Hamiltonian Quasimodules and Trimedial Quasigroups

T. KEPKA
Department of Mathematics, Charles University, Prague*)

Received 19 October 1984

Hamiltonian quasimodules and trimedial quasigroups are studied.

Studují se hamiltonovské kvazimoduly a trimediální kvazigrupy.

Изучаются гамильтоновы квазимодулы и квазигруппы.

1. Commutative Moufang loops and quasimodules

A loop $Q(+)$ satisfying the identity $(x + x) + (y + z) = (x + y) + (x + z)$ is commutative and is called a commutative Moufang loop. We denote by $C(Q(+))$ the centre of $Q(+)$, by $A(Q(+))$ the associator subloop of $Q(+)$, by $0 = C_0(Q(+)) \subseteq \subseteq C_1(Q(+)) = C(Q(+)) \subseteq C_2(Q(+)) \subseteq \ldots \subseteq C_n(Q(+)) \subseteq \ldots$ the upper central series of $Q(+)$ and by $Q = A_0(Q(+)) \supseteq A_1(Q(+)) = A(Q(+)) \supseteq A_2(Q(+)) \supseteq \ldots \ldots \supseteq A_n(Q(+)) \supseteq \ldots$ the lower central series of $Q(+)$.

1.1. Lemma. Let $Q(+)$ be a commutative Moufang loop and let $a, b, c \in Q$ be such that $(a + b) + c = -a + (b + c)$. Then $2a = 0$ and $a \in C(Q(+))$.

Proof. We have $(a + b) + (3a + c) = ((a + b) + c) + 3a = (-a + (b + c)) + 3a = 2a + (b + c) = (a + b) + (a + c)$, so that $2a = 0$.

Throughout the paper, let R be an associative ring with unit possessing a ring homomorphism Φ onto the three-element field Z_3. Put $I = \operatorname{Ker} \Phi$. By a ($\Phi$-special unitary left $R-$) quasimodule Q we mean a commutative Moufang loop $Q(+)$ supplied with a scalar multiplication by elements from R such that the usual module identities are satisfied and, moreover, $rx \in C(Q(+))$ for all $r \in I$ and $x \in Q$. In this case, all the members of the upper central series as well as of the lower central series of $Q(+)$ are subquasimodules of Q.

A quasimodule Q is said to be primitive if $rx = 0$ for all $r \in I$ and $x \in Q$.

If Q is a quasimodule then both $A(Q)$ and $Q/C(Q)$ are primitive.

By a preradical p (for quasimodules) we mean any subfunctor of the identity functor. In this case, $p(Q)$ is a normal subquasimodule of Q for any quasimodule Q.

*) 186 00 Praha 8, Sokolovská 83, Czechoslovakia.

For a quasimodule Q, let $K(Q)$ be the subquasimodule generated by all primitive subquasimodules of Q. Then $K(Q)$ is a primitive quasimodule and we define $L(Q)$ by $L(Q) = \bigcup Q_\alpha$, where $Q_0 = 0$, $Q_{\alpha+1}/Q_\alpha = K(Q/Q_\alpha)$ and $Q_\alpha = \bigcup Q_\beta$, $\beta < \alpha$, if $\alpha \geqq 1$ is limit. Then both K and L are hereditary preradicals and L is a radical.

For a quasimodule Q, let $S(Q)$ be the subquasimodule generated by all minimal subquasimodules. Further, define $T(Q)$ similarly as $L(Q)$.

For a quasimodule Q, let $B(Q) = 3Q$.

1.2. Lemma. Let P be a subquasimodule of a quasimodule Q such that $P \cap C(Q) = 0$. Then P is primitive and $P \subseteq K(Q)$. Moreover, if P is cyclic then either $P = 0$ or P is isomorphic to Z_3 (the module structure on Z_3 is induced by Φ).

Proof. Obvious.

1.3. Lemma. Let P be a non-zero normal cyclic subquasimodule of a quasimodule Q. Then $P \cap C(Q) \neq 0$ and if P is simple then $P \subseteq C(Q)$.

Proof. Suppose that $P \cap C(Q) = 0$. By 1.2, P contains just three elements, so that $P = \{a, -a, 0\}$. Since $a \notin C(Q)$ and P is normal, $f(a) = a$ for every inner automorphism f of Q (use 1.1). Hence $a \in C(Q)$.

1.4. Lemma. Let Q be a non-associative quasimodule generated by three elements. Then:

(i) $A(Q)$ is isomorphic to the module Z_3.

(ii) card $Q/C(Q) = 27$ and $Q/C(Q)$ is isomorphic to Z_3^3.

(iii) $C(Q) = A(Q) + B(Q)$.

(iv) If $C(Q) \neq B(Q)$ then $Q/B(Q)$ is a free primitive quasimodule of rank 3 and of rank 3 and $A(Q) \cap B(Q) = 0$.

(v) If P is a proper subquasimodule of Q and $C(Q) \subseteq P$ then P is a module.

(vi) If P is a non-associative subquasimodule of Q then $A(Q) \subseteq P$, $Q = P + B(Q)$ and P is a normal subquasimodule.

Proof. (i) If Q is generated by $\{a, b, c\}$ and $d = [a, b, c]$ then Q/Rd is associative and $A(Q) = Rd$.

(ii) $Q/C(Q)$ is not generated by two elements and it is a primitive module generated by three elements.

(iii) Put $P = A(Q) + B(Q)$. Then $P \subseteq C(Q)$, Q/P is a primitive module and card $Q/P \leqq 27$. Hence $P = C(Q)$.

(iv) Since $B(Q) \neq C(Q)$, card $Q/B(Q) = 81$. On the other hand, $Q/B(Q)$ is a homomorphic image of the free primitive quasimodule of rank 3 and this contains just 81 elements.

(v) Obviously, $f(P)$ is a proper submodule of $Q/C(Q)$, f being the natural homomorphism. By (ii), $f(P)$ can be generated by two elements. Since $C(Q) \subseteq C(P)$, P is associative.

(vi) We have $A(Q) \subseteq P$ and P is normal in Q. If $P + B(Q) \neq Q$ then there is a normal subquasimodule V of Q such that $P \subseteq V$ and Q/V is isomorphic to Z_3. Consequently, $A(Q)$ and $B(Q)$ are contained in V and $C(Q) \subseteq V$. By (v), V is a module,

1.5. Lemma. Let Q be an L-torsion quasimodule generated by three elements. Then every proper subquasimodule of Q is a module.

Proof. Use 1.4.

1.6. Lemma. Let Q be a non-associative subdirectly irreducible quasimodule nilpotent of class at most two. Then $A(Q)$ is isomorphic to Z_3 and every proper homomorphic image of Q is a module.

Proof. We have $0 \neq A(Q) \subseteq C(Q)$. Since $A(Q)$ is subdirectly irreducible and primitive, $A(Q)$ is isomorphic to Z_3. The rest is clear.

1.7. Proposition. The following conditions are equivalent for a non-associative L-torsion quasimodule Q:

(i) Q is subdirectly irreducible and it is generated by at most three elements.

(ii) Every proper factorquasimodule as well as every proper subquasimodule of Q is a module.

Proof. Apply 1.4, 1.5 and 1.6.

2. Hamiltonian quasimodules

A quasimodule Q is said to be hamiltonian if every subquasimodule of Q is normal.

2.1. Proposition. Let Q be a hamiltonian quasimodule. Then Q is nilpotent of class at most 2 and $S(Q) \subseteq C(Q)$.

Proof. $S(Q) \subseteq C(Q)$ by 1.3. Further, $A(Q) \subseteq K(Q) \subseteq S(Q) \subseteq C(Q)$, and hence Q is nilpotent of class at most 2.

2.2. Proposition. Let Q be a subdirectly irreducible non-associative hamiltonian quasimodule. Then:

(i) Q is cocyclic and $A(Q) = K(Q) = S(Q)$ is isomorphic to Z_3.

(ii) Every proper homomorphic image of Q is associative.

(iii) If R is commutative and I finitely generated then Q is L-torsion. If, moreover, Q is finitely generated then Q is finite and card $Q = 3^n$ for some $n \geqq 4$.

Proof. (i) and (ii). These assertions are easy.

(iii) $C(Q)$ is a cocyclic module, and hence it is L-torsion. On the other hand, $Q/C(Q)$ is primitive and consequently, Q is L-torsion.

2.3. Proposition. Let Q be a non-associative hamiltonian quasimodule which is generated by at most three elements. Then:

(i) $A(Q)$ is isomorphic to Z_3.

(ii) $C(Q) = B(Q)$ and $Q/C(Q)$ is isomorphic to Z_3^3.

(iii) If Q is L-torsion then every proper subquasimodule of Q is a module.

Proof. Apply 1.4 and 1.5.

2.4. Proposition. Suppose that R is commutative and I is a finitely generated ideal. Let Q be a non-associative hamiltonian quasimodule such that Q is subdirectly irreducible and generated by at most three elements. Then Q is finite, L-torsion card $Q = 3^n$ for some $n \geqq 4$ and every proper factorquasimodule as well as every proper subquasimodule of Q is a module.

Proof. See the previous results.

2.5. Proposition. Suppose that R is commutative, I is finitely generated and there exists a non-associative hamiltonian quasimodule. Then there exists a finite cocyclic L-torsion module M such that M cannot be generated by two elements.

Proof. There exists a non-associative hamiltonian quasimodule $Q' = Q(*, rx)$ such that Q' is subdirectly irreducible, L-torsion, finite and generated by at most three elements. Then there are a module $Q = Q(+, rx)$ with the same underlying set and the same scalar multiplication and a trilinear mapping T of Q^3 into Q such that $T(x, x, y) = 0$, $T(T(x, y, z), u, v) = 0$, $T(u, v, T(x, y, z)) = 0$, $sT(x, y, z) = 0$ and $x * y = x + y + T(x, y, x - y)$ for all $x, y, z, u, v \in Q$ and $s \in I$. If P is a non-zero cyclic submodule of Q then P is also a subquasimodule of Q' and hence $A(Q') \subseteq P$. From this we conclude that Q is cocyclic. Obviously, Q is L-torsion. Finally, since Q' is not associative, $T \neq 0$ and Q is not generated by two elements.

2.6. Proposition. Suppose that I is finitely generated as a left ideal and let there exist a finitely generated cocyclic L-torsion module which is not generated by two elements. Then there exists a non-associative hamiltonian quasimodule.

Proof. Put $F = R \times R \times R \times Z_3$, $a_1 = (1, 0, 0, 0)$, $a_2 = (0, 1, 0, 0)$, $a_3 = (0, 0, 1, 0)$, $a_4 = (0, 0, 0, 1)$ and define a trilinear mapping T of F^3 into F by $T(a_1, a_2, a_3) = a_4$, $T(a_2, a_1, a_3) = -a_4$ and $T(a_i, a_j, a_k) = 0$ otherwise. Further, put $x * y = x + y + T(x, y, x - y)$ for all $x, y \in F$. Then $F' = F(*, rx)$ is a quasimodule, namely the free quasimodule freely generated by a_1, a_2, a_3. Now, let B be a submodule of $N = R \times R \times R$ such that $M = N/B$ is a cocylic L-torsion module and M is not generated by two elements. The rest of the proof is divided into three parts:

(i) We shall show that $B \subseteq I \times I \times I$ and $B \neq IN$. We have $J(M) = (IN + B)/B$, since M is L-torsion; here, J is the Jacobson radical. Consequently,

$M/J\,M)$ is isomorphic to $N/(IN + B)$. Since M cannot be generated by two elements, $N/(IN + B)$ has the same property and we have $IN = IN + B$, so that $B \subseteq IN$. Clearly, $B \neq IN$.

(ii) Let $B \subseteq A \subseteq IN$ be such that A/B is simple (non-zero). There is a surjective module homomorphism f of A onto Z_3 such that $\operatorname{Ker} f = B$. Now, define a subset P of F by $(x_1, x_2, x_3, x_4) \in P$ iff $x = (x_1, x_2, x_3) \in A$ and $x_4 = f(x)$. Obviously, P is a submodule of $IN \times Z_3$, and therefore $P' = P(*)$ is a subquasimodule of F'. Put $Q' = F'/P'$. Then card $Q' = 3$card M.

(iii) We shall prove that Q' is a non-associative L-torsion hamiltonian quasimodule. We have $P \cap Ra_4 = 0$, so that Q' is not associative. Let $x = (x_1, x_2, x_3, x_4) \in F$ be such that $x \notin P$ and put $y = (x_1, x_2, x_3)$. Then either $y \notin A$ or $y \in A$ and $f(y) \neq x_4$. First, assume that $y \notin A$. The module M is cocyclic, finitely generated and L-torsion. Since I is finitely generated as a left ideal, $I^nN \subseteq B$ for some $n \geqq 1$. Clearly, $n \geqq 2$ and if $Iy \subseteq B$ then $I(y + B/B) = 0$, $y + B \in S(M) = A/B$ and $y \in A$, a contradiction. We have $Iy \notin B$ and let $m \geqq 2$ be the least with $I^my \subseteq B$. There is $r \in I^{m-1}$ such that $ry \notin B$. Since $Iry \subseteq B$, $ry \in A$. Moreover, $rx = (ry, 0)$ and let $z = f(ry) \in Ra_4$. Then $(ry, z) \in P$, $rx - z \in P$, and so $r(x + P/P) = (z + P)/P$. However, $z \neq 0$. Finally, let $y \in A$ and $f(y) \neq x_4$. Then $u = (y, f(y)) \in P$ and $x - u = (0, 0, 0, v)$, $v \neq 0$.

2.7. Theorem. Suppose that R is commutative and I is a finitely generated ideal. Then there exists a non-associative hamiltonian quasimodule iff there exists a finite cocyclic L-torsion module which is not generated by two elements.

Proof. Apply 2.5 and 2.6.

2.8. Corollary. Suppose that R is commutative and I/I^2 is a simple module (e.g. I is principal). Then every hamiltonian quasimodule is a module.

2.9. Example. Let $S = Z_9[x, y]$ (the polynomial ring), $J = S(x^6 - 1) + S(y^6 - 1)$ and $R = S/J$. Put $M = Z_9 \times Z_9 \times Z_9$, $f(x_1, x_2, x_3) = (-x_1, 2x_2, -x_3)$ and $g(x_1, x_2, x_3) = (2x_1, -x_2, -x_3)$ for every $(x_1, x_2, x_3) \in M$. Then M is a cocyclic L-torsion R-module (via f and g) and M is not generated by two elements. Since f and g are commuting automorphisms, the same is true for $S = Z_9[x, y, x^{-1}, y^{-1}]$ and $R = S/J$.

3. Trimedial quasigroups

Throughout this section, let $R = Z[\alpha, \beta, \alpha^{-1}, \beta^{-1}]$, α and β being two commuting indeterminates over the ring Z of integers. Then R is a finitely generated integral domain, and hence R is also a commutative noetherian ring. Moreover, there exists a unique homomorphism Φ of R onto Z_3 and we have $\Phi(\alpha) = \Phi(\beta) =$

$= -1$. Clearly, $I = \operatorname{Ker} \Phi = R3 + R(1 + \alpha) + R(1 + \beta)$. Further, we denote by $\mathcal{M}$ the variety of quasimodules and by $\mathcal{M}^c$ the variety of centrally pointed quasimodules, so that a quasimodule Q together with a point $a \in Q$ belongs to $\mathcal{M}^c$ iff $a \in C(Q)$.

A quasigroup Q is said to be trimedial if every subquasigroup of Q generated by at most three elements is medial, i.e. satisfies the identity $xy \, . \, uv = xu \, . \, yv$. Denote by $\mathcal{P}$ the variety of trimedial quasigroups. We are going to prove that the variety $\mathcal{P}^p$ of pointed trimedial quasigroups is equivalent to the variety $\mathcal{M}^c$.

3.1. Lemma. Let $Q(+)$ be a commutative loop and h a mapping of Q into Q. The following conditions are equivalent:

(i) $(x + h(x)) + (y + z) = (x + y) + (h(x) + z)$ for all $x, y, z \in Q$.

(ii) $Q(+)$ is a commutative Moufang loop and $h(x) - x \in C(Q(+))$ for every $x \in Q$.

Proof. (i) implies (ii). As an immediate consequence of (i) we have $(x + h(x)) + y = x + (h(x) + y) = h(x) + (x + y)$ for all $x, y \in Q$. Hence $(x + h(x)) + (y + z) = x + (h(x) + (y + z)) = h(x) + (x + (y + z)) = (x + y) + (h(x) + z)$ for all $x, y, z \in Q$. In particular, $h(x) + (x + (z - x)) = h(x) + z$ (we put $y = -x$), $x + (z - x) = z$ and we see that $Q(+)$ is an IP-loop. Further $(x + y) + (h(x) + (z - y)) = (x + h(x)) + z$, $h(x) + (z - y) = ((x + h(x)) + z) + (-x - y)$, $-h(x) + (y - z) = ((-x - h(x)) - z) + (x + y)$, and hence $(x + y) + ((-x - h(x)) + z) = -h(x) + (y + z)$ for all $x, y, z \in Q$. On the other hand $x + (h(x) + ((-x - h(x)) + z)) = (x + h(x)) + ((-x - h(x)) + z) = z$, $h(x) + ((-x - h(x)) + z) = z - x$, and therefore $(x + (x + y)) + (z - x) = (x + h(x)) + ((x + y) + ((-x - h(x)) + z)) = (x + h(x)) + (-h(x) + (y + z)) = x + (y + z)$, i.e. $(x + (x + y)) + z = x + (y + (x + z))$ for all $x, y, z \in Q$. From this, $(x + x) + z = x + (x + z)$ and we have $(x + y) + (x + z) = (x + (x + (y - x)) + (x + z) = x + ((y - x) + ((x + x) + z)) = x + (x + (z + y)) = (x + x) + (y + z)$, so that $Q(+)$ is a commutative Moufang loop. Finally, $h(x) + ((y + z) - x) = (-x + x + h(x)) + ((y + z) - x) = -2x + ((x + h(x)) + (y + z)) = -2x + ((x + y) + (h(x) + z) = y + (-x + (h(x) + z))$, hence $h(x) + (y - x) = y + (h(x) - x)$, $(h(x) - x) + (y + z) = h(x) + ((y + z) - x) = y + (-x + (h(x) + z))$, $(h(x) - x) + z = -x + (h(x) + z)$, $(h(x) - x) + (y + z) = y + (z + (h(x) - x))$ and $h(x) - x \in C(Q(+))$.

(ii) implies (i). We have $(x - h(x)) + ((x + y) + (h(x) + z)) = (x + y) + (x + z) = (x + x) + (y + z) = (x - h(x)) + ((x + h(x) + (y + z))$ for all $x, y, z \in Q$.

Let Q be a quasigroup. A quadruple $(Q(+), f, g, a)$ is said to be an arithmetical form of Q if $Q(+)$ is a commutative Moufang loop defined on the same underlying set, f and g are commuting 1-central automorphisms of $Q(+)$ (i.e. $x + f(x)$, $x + g(x) \in C(Q(+)))$, a is an element from $C(Q(+))$ and, finally, $xy = f(x) + g(y) + a$ for all $x, y \in Q$.

3.2. Lemma. Let $(Q(+), f, g, a)$ and $(Q(*), p, q, b)$ be arithmetical forms of the same quasigroup Q. Suppose that the loops $Q(+)$ and $Q(*)$ have the same zero element 0. Then $Q(+) = Q(*)$, $f = p$, $g = q$ and $a = b$.

Proof. We have $f(x) + g(y) + a = p(x) * q(y) * b$ for all $x, y \in Q$. Hence $a = b$, $g(y) + a = q(y) * a$, $f(x) + z = p(x) * z$, $f = p$, $+ = *$ and $g = q$.

3.3. Lemma. Let Q be a quasigroup having an arithmetical from $(Q(+), f, g, a)$ and let $u \in Q$. Then there is an arithmetical form $(Q(*), p, q, b)$ of Q such that u is the neutral element of $Q(*)$.

Proof. Put $v = -u$ and $x * y = (x + y) + v$ for all $x, y \in Q$. Then $Q(*)$ is a loop and u is the neutral element of $Q(*)$. Moreover, the mapping $h: x \to x + v$ is an isomorphism of $Q(*)$ onto $Q(+)$; we have $h^{-1}(x) = x + u$. Further, $p(x) = h^{-1}f\, h(x) = (f(x) + f(v)) + u$, $q(x) = h^{-1}g\, h(x) = (g(x) + g(v)) + u$ and both p and q are 1-central automorphisms of $Q(*)$. Now, put $c = a + 3v + (u - f(v)) + (u - g(v))$ and $b = c + u$. Then $b, c \in C(Q(*))$ and $p(x) * q(y) * b = (((((f(x) + f(v)) + u) + ((g(y) + g(v)) + u)) + v) + (c + u)) + v = f(x) + g(y) + a = xy$.

3.4. Lemma. Let $(Q(+), f, g, a)$ and $(P(+), p, q, b)$ be arithmetical forms of quasigroups Q and P, resp. Let h be a mapping of Q into P such that $h(0) = 0$. Then h is a homomorphism of the quasigroups iff h is a homomorphism of the commutative Moufang loops, $hf = ph$, $hg = qh$ and $h(a) = b$.

Proof. Clearly, h is a homomorphism of the quasigroups iff $h(f(x) + g(y) + a) = ph(x) + qh(y) + b$ for all $x, y \in Q$. This equality implies $h(a) = b$, $hf(x) = ph(x) + qhg^{-1}(-a) + b$, $qhg^{-1}(-a) + b = 0$, $hf = ph$, $hg = qh$, $h(x + y + a) = h(x) + h(y) + h(a)$, $h(y + a) = h(y) + h(a)$, $h(x + z) = h(x) + h(z)$. The rest is clear.

3.5. Lemma. Let Q be a quasigroup having an arithmetical form. Then Q is trimedial.

Proof. Let $b, c, d \in Q$. By 3.3, there is an arithmetical form $(Q(+), f, g, a)$ of Q such that $b = 0$. Denote by $P(+)$ the subloop of $Q(+)$ generated by $\{c, d\} \cup C(Q(+))$. Then $P(+)$ is an abelian group, $a \in P$ and $f(P) = P = g(P)$. Consequently, P is a subquasigroup of Q and P is medial.

Let Q be a quasigroup and $a, b \in Q$. Put $R_a(x) = xa$ and $L_b(x) = bx$ for all $x, y \in Q$. Then R_a, L_b are permutations of Q.

3.6. Lemma. Let Q be a trimedial quasigroup, $a, b \in Q$ and $x + y = R_a^{-1}(x)\, L_b^{-1}(y)$ for all $x, y \in Q$. Then:

(i) $Q(+)$ is a loop and $ba = 0$.

(ii) $Q(+)$ is commutative iff $bx \,.\, ya = by \,.\, xa$ for all $x, y \in Q$.

(iii) If both a and b belong to the subquasigroup generated by an element c then $Q(+)$ is commutative.

(iv) If $Q(+)$ is commutative and $R_a L_b = L_b R_a$ then $Q(+)$ is a commutative Moufang loop.

Proof. (i) This is obvious.

(ii) We have $(x + y)(aa) = xL_b^{-1}(y)\, a$, $(y + x)(aa) = yL_b^{-1}(x)\, a$. Hence $x + y = y + x$ for all $x, y \in Q$ iff $bx \,.\, ya = by \,.\, xa$.

(iii) This is an immediate consequence of (ii).

(iv) Let $r, s \in Q$ be such that $rb = v$ and $as = a$. Put $h = L_r R_a^{-1}$. We have $(h(x)\, h(x))\,(yz) = (h(x)\, y)\,(h(x)\, z)$ for all $x, y, z \in Q$. But $h(x)\, h(x) = (rR_a^{-1}(x))\,.\,(bL_b^{-1}h(x)) = b(R_a^{-1}(x)\, L_b^{-1}h(x))$, $yz = (R_a^{-1}(y)\, R_s^{-1}(z))\, a$, $h(x)\, y = b(R_a^{-1}(x)\,.\,L_b^{-1}(y))$ and $h(x)\, z = (R_a^{-1}h(x)\, R_s^{-1}(z))\, a$. Consequently, $L_b(x + h(x))\, R_a(y + z) = L_b(x + y)\, R_a(h(x)) + z)$ for all $x, y, z \in Q$. But $L_{bb}(xy) = L_b(x)\, L_b(y)$, hence $L_{bb}^{-1}(xy) = L_b^{-1}(x)\, L_b^{-1}(y)$ for all $x, y \in Q$. Similarly, $R_{aa}^{-1}(xy) = R_a^{-1}(x)\, R_a^{-1}(y)$. Now, $(x + h(x)) + (y + z) = R_a^{-1}(x + h(x))\, L_b^{-1}(y + z) = L_{bb}^{-1} R_{aa}^{-1}(L_b(x + h(x))\,.\,R_a(y + z) = L_{bb}^{-1} R_{aa}^{-1}(L_b(x + y)\, R_a(h(x) + z)) = R_a^{-1}(x + y)\, L_b^{-1}(h(x) + z) = (x + y) + (h(x) + z)$ for all $x, y, z \in Q$. By 3.1, $Q(+)$ is a commutative Moufang loop.

3.7. Lemma. Let Q be a trimedial quasigroup and let $a, b, c, d \in Q$ be such that $ba = a = ac$ and $bd = b$. Then $dc = c$, $R_c L_c = L_b R_c$ and the elements b, c belong to the subquasigroup generated by a.

Proof. We have $a \,.\, dc = ba \,.\, dc = bd \,.\, ac = ba = a = ac$, so that $dc = c$. On the other hand, $bx \,.\, c = bx \,.\, dc = bd \,.\, xc = b \,.\, xc$ for every $x \in Q$.

3.8. Lemma. Let Q be a trimedial quasigroup. Then every loop isotopic to Q is a Moufang loop.

Proof. By 3.7, 3.6(iii), (iv), Q is isotopic to a commutative Moufang loop. However, as it is well known, the class of Moufang loops is closed under isotopy.

3.9. Lemma. Let Q be a trimedial quasigroup. Then Q has an arithmetical form.

Proof. Let $u, v \in Q$ be such that $Q(+)$ is commutative where $x + y = R_u^{-1}(x)\,.\,L_v^{-1}(y)$ for all $x, y \in Q$ (see 3.6(ii), (iii)). By 3.8, $Q(+)$ is a commutative Moufang loop and we have $xy = p(x) + q(y)$, $p = R_u$, $q = L_v$. Now, $p(p(x) + q(x)) + q(p(y) + q(z)) = xx \,.\, yz = xy \,.\, xz = p(p(x) + q(y)) + q(p(x) + q(z))$, so that $p(x + qp^{-1}(x)) + q(y + z) = p(x + qp^{-1}(y)) = q(x + z)$ for all $x, y, z \in Q$. Consequently, $b + q(y + z) = pqp^{-1}(y) + q(z)$, $b = pqp^{-1}(0)$. Further, $(b + q(y)) - c = pqp^{-1}(y)$, $c = q(0)$, and $b + q(y + z) = ((b + q(y)) - c) + q(z)$ for all $y, z \in Q$. But $q(y + z) = q(z + y)$, so that $((b + y) - c) + z = ((b + z) - c) + y$,

$(b + y) - c = (b - c) + y$, $((b - c) + y) + z = ((b - c) + z) + y$ and $b - c \in C(Q(+))$. Then $c + q(y + z) = (c - b) + (b + q(y + z)) = (c - b) + ((b - c) + q(y)) + q(z) = q(y) + q(z)$ and the mapping g, $g(x) = q(x) - c$ is an automorphism of $Q(+)$. Dually, the mapping f, $f(x) = p(x) - d$, $d = p(0)$ is an automorphism of $Q(+)$. Now, $xy = p(x) + q(y) = (f(x) + d) + (g(y) + c)$ for all $x, y \in Q$. In the rest of the proof, let $u = v = ww$ for some $w \in Q$. Put $h = R_u L_u^{-1}$. We have $h(x + y) = R_u L_u^{-1}(R_u^{-1}(x) L_u^{-1}(y)) = R_u(L_w^{-1} R_u^{-1}(x) L_w^{-1} L_u^{-1}(y)) = R_u(R_w^{-1} L_w^{-1}(x) L_w^{-1} L_u^{-1}(y)) = R_w R_w^{-1} L_u^{-1}(x) R_w L_w^{-1} L_u^{-1}(y) = L_u^{-1}(x) R_w L_w^{-1} L_u^{-1}(y) = R_u^{-1} R_u L_u^{-1}(x) L_u^{-1} R_u L_u^{-1}(y) = h(x) + h(y)$ for all $x, y \in Q$; take into account that $u \,.\, xw = ww \,.\, xw = wx \,.\, ww = wx \,.\, u$, $L_w^{-1} R_u^{-1}(x) = R_w^{-1} L_u^{-1}(x)$ and $R_u L_u^{-1}(x) = R_w L_w^{-1}(x)$ for every $x \in Q$. We have proved that h is an automorphism of the loop $Q(+)$. Further, $(h(x) + x) + (y + z) = R_u^{-1}(R_u^{-1} h(x) L_u^{-1}(x)) \,.\, L_u^{-1}(R_u^{-1}(y) L_u^{-1}(z)) = (R_w^{-1} L_u^{-1}(x) R_w^{-1} L_u^{-1}(x)) (L_w^{-1} R_u^{-1}(y) L_w^{-1} L_u^{-1}(z)) = (R_w^{-1} R_u^{-1}(x) R_w^{-1} L_u^{-1}(y)) (R_w^{-1} L_u^{-1}(x) L_w^{-1} L_u^{-1}(z)) = (R_w^{-1} R_u^{-1} h(x) R_w^{-1} L_u^{-1}(y)) \,.\, (L_w^{-1} R_u^{-1}(x) L_w^{-1} L_u^{-1}(z)) = R_u^{-1}(R_u^{-1} h(x) L_u^{-1}(y)) L_u^{-1}(R_u^{-1}(x) L_u^{-1}(z)) = (h(x) + y) + (x + z)$. By 3.1, $h(x) - x \in C(Q(+))$. Now, we have $h(c) = pq^{-1} q(0) = p(0) = d$, and so $xy = (f(x) + d) + (g(y) + c) = (f(x) + h(c)) + (g(y) + c) = (f(x) + g(y)) + a$, $a = c + h(c)$, for all $x, y \in Q$. Further, $(g f(x) + f(a)) + a = (f((f(0) + g(0)) + a) + g((f(x) + gg^{-1}(-a)) + a)) + a = 00 \,.\, xg^{-1}(-a) = 0x \,.\, 0g^{-1}(-a) = (f((f(0) + g(x)) + a) + g((f(0) + gg^{-1}(-a)) + a)) + a = (f g(x) + f(a)) + a$, so that $fg = gf$. Further, $h(x) = R_u L_u^{-1}(x) = pq^{-1}(x) = (fg^{-1}(x) - fg^{-1}(c)) + d$, $h(0) = d - fg^{-1}(c) \in C(Q(+))$, and hence $fg^{-1}(x) - x \in C(Q(+))$ for every $x \in Q$. Consequently, $f(x) - g(x) \in C(Q(+))$. Now, the equality $(xx \,.\, x)(yz) = (xx \,.\, y)(xz)$ for all $x, y, z \in Q$, yields $((((f^2 g^{-1}(x) + f(x)) + f^2(a)) + x) + f(a)) + ((y + z) + g(a)) = ((((f^2 g^{-1}(x) + f(x)) + f^2(a)) + y) + f(a)) + ((x + z) + g(a))$ for all $x, y, z \in Q$. But $f(x) - f^2 g^{-1}(x) \in C(Q(+))$ and $3 f(x) \in C(Q(+))$. Hence we have $m = n$ where $m = (((-f(x) + f^2(a)) + x) + f(a)) + ((y + z) + g(a))$ and $n = (((-f(x) + f^2(a)) + y) + f(a)) + (x + z) + g(a))$. Further, $f(a) - g(a) \in C(Q(+))$ and from the equality $m + f(a) - g(a) = n + f(a) - g(a)$ we get $((-f(x) + f^2(a)) + x) + (y + z) = ((-f(x) + f^2(a)) + y) + (x + z)$. Now, by 3.1, the element $-x + (-f(x) + f^2(a))$ is contained in $C(Q(+))$ for every $x \in Q$. We have proved that f is 1-central. Similarly, using the equality $(yz)(x \,.\, xx) = (yx)(z \,.\, xx)$, we can show that g is 1-central.

3.10. Theorem. The varieties $\mathscr{P}^p$ of pointed trimedial quasigroups and $\mathscr{M}^c$ of centrally pointed quasimodules are equivalent.

Proof. Apply the preceding results.

4. Hamiltonian trimedial quasigroups

A quasigroup Q is called hamiltonian if every subquasigroup of Q is normal.

4.1. Proposition. Let Q be a trimedial quasigroup and Q' the corresponding quasimodule.

(i) If Q' is hamiltonian then Q is hamiltonian.

(ii) If Q contains at least one idempotent and is hamiltonian then Q' is hamiltonian.

Proof. (i) Let P be a subquasigroup of Q and let $b \in P$. Let (Q'', a) be the centrally pointed quasimodule corresponding to (Q, b), so that $b = 0$. Then P is a subquasimodule of Q'', P is a normal subquasimodule (Q'' is isomorphic to Q') and P is a normal subquasigroup of Q.

(ii) Let $b \in Q$ be such that $bb = b$ and let (Q'', a) be the centrally pointed quasimodule corresponding to (Q, b). Let P be a subquasimodule of Q''. We have $a = bb = b = 0$, $a \in P$, P is a subquasigroup of Q and P is normal. Hence P is a normal subquasimodule.

4.2. Proposition. Let Q be a trimedial quasigroup such that Q is subdirectly irreducible and nilpotent of class at most two. Let P be a subquasigroup of Q and suppose that P is not idempotent. Then P is a normal subquasigroup.

Proof. By 3.3, Q has an arithmetical form $(Q(+), f, g, a)$ such that $0 \neq a \in P$ and $0 \in P$. Then P is a subloop of $Q(+)$ and the intersection $P \cap C(Q(+))$ is non-trivial. Consequently, the centre is contained in P and P is normal.

4.3. Corollary. Let Q be a trimedial quasigroup with 81 elements such that Q contains no idempotent. Then Q is hamiltonian.