and the rest needs just a tedious checking. ∎

For every $n \in N$ we define a term $u(n, x, y)$ in variables x, y by

$$u(0, x, y) = x^{-1},$$
$$u(n + 1, x, y) = x(u(n, x, y)\, x).$$

13.26. Lemma. *Let* $Q(\cdot, {}^{-1})$ *be a commutative abelian IP-groupoid and let* $Q(+)$ *be an abelian group with an automorphism* φ *and an element* $g \in Q$ *such that* $ab = \varphi(a) + \varphi(b) + g$ *for all* $a, b \in Q$. *Then*

(i) $a^{-1} = \varphi^{-1}(-a - g - \varphi(g))$ *for all* $a \in Q$,
(ii) $u(n, 0^{-1}, a) = na = a + \ldots + a$ *for all* $n \in N$ *and* $a \in Q$,
(iii) $\varphi(a) = 00^{-1} . a$ *for all* $a \in Q$,
(iv) $\varphi(-a) = 00^{-1}(0(0(00^{-1} . a^{-1})))$ *for all* $a \in Q$,
(v) $\varphi(-g) = 00^{-1}$.

Proof. It is a matter of routine. ∎

Finally, for every $n \in N$ we define a term $v(n, x, y)$ by $v(n, x, y) = u(n, x, xx^{-1}(x^{-1}(x^{-1}(xx^{-1} . y^{-1}))))$.

13.27. Theorem. *The lattice $\mathscr{L}(\mathscr{D})$ is isomorphic to the lattice $\mathscr{N}$. The isomorphism is given as follows:*

(i) *If $n, m \in N$ then the variety corresponding to $\langle n, m, 1, 1\rangle$ is just the subvariety of $\mathscr{D}$ given by*

$$u(n, x, y) = v(n, x, y)\,, \quad u(m, x, y) = u(m, x, xx^{-1} . y)\,.$$

(ii) *If $n, m \in N$, $0 \neq m$ and $3 \lhd m$ then the variety corresponding to $\langle n, m, 1, 0\rangle$ is just the subvariety of $\mathscr{D}$ given by*

$$\begin{aligned} u(n, x, y) &= v(n, x, y)\,,\\ u(m, x, y) &= u(m, x, xx^{-1} . y)\,,\\ u(n, x, x^{-1}x^{-1}) &= u(n, x, xx^{-1})\,,\\ u(m/3, x, x^{-1}x^{-1}) &= u(m/3, x, xx^{-1} . x^{-1}x^{-1})\,. \end{aligned}$$

(iii) *If $n, m \in N$ are non-zero, $2 \lhd n + m$ and $n \geqq m$ then the variety corresponding to $\langle n, m, 0, 1\rangle$ is just the subvariety of $\mathscr{D}$ given by*

$$u((n + m)/2, x, y) = v((n - m)/2, x, y)\,.$$

(iv) *If $n, m \in N$ are non-zero, $2 \lhd n + m$ and $n \leqq m$ then the variety corresponding to $\langle n, m, 0, 1\rangle$ is just the subvariety of $\mathscr{D}$ given by*

$$u((n + m)/2, x, y) = u((m - n)/2, x, xx^{-1} . y)\,.$$

(v) *If $n, m \in N$ are non-zero, $2 \lhd n + m$, $3 \lhd m$ and $n \geqq m$ then the variety corresponding to $\langle n, m, 0, 0\rangle$ is just the subvariety of $\mathscr{D}$ given by*

$$\begin{aligned} u((n + m)/2, x, y) &= v((n - m)/2, x, y)\,,\\ u((3n + m)/6, x, x^{-1}x^{-1}) &= u((3n - m)/6, x, xx^{-1})\,. \end{aligned}$$

(vi) *If $n, m \in N$ are non-zero, $2 \lhd n + m$, $3 \lhd m$ and $m/3 \leqq n \leqq m$ then the variety corresponding to $\langle n, m, 0, 0\rangle$ is just the subvariety of $\mathscr{D}$ given by*

$$\begin{aligned} u((n + m)/2, x, y) &= u((m - n)/2, x, xx^{-1} . y)\,,\\ u((3n + m)/6, x, x^{-1}x^{-1}) &= u((3n - m)/6, x, xx^{-1})\,. \end{aligned}$$

(vii) *If $n, m \in N$ are non-zero, $2 \lhd n + m$, $3 \lhd m$ and $n \leqq m/3$ then the variety corresponding to $\langle n, m, 0, 0\rangle$ is just the subvariety of $\mathcal{D}$ given by*

$$u((n + m)/2, x, y) = u((m - n)/2, x, xx^{-1} . y),$$
$$u((3n + m)/6, x, x^{-1}x^{-1}) = u((m - 3n)/6, x, xx^{-1} . x^{-1}x^{-1}).$$

Proof. The proof of this theorem requires almost everything what has been done. A special attention should be paid to 6.2, 6.3, 13.22 and 13.26. ∎

Let us remark that (by 7.5 and 8.2) the variety $\mathcal{D}$ is extensive but it is not a Schreier variety.

14. THE LATTICE OF VARIETIES OF TOTALLY SYMMETRIC ABELIAN QUASIGROUPS

14.1. Lemma. *The following conditions are equivalent for any groupoid Q:*

(i) *Q satisfies the identities $x . xy = yx . x = y$ for all $x, y \in Q$.*
(ii) *Q is a commutative IP-groupoid and $x^{-1} = x$.*

Proof. (i) implies (ii). It suffices to prove the commutative law. We have $y . xy = (x . xy)(x(x . xy)) = (x . xy)(xy) = x$. Hence $xy = y(y . xy) = yx$.

(ii) implies (i). This implication is obvious. ∎

A groupoid satisfying the equivalent conditions of the preceding lemma is called a TS-groupoid. We denote by $\mathcal{F}$ the variety of all abelian TS-groupoids.

If $Q(\cdot, /, \backslash)$ is a quasigroup then the groupoid $Q(\cdot)$ is a TS-groupoid iff $Q(\cdot, /, \backslash)$ satisfies the identites $xy = x / y = x \backslash y$. Such quasigroups are said to be TS-quasigroups. It is clear that the variety $\mathcal{F}$ is equivalent to the variety of all abelian TS-quasigroups. This last variety will be denoted by $\mathcal{F}$, too.

14.2. Lemma. *The following conditions are equivalent for any quasigroup $Q(\cdot, /, \backslash)$:*

(i) *$Q(\cdot, /, \backslash)$ is an abelian TS-quasigroup.*
(ii) *$Q(\cdot, /, \backslash)$ is a $(Z, -1, -1)$-quasigroup.*

Proof. Easy. ∎

Proceeding similarly as in the preceding section, we obtain a description of the lattice $\mathcal{L}(\mathcal{F})$. In fact, we could apply 13.27, since $\mathcal{F}$ is clearly a subvariety of $\mathcal{D}$. At all events, we shall formulate here only the final result.

Let $\mathcal{E} \subseteq N \times \{0, 1\}$ be the subset such that $\langle n, 1\rangle \in \mathcal{E}$ for all $n \in N$ and $\langle n, 0\rangle \in \mathcal{E}$ iff $0 \neq n$ and $3 \lhd n$. Define an ordering $\leqq$ on $\mathcal{E}$ by $\langle n, x\rangle \leqq \langle m, y\rangle$ iff $n \lhd m$ and either $x \leqq y$ or $3 \lhd m/n$. Then $\mathcal{E}$ is a lattice.

14.3. Theorem. *The lattice $\mathscr{L}(\mathscr{F})$ is isomorphic to the lattice $\mathscr{E}$. The isomorphism is given as follows:*

(i) *If $n \in N$ then the variety corresponding to $\langle n, 1\rangle$ is just the subvariety of $\mathscr{F}$ given by*

$$u(n, x, y) = x$$

(u is defined in the same way as in Section 13).

(ii) *If $0 \neq n \in N$ and $3 \lhd n$ then the variety corresponding to $\langle n, 0\rangle$ is just the subvariety of $\mathscr{F}$ given by*

$$u(n, x, y) = x\,, \quad u(n/3, x, xx) = x\,. \quad \blacksquare$$

Remark. It is proved in [2] that there are uncountably many minimal varieties of TS-quasigroups.

15. SOME OTHER EXAMPLES

A quasigroup $Q(\cdot, /, \backslash)$ is called unipotent if $xx = yy$ for all $x, y \in Q$.

15.1. Lemma. *The following conditions are equivalent for any quasigroup Q:*

(i) *Q is a unipotent abelian quasigroup.*
(ii) *Q is a $(ZA_1, a_1, -a_1)$-quasigroup.*

Proof. Easy. $\blacksquare$

15.2. Theorem. *The lattice of all varieties of unipotent abelian quasigroups is isomorphic to the dual of $\mathscr{I}(ZA_1)$.*

Proof: We have $a_1 + (-a_1) - 1 = -1$, and so the dual of $\mathscr{I}(ZA_1)$ is isomorphic to $\mathscr{S}(ZA_1, a_1, -a_1)$. Now we can use 15.1. $\blacksquare$

15.3. Lemma. *The following conditions are equivalent for any quasigroup Q:*

(i) *Q is a commutative unipotent abelian quasigroup.*
(ii) *Q is a $(\mathrm{GF}(2)\, A_1, a_1, a_1)$-quasigroup.*

Proof. Easy. $\blacksquare$

15.4. Theorem. *The lattice of all varieties of commutative unipotent abelian quasigroups is isomorphic to the lattice of all non-negative integers with respect to divisibility.*

Proof. The ring $\mathrm{GF}(2)\, A_1$ is a localization of the polynomial ring $\mathrm{GF}(2)\,[x]$. Hence $\mathrm{GF}(2)\, A_1$ is a principal ideal domain. The set of all prime elements of $\mathrm{GF}(2)$ A_1 is infinite and countable. The rest is clear. $\blacksquare$

15.5. Lemma. *The following conditions are equivalent for any quasigroup Q:*
(i) *Q is a unipotent abelian quasigroup and a right loop.*
(ii) *Q is a $(Z, 1, -1)$-quasigroup.*

Proof. Easy. ∎

15.6. Theorem. *The lattice of all varieties of unipotent abelian right loops is isomorphic to the lattice of all non-negative integers with respect to divisibility.*

Proof. This follows from 15.5. ∎

15.7. Lemma. *The following conditions are equivalent for any quasigroup Q:*
(i) *Q is a unipotent abelian IP-quasigroup.*
(ii) *Q is a $(ZC(2), \alpha, -\alpha)$-quasigroup.*

Proof. Easy. ∎

15.8. Corollary. *The lattice of all varieties of unipotent abelian IP-quasigroups is isomorphic to the lattice $\mathscr{R}$ defined in Section* 13. ∎

15.9. Lemma. *The following conditions are equivalent for any quasigroup Q:*
(i) *Q is a commutative idempotent abelian quasigroup.*
(ii) *Q is an $(R, 1/2, 1/2)$-quasigroup, where R is the ring of rational numbers of the form $z/2^n$, $z \in Z$, $n \in N$.*

Proof. Easy. ∎

15.10. Theorem. *The lattice of all varieties of commutative idempotent abelian quasigroups is isomorphic to the lattice of all non-negative integers with respect to divisibility.*

Proof. This follows from 15.9. ∎

Remark. The lattice of varieties of commutative idempotent abelian quasigroups is thus isomorphic to the lattice of varieties of commutative unipotent abelian quasigroups. On the other hand, we have proved in [7] that the lattice of varieties of commutative idempotent abelian groupoids is countable while that of commutative unipotent abelian groupoids is uncountable.

15.11. Lemma. *The following conditions are equivalent for any quasigroup Q:*
(i) *Q is an abelian IP-quasigroup and a right loop.*
(ii) *Q is a $(ZC(2), 1, \alpha)$-quasigroup.*

Proof. Easy. ∎

15.12. Theorem. *The lattice of all varieties of abelian IP-quasigroups with right unit is isomorphic to the lattice $\mathcal{R}$ defined in Section* 13.

Proof. This follows from 15.11. ∎

References

[1] *V. D. Belousov:* Foundations of the theory of quasigroups and loops (Russian). Moskva, Nauka 1967.

[2] *A. D. Bol'bot:* On equationally complete varieties of totally symmetric quasigroups (Russian). Algebra i logika 6/2, 1967, 13—19.

[3] *N. Bourbaki:* Algèbre commutative. Hermann, Paris 1963.

[4] *B. Csákány:* Varieties of affine modules. (To appear in Acta Sci. Math.)

[5] *B. Csákány:* Varieties of idempotent medial quasigroups. (Toappear in Acta Sci. Math.)

[6] *J. Ježek* and *T. Kepka:* Extensive varieties. (To appear in Acta Univ. Carolinae.)

[7] *J. Ježek* and *T. Kepka:* The lattice of varieties of commutative abelian distributive groupoids. Algebra Univ. *5*, 1975, 225—237.

[8] *J. Ježek* and *T. Kepka:* Atoms in the lattice of varieties of distributive groupoids. (To appear.)

[9] *J. Ježek* and *T. Kepka:* Quasigroups, isotopic to a group. Commentationes Math. Univ. Carolinae *16*, 1975, 59—76.

[10] *T. Kepka* and *P. Němec:* T-quasigroups II. Acta Univ. Carolinae Math. et Phys. 12/2, 1971, 31—49.

[11] *J. Lambek:* Lectures on rings and modules. Blaisdell Publ. Comp. Waltham, Toronto, London 1966.

[12] *S. Lang:* Algebra. Addison-Wesley Publ. Comp., Reading 1965.

[13] *P. Němec* and *T. Kepka:* T-quasigroups I. Acta Univ. Carolinae Math. et Phys. 12/1, 1971, 39—49.

Authors' address: 186 00 Praha 8 - Karlín, Sokolovská 86, ČSSR (Matematicko-fyzikální fakulta UK).