Aleš Drápal; Tomáš Kepka; Petr Maršálek

Multiplication groups of quasigroups and loops II.

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 35 (1994), No. 1, 9--29

Persistent URL: http://dml.cz/dmlcz/142660

Multiplication Groups of Quasigroups and Loops II.

ALEŠ DRÁPAL, TOMÁŠ KEPKA and PETR MARŠÁLEK*)

MFF UK Praha

Received 10. October 1993

Basic properties of permutation groups generated by left and right translations of quasigroups and loops are collected.

Základní vlastnosti permutačních grup generovaných levými a pravými translacemi kvazigrup a lup jsou sebrány.

1. Multiplication groups – first observations

1.1 A groupoid is a non-empty set supplied with a binary operation. This operation is usually denoted multiplicatively, i.e. by . or juxtaposition.

Let G be a groupoid. For each $a \in Q$, we have two transformations $\mathscr{L}(G, a)$ and $\mathscr{R}(G, a)$ of G defined by $\mathscr{L}(G, a)(x) = ax$ and $\mathscr{R}(G, a)(x) = xa$, resp. The transformation $\mathscr{L}(G, a)$ $(\mathscr{R}(G, a))$is called the left (right) translation by a (of G) and will be also denoted by $\mathscr{L}(a)$ $(\mathscr{R}(a))$ when G is clear from the context.

A groupoid is called a quasigroup if all the translations are permutations (i.e. bijective transformations).

A loop is a quasigroup possesing a neutral element.

1.2 Let Q be a quasigroup. The subgroup $\mathscr{M}_l(Q) = \langle \mathscr{L}(a); a \in Q \rangle$ generated by all the left translations (in the group $\mathscr{S}(Q)$ of all permutations of Q) is called the left multiplication group of Q. Similarly $\mathscr{M}_r(Q) = \langle \mathscr{R}(a); a \in Q \rangle$ is the right multiplication group and $\mathscr{M}(Q) = \langle \mathscr{R}(a), \mathscr{L}(a); a \in Q \rangle = \langle \mathscr{M}_l(Q) \cup \mathscr{M}_r(Q) \rangle$ is the multiplication group of Q.

For $a \in Q$, the stabilizer $\mathscr{I}_l(Q, a) = \mathrm{St}(\mathscr{M}_l(Q), Q, a) = \{f \in \mathscr{M}_l(Q); f(a) = a\}$ is called the left inner permutation group (with respect to a). Similarly $\mathscr{I}_r(Q, a) =$

*) Department of Mathematics, Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic

$= \mathrm{St}(\mathcal{M}_r(Q), Q, a)$ is the right inner permutation group and $\mathcal{I}(Q, a) = \mathrm{St}(\mathcal{M}(Q), Q, a)$ is the inner permutation group (with respect to a). If Q is a loop, then $\mathcal{I}(Q) = \mathcal{I}(Q, 1)$ is called the inner permutation group of Q.

1.3 In the rest of this section, let Q be a quasigroup, $S = \mathcal{S}(Q)$, $G_l = \mathcal{M}_l(Q)$, $G_r = \mathcal{M}_r(Q)$, $G = \mathcal{M}(Q)$, $H_l(a) = \mathcal{I}_l(Q, a)$, $H_r(a) = \mathcal{I}_r(Q, a)$, and $H(a) = \mathcal{I}(Q, a)$.

1.4 Observation. (i) *The permutation group G (G_l, G_r) is transitive on Q and consequently the stabilizers $H(a)$ $(H_l(a), H_r(a))$, $a \in Q$, are conjugate in G (G_l, G_r). In particular, the stabilizers are isomorphic.*

(ii) $\bigcap_{a \in Q} H(a) = 1$ $\left(\bigcap_{a \in Q} H_l(a) = 1, \bigcap_{a \in Q} H_r(a) = 1\right)$.

(iii) $\mathbf{L}_G(H(A)) = 1$ $(\mathbf{L}_{G_l}(H_l(A)) = 1, \mathbf{L}_{G_r}(H_r(A)) = 1)$ *(here, $\mathbf{L}_G(K)$ denotes the core of a subgroup K in G).*

(iv) $\langle \bigcup H(a); a \in Q \rangle$ $(\langle \bigcup H_l(a); a \in Q \rangle, \langle \bigcup H_r(a); a \in Q \rangle)$ *is normal in G (G_l, G_r).*

(v) $\mathrm{card}(G) = \mathrm{card}(Q) \cdot \mathrm{i}(Q)$ $(\mathrm{card}(G_l) = \mathrm{card}(Q) \cdot \mathrm{i}_l(Q), \mathrm{card}(G_r) = \mathrm{card}(Q) \cdot \mathrm{i}_r(Q))$, *where* $\mathrm{i}(Q) = \mathrm{card}(H(a))$ $(\mathrm{i}_l(Q) = \mathrm{card}(H_l(a)), \mathrm{i}_r(Q) = \mathrm{card}(H_r(a)))$.

(vi) $\mathrm{i}_l(Q) \leqq \mathrm{i}(Q)$ *and* $\mathrm{i}_r(Q) \leqq \mathrm{i}(Q)$, *moreover, both* $\mathrm{i}_l(Q)$ *and* $\mathrm{i}_r(Q)$ *divide* $\mathrm{i}(Q)$, *provided that* $\mathrm{i}(Q)$ *is finite.*

1.5 Observation. (i) $\mathbf{Z}(G_l) \subseteqq \mathbf{C}_S(G_l) = \{f \in S;\ f = \mathcal{R}(f(a))\, \mathcal{R}(a)^{-1}$ *for each* $a \in Q\} \subseteqq G_r$ *(here, $\mathbf{Z}(K)$ is the centre of K and $\mathbf{C}_S(K)$ is the centralizer of K for a subgroup K of S).*

(ii) $\mathbf{Z}(G_r) \subseteqq \mathbf{C}_S(G_r) = \{f \in S;\ f = \mathcal{L}(f(a))\, \mathcal{L}(a)^{-1}$ *for each* $a \in Q\} \subseteqq G_l$.

(iii) $\mathbf{Z}(G) = \mathbf{C}_S(G) \subseteqq G_l \cap G_r$.

(iv) $\mathbf{Z}(G) = \mathbf{Z}(G_l) \cap \mathbf{Z}(G_r)$.

(v) $\mathbf{Z}(G_l) \cup \mathbf{Z}(G_r) \subseteqq G_l \cap G_r$.

(vi) *If Q is a loop, then* $\mathbf{Z}(G) = \{\mathcal{L}(a);\ a \in \mathbf{Z}(Q)\} = \{\mathcal{R}(a);\ a \in \mathbf{Z}(Q)\}$; *in particular, the groups $\mathbf{Z}(G)$ and $\mathbf{Z}(Q)$ are isomorphic.*

(vii) *Every automorphism of Q is contained in each of the normalizers* $\mathbf{N}_S(G)$, $\mathbf{N}_S(G_l)$, $\mathbf{N}_S(G_r)$.

(viii) *Suppose that Q is a loop and that the automorphism group of Q is transitive on $Q - \{1\}$. Then each of the normalizers* $\mathbf{N}_S(G)$, $\mathbf{N}_S(G_l)$, $\mathbf{N}_S(G_r)$ *is 2-transitive on Q.*

1.6 Observation. *Put* $A = \{\mathcal{L}(a);\ a \in Q\}$ *and* $B = \{\mathcal{R}(a);\ a \in Q\}$.

(i) *The set A is a transversal to each of the subgroups $H_l(a)$ in G_l, i.e. A is a stable transversal.*

(ii) *The set B is a stable transversal to each of the subgroups $H_r(a)$ in G_r.*

(iii) *Both A and B are stable transversals to each of the subgroups $H(a)$ in G. Moreover, A, B are $H(a)$-semiconnected transversals* (see I.4.1).

(iv) *If Q is a loop, then A and B are $H(1)$-connected, i.e. the mutual commutator* $[A, B]$ *is contained in* $H(1)$.

1.7 Observation. (i) *The following conditions are equivalent:*

(a) $i_l(Q) = 1$ ($i_r(Q) = 1$).

(b) G_l (G_r) *is a regular permutation group.*

(c) $G_l = A$ ($G_r = B$).

(d) Q *is a left (right) loop isotopic to a group.*

(e) *There exist a group* $Q(+)$ *(possibly non-commutative) and* $f \in S$ *such that* $f(0) = 0$ *and* $xy = f(x) + y$ ($xy = x + f(y)$) *for all* $x, y \in Q$.

(ii) *The following conditions are equivalent:*

(a) $i_l(Q) = 1 = i_r(Q)$.

(b) *Both* G_l *and* G_r *are regular permutation groups.*

(c) $G_l = A$ *and* $G_r = B$.

(d) Q *is a group.*

In this case, the groups Q, G_l, G_r are isomorphic and G is isomorphic to the factorgroup $(Q \times Q)/K$, $K = \{(a,a); a \in \mathbf{Z}Q\}$. Moreover, $H(1)$ is isomorphic to $Q/\mathbf{Z}(Q)$.

(iii) *The following conditions are equivalent:*

(a) $i(Q) = 1$.

(b) G *is regular permutation group.*

(c) Q *is an abelian group.*

In this case, the groups Q and $G = G_l = G_r$ are isomorphic.

1.8 Let r be a binary relation defined on Q. Then r is called

- left (right) stable if $(a, b) \in r$ implies $(xa, xb) \in r$ $((ax, bx) \in r)$ for every $x \in Q$;
- stable if it is both left and right stable;
- left (right) cancellative if $(ca, cb) \in r$ $((ac, bc) \in r)$ implies $(a, b) \in r$;
- cancellative if it is both left and right cancellative.

Clearly, a congruence of Q (i.e. a stable equivalence) is cancellative iff the corresponding factorgroupoid is again a quasigroup.

1.9 Observation (i) *Let* N *be a normal subgroup of* G_l (G_r). *Define a relation* r *on* Q *by* $(a, b) \in r$ *iff* $b = f(a)$ *for some* $f \in N$. *Then* r *is left (right) cancellative left (right) stable equivalence on* Q. *Moreover,* $r = \mathrm{id}_Q$ *iff* $N = 1$ *and* $r = Q \times Q$ *iff* N *is transitive on* Q.

(ii) *Let* r *be left (right) cancellative left (right) stable equivalence defined on* Q. *Then* $N = \{f \in G_l\ (f \in G_r); (x; f(x)) \in r$ *for each* $x \in Q\}$ *is a normal subgroup of* G_l (G_r). *Moreover,* $N = G_l$ ($N = G_r$) *iff* $r = Q \times Q$.

(iii) *The permutation group* G_l (G_r) *is primitive iff* id_Q *and* $Q \times Q$ *are the only left (right) cancellative left (right) stable equivalences on* Q.

1.10 Observation. *Let* $\mathcal{N}$ *denote the lattice of normal subgroup of* G *and* $\mathcal{C}$ *the lattice of cancellative congruences of the quasigroup* Q.

(i) *For every* $N \in \mathscr{N}$, $r = \Phi(N)$ *defined by* $(a, b) \in r$ *iff* $a, b \in Q$ *and* $b = f(a)$ *for some* $f \in N$ *is a cancellative congruence of* Q.

(ii) *for every* $r \in \mathscr{C}$, $N = \Psi(r) = \{f \in G;\ (x, f(x)) \in r$ *for each* $x \in Q\}$ *is a normal subgroup of* G.

(iii) $\Phi(N) = \mathrm{id}_Q$ *iff* $N = 1$ *and* $\Phi(N) = Q \times Q$ *iff* N *is transitive on* Q.

(iv) $\Psi(r) = 1$ *iff* $r = \mathrm{id}_Q$ *and* $\Psi(r) = G$ *iff* $r = Q \times Q$.

(v) *If* $N, M \in \mathscr{N}$ *and* $N \subseteq M$, *then* $\Phi(N) \subseteq \Phi(M)$.

(vi) *If* $r, s \in \mathscr{C}$ *and* $r \subseteq s$, *then* $\Psi(r) \subseteq \Psi(s)$.

(vii) *Let* $N \in \mathscr{N}$ *and* $g \in G$. *Then* $g \in \Psi\Phi(N)$ *iff for every* $x \in Q$ *there is* $f \in N$ *with* $g(x) = f(x)$; *in particular,* $N \subseteq \Psi\Phi(N)$.

(viii) *Let* $r \in \mathscr{C}$ *and* $a, b \in Q$. *Then* $(a, b) \in \Phi\Psi(r)$ *iff* $b = g(a)$ *for some* $g \in G$ *such that* $(x, g(x)) \in r$ *for every* $x \in Q$; *in particular,* $\Phi\Psi(r) \subseteq r$.

(ix) *If* $N, M \in \mathscr{N}$, *then* $\Phi(N, M) = \Phi(N)\,\Phi(M)$ *and* $\Phi(N \cap M) \subseteq \Phi(N) \cap \Psi(M)$.

(x) *If* $r, s \in \mathscr{C}$, *then* $\Psi(r)\,\Psi(s) \subseteq \Psi(rs)$ *and* $\Psi(r \cap s) = \Psi(r) \cap \Psi(s)$.

1.11 Proposition. *Let* $N \in \mathscr{N}$ *and* $M = \Psi\Phi(N)$. *Then:*

(i) *For each* $a \in Q$, $M = \mathbf{L}_G(NH(a)) = NK$, *where* $K = \{f \in H(a);\ g^{-1}fg \in NH(a)$ *for each* $g \in G\}$.

(ii) $M = \bigcap_{a \in Q} NH(a)$.

(iii) $\Psi\Phi(M) = M$.

Proof. The assertions follow easily from 1.10(vii).

1.12 Proposition. (i) $\Psi\Phi = \mathrm{id}_{\mathscr{C}}$.

(ii) *The mapping* Φ: $\mathscr{N} \to \mathscr{C}$ *is projective.*

(iii) *The mapping* Ψ: $\mathscr{C} \to \mathscr{N}$ *is injective.*

Proof. Let $r \in \mathscr{C}$ and $s = \Phi\Psi(r)$. By 1.10(viii), $s \subseteq r$. Now, let $(a, b) \in r$. Then $(x, \mathscr{L}(a)^{-1}\,\mathscr{L}(b)\,(x)) \in r$ for every $x \in Q$ (since r is cancellative), and hence $(a, \mathscr{L}(a)^{-1}\,\mathscr{L}(b)\,(a)) \in s$ by 1.10(viii). However, s is a cancellative congruence of Q and consequently $(aa, ba) \in s$ and $(a, b) \in s$. We have proved that $r = s$.

1.13 Observation. *Let* $r \in \mathscr{C}$, $P = Q/r$ *(i.e.,* P *is the factorquasigroup of* Q *by* r*) and let* ψ: $Q \to P$ *denote the natural projection.*

(i) *Put* $N = \Psi(r)$. *Then* $\Psi\Phi(N) = \Psi\Phi\Psi(r) = \Psi(r) = N$. *Hence also* $N = \mathbf{L}_G(NH(a))$ *for each* $a \in Q$ *and* $N = \bigcap_{a \in Q} NH(a)$ *(see 1.11 and 1.12).*

(ii) *There exists a projective homomorphism* φ: $G \to \mathscr{M}(P)$ *such that* $\mathrm{Ker}(\varphi) = N$ *and* $\varphi(\mathscr{L}(Q, a)) = \mathscr{L}(P, \psi(a))$, $\varphi(\mathscr{R}(Q, a)) = \mathscr{R}(P, \psi(a))$ *for every* $A \in Q$. *In particular, the groups* $\mathscr{M}(P)$ *and* G/N *are isomorphic. Moreover,* $\varphi(G_l) = \mathscr{M}_l(P) \cong$ $\cong G_l/G_l \cap N \cong G_lN/N$ *and* $\varphi(G_r) = \mathscr{M}_r(P) \cong G_r/G_r \cap N \cong G_rN/N$.

1.14 Observation. *The permutation group G is primitive iff the quasigroup Q is c-simple (i.e., id_Q and $Q \times Q$ are the only cancellative congruences of Q).*

1.15 Observation. *Let P be a subquasigroup of Q, $K_l = \langle \mathscr{L}(Q,a);\ a \in P \rangle \subseteqq G_l$, $K_r = \langle \mathscr{R}(Q,a);\ a \in P \rangle \subseteqq G_r$ and $K = \langle K_r \cup K_l \rangle \subseteqq G$. Then there exists a projective homomorphism $\varphi\colon K \to \mathscr{M}(P)$ such that $\varphi(f) = f|P$ for each $f \in K$. Moreover, $\varphi(K_l) = \mathscr{M}_l(P)$, $\varphi(K_r) = \mathscr{M}_r(P)$ and $\mathrm{Ker}(\varphi) = \bigcap_{a \in P} H(a) \cap K$.*

1.16 Observation. *Suppose that $Q = \Pi Q_i$, where Q_i, $i \in I$, is a non-empty system of quasigroups. Then there exists an injective homomorphism $\varphi\colon \Pi \mathscr{M}(Q_i) \to S$ such that $\varphi(\Pi f_i) = \Pi f_i$, $f_i \in \mathscr{M}(Q_i)$. Moreover, $G \subseteqq \mathrm{Im}(\varphi)$, $G_l \subseteqq \varphi(\Pi \mathscr{M}_l(Q_i))$ and $G_r \subseteqq \varphi(\Pi \mathscr{M}_r(Q_i))$.*

1.17 Observation. (i) *The following conditions are equivalent:*

(a) *G_l is abelian.*

(b) *Q is left permutable (i.e., $x \cdot yz = y \cdot xz$ for all $x, y, z \in Q$).*

(c) *There exists an abelian group $Q(+)$ and $f \in S$ such that $f(0) = 0$ and $xy = f(x) + y$ for all $x, y \in Q$. In this case, $\mathrm{i}_l(Q) = 1$ (see 1.7(i)).*

(ii) *The following conditions are equivalent:*

(a) *G_r is abelian.*

(b) *Q is right permutable (i.e., $x \cdot yz = y \cdot xz$ for all $x, y, z \in Q$).*

(c) *There exists an abelian group $Q(+)$ and $f \in S$ such that $f(0) = 0$ and $xy = x + f(y)$ for all $x, y \in Q$. In this case, $\mathrm{i}_r(Q) = 1$ (see 1.7(i)).*

(iii) *The following conditions are equivalent:*

(a) *Both G_r and G_l are abelian.*

(b) *G is abelian.*

(c) *G is regular.*

(d) $\mathrm{i}(Q) = 1$.

(e) *Q is an abelian group.*

(f) *$H(a)$ is normal in G.*

1.18 Proposition. *If Q is non-trivial and the multiplication group G is simple, then, for each $a \in Q$, $H(a)$ is a maximal subgroup of G.*

Proof. The result follows from 1.6(iii) and I.3.13.

2. Inner permutation groups

2.1 This section is an immediate continuation of the preceding one.

For $a, x, y \in Q$, let $\mathscr{L}(x, y, a) = \mathscr{L}(Q, x, y, a) = \mathscr{L}(y)^{-1}\ \mathscr{L}(x)^{-1}\ \mathscr{L}(v)$, $v = \mathscr{R}(a)^{-1}(x \cdot ya)$, $\mathscr{R}(x, y, a) = \mathscr{R}(Q, x, y, a) = \mathscr{R}(y)^{-1}\ \mathscr{R}(x)^{-1}\ \mathscr{R}(w)$, $w = \mathscr{L}(a)^{-1}(ax \cdot x)$

and $\mathscr{T}(x,a)=\mathscr{T}(Q,x,a)=\mathscr{L}(x)^{-1}\mathscr{R}(z)$, $z=\mathscr{L}(a)^{-1}(xa)$. Clearly, $\mathscr{L}(x,y,a)\in H_l(a)$, $\mathscr{R}(x,y,a)\in H_r(a)$, and $\mathscr{T}(x,a)\in H(a)$. If Q is a loop and $a=1$, then $\mathscr{L}(x,y)=$ $=\mathscr{L}(x,y,1)=\mathscr{L}(y)^{-1}\mathscr{L}(x)^{-1}\mathscr{L}(xy)$, $\mathscr{R}(x,y)=\mathscr{R}(x,y,1)=\mathscr{R}(y)^{-1}\mathscr{R}(x)^{-1}\mathscr{R}(xy)$, and $\mathscr{T}(x)=\mathscr{T}(x,1)=\mathscr{L}(x)^{-1}\mathscr{R}(x)$.

2.2 Proposition. ([1]) *Let $A\in Q$.*

(i) *The inner permutation group $H(a)$ is generated by the permutations $\mathscr{L}(x,y,a)$, $\mathscr{R}(x,y,a)$, $\mathscr{T}(x,a)$, $x,y\in Q$.*

(ii) *The left inner permutation group $H_l(a)$ is generated by the permutations $\mathscr{L}(x,y,a)$, $x,y\in Q$.*

(iii) *The right inner permutation group $H_r(a)$ is generated by the permutations $\mathscr{R}(x,y,a)$, $x,y\in Q$.*

Proof. (i) Let K denote the subgroup of G generated by the permutations in (i). Then $K\subseteqq H(a)$ and we are going to prove that $H(a)\subseteqq K$.

Let $f\in H(a)$. There are $n\geqq 1$, $R_1,\ldots,R_n\in\{\mathscr{L},\mathscr{R}\}$, $u_1,\ldots,u_n\in Q$ and $r_1,\ldots,r_n\in\{1,-1\}$ such that $f=R_1(u_1)^{r_1}\ldots R_n(u_n)^{r_n}$. Now, proceeding by induction on n, we prove that $f\in K$. We can assume, without loss of generality, that $R_n=\mathscr{R}$.

First, let $n=1$. Then $au_1=a$ and $\mathscr{R}(u_1)=\mathscr{R}(u_1,u_1,a)^{-1}\in K$. Consequently, $f=\mathscr{R}(u_1)^{r_1}\in K$.

Now, let $n\geqq 2$. The rest is divided into several parts.

(a) Let $R_{n-1}=\mathscr{R}$ and $r_{n-1}=1=r_n$. Then we have $f=g\mathscr{R}(u_{n-1})\mathscr{R}(u_n)$, where $g=R_1(u_1)^{r_1}\ldots R_{n-1}(u_{n-2})^{r_{n-2}}$, $g=\mathrm{id}_Q$ for $n=2$. Further, $h=\mathscr{R}(u_{n-1},u_n,a)\in K$ and $fh=g\mathscr{R}(w)$, where $aw=au_n\cdot u_{n-1}$. But $g\mathscr{R}(w)(a)=fh(a)=a$, and therefore $g\mathscr{R}(w)\in H(a)$ and $fh=g\mathscr{R}(w)\in K$ by induction. Since $h\in K$, we have also $f\in K$.

(b) Let $R_{n-1}=\mathscr{L}$ and $r_{n-1}=1=r_n$. Then $f=g\mathscr{L}(u_{n-1})\mathscr{R}(u_n)$, $h=$ $=\mathscr{R}(u_n)^{-1}\mathscr{L}(z)\in K$, where $au_n=za$, and $fh=g\mathscr{L}(u_{n-1})\mathscr{L}(v)\in H(a)$. Now, this case is dual to the case (a).

(c) Let $R_{n-1}=\mathscr{R}$ and $r_{n-1}=-1$, $r_n=1$. Then $f=g\mathscr{R}(u_{n-1})^{-1}\mathscr{R}(u_n)=$ $=g\mathscr{R}(u)h$, where $au_n=au\cdot u_{n-1}$, $h=\mathscr{R}(u)^{-1}\mathscr{R}(u_{n-1})^{-1}\mathscr{R}(u_n)=\mathscr{R}(u_{n-1},u,a)\in K$. From this, $fh^{-1}=g\mathscr{R}(u)\in H(a)$, $g\mathscr{R}(u)\in K$ by induction and $f\in K$.

(d) Let $\mathscr{R}_{n-1}=\mathscr{L}$ and $r_{n-1}=-1$, $r_n=1$. Then $f=g\mathscr{L}(u_{n-1})^{-1}\mathscr{R}(u_n)$, $h=$ $=\mathscr{R}(u_n)^{-1}\mathscr{L}(z)\in K$, where $za=au_n$, $fh=g\mathscr{L}(u_{n-1})\mathscr{L}(v)\in H(a)$ and this case is dual to the case (c).

(e) Finally, let $r_n=-1$, so that $f=g\mathscr{R}(u_n)^{-1}$. Let $w,z\in Q$ be such that $aw=a=az\cdot u_n$. Then $h=\mathscr{R}(u_n,z,a)=\mathscr{R}(z)^{-1}\mathscr{R}(u_n)^{-1}\mathscr{R}(w)\in K$ and $\mathscr{R}(w)\in K$. Further, $f\mathscr{R}(w)=g\mathscr{R}(z)h\in H(a)$, so that $g\mathscr{R}(z)H(a)$ and, consequently, $g\mathscr{R}(z)\in K$ by induction. Then also $f=g\mathscr{R}(z)h\mathscr{R}(w)^{-1}\in K$.

2.3 Consider the situation from 1.13.

(i) It follows easily from 2.2(i) that, for each $a\in Q$, $\varphi(H(a))=\mathscr{I}(P,\psi(a))$ and $\mathrm{Ker}(\varphi|H(a))=H(a)\cap N$. Thus we have the isomorphisms $\mathscr{I}(P,\psi(a))\cong$ $\cong H(a)/H(a)\cap N\cong H(a)N/N$.

(ii) $\varphi(H_l(a)) = \mathscr{I}_l(P, \psi(a))$, $\mathrm{Ker}(\varphi \mid H_l(a)) = H_l(a) \cap N$ and $\mathscr{I}_l(P, \psi(a)) \cong H_l(a)/H_l(a) \cap$ $\cap N \cong H_l(a)\, N/N$.

(iii) $\varphi(H_r(a)) = \mathscr{I}_r(P, \psi(a))$, $\mathrm{Ker}(\varphi \mid H_r(a)) = H_r(a) \cap N$ and $\mathscr{I}_r(P, \psi(a)) \cong H_r(a)/H_r(a) \cap$ $\cap N \cong H_r(a)\, N/N$.

2.4 Consider the situation from 1.15.

(i) For $a \in P$, let $I(a) = \langle \mathscr{L}(x, y, a), \mathscr{R}(x, y, a), \mathscr{T}(x, a);\ x, y \in P \rangle \subseteqq K$. Then $\varphi(I(a)) = \mathscr{I}(P, a)$ and $I(a) \subseteqq H(a)$.

(ii) For $a \in P$, let $I_l(a) = \langle \mathscr{L}(x, y, a);\ x, x \in P \rangle \subseteqq K_l$. Then $\varphi(I_l(a)) = \mathscr{I}_l(P, a)$ and $I_l(a) \subseteqq H_l(a)$.

(iii) For $a \in P$, let $I_r(a) = \langle \mathscr{R}(x, y, a);\ x, x \in P \rangle \subseteqq K_r$. Then $\varphi(I_r(a)) = \mathscr{I}_r(P, a)$ and $I_r(a) \subseteqq H_r(a)$.

2.5 Consider the situation from 1.16. Then, for $a = (a_i) \in Q$, $H(a)$ $(H_l(a), H_r(a))$ can be embedded into $\Pi.\mathscr{I}(Q_i, a_i)$ $(\Pi.\mathscr{I}_l(Q_i, a_i), \Pi.\mathscr{I}_r(Q_i, a_i))$.

2.6 Lemma. *Let $a, b \in Q$. The following conditions are equivalent:*

(i) $H(a) \subseteqq H(b)$.

(ii) $H(b) \subseteqq H(a)$.

(iii) $H(a) = H(b)$.

(iv) $\mathscr{L}(b)\, \mathscr{L}(a)^{-1} = \mathscr{R}(b)\, \mathscr{R}(a)^{-1} \in \mathbf{Z}(G)$.

(v) $\mathscr{L}(a)\, \mathscr{L}(b)^{-1} = \mathscr{R}(a)\, \mathscr{R}(b)^{-1} \in \mathbf{Z}(G)$.

Proof. First, observe that $\mathscr{L}(x, y, a) \in H(b)$ iff $\mathscr{L}(x)\, \mathscr{R}(b)\, (y) =$ $= \mathscr{R}(b)\, \mathscr{R}(a)^{-1}\, \mathscr{L}(x)\, \mathscr{R}(a)\, (y)$, $\mathscr{R}(x, y, a) \in H(b)$ iff $\mathscr{R}(x)\, \mathscr{L}(b)\, (y) =$ $= \mathscr{L}(b)\, \mathscr{L}(a)^{-1}\, \mathscr{R}(x)\, \mathscr{L}(a)\, (y)$ and $\mathscr{T}(x, a) \in H(b)$ iff $\mathscr{L}(b)\, \mathscr{L}(a)^{-1}\, \mathscr{R}(a)\, (x) =$ $= \mathscr{R}(b)\, (x)$. Consequently $\mathscr{L}(x, y, a) \in H(b)$ for every $y \in Q$ iff $\mathscr{L}(x)\, \mathscr{R}(b)\, \mathscr{R}(a)^{-1} =$ $= \mathscr{R}(b)\, \mathscr{R}(a)^{-1}\, \mathscr{L}(x)$. Similarly $\mathscr{R}(x, y, a) \in H(b)$ for every $y \in Q$ iff $\mathscr{R}(x)\, \mathscr{L}(b)\, \mathscr{L}(a)^{-1} = \mathscr{L}(b)\, \mathscr{L}(a)^{-1}\, \mathscr{R}(x)$. Moreover $\mathscr{T}(x, a) \in H(b)$ for every $x \in Q$ iff $\mathscr{L}(b)\, \mathscr{L}(a)^{-1} = \mathscr{R}(a)\, \mathscr{R}(b)^{-1}$. Using this, we see easily that (i) implies (iv). Conversely, iff (iv) is satisfied, then (i) follows by 2.2(i), and so (i) and (iv) are equivalent. Quite similarly, (ii) and (v) are equivalent and, trivially, (iv) and (v) are equivalent.

2.7 Proposition. ([4]) *Let $a \in Q$.*

(i) *$f \in \mathbf{N}_G(H(a))$ iff $f \in G$ and $H(f(a)) = H(a)$.*

(ii) $\mathbf{N}_G(H(a)) = H(a)\, \mathbf{Z}(G)$.

Proof. First, let $g \in \mathbf{N}_G(H(a))$ and $g \in H(a)$. Then $h = f^{-1} g f \in H(a)$, $gf(a) =$ $= fh(a) = f(a)$ and $g \in H(f(a))$. We have proved that $H(a) \subseteqq H(f(a))$, and so $H(f(a)) = H(a)$ by 2.6.

Now, let $H(f(a)) = H(a)$ and let $b \in Q$ be such that $a = ab$. By 2.6, $\mathscr{L}(f(a))\, \mathscr{L}(a)^{-1} \in \mathbf{Z}(G)$. However, $\mathscr{R}(b) \in H(a) = H(f(a))$, $f(a) = f(a)\, b$, $f^{-1} \mathscr{L}(f(a))\, \mathscr{L}(a)^{-1} \in H(a)$ and $f \in H(a)\, \mathbf{Z}(G) \subseteqq \mathbf{N}_G(H(a))$.

Another proof of (ii) follows from 1.6(iii) and I.3.18.

2.8 Lemma. *Let $a, b \in Q$. The following conditions are equivalent:*

(i) $H_l(a) \subseteq H_l(b)$ $(H_r(a) \subseteq H_r(b))$.

(ii) $H_l(b) \subseteq H_l(a)$ $(H_r(b) \subseteq H_r(a))$.

(iii) $H_l(a) = H_l(b)$ $(H_r(a) = H_r(b))$.

(iv) $\mathscr{R}(b)\mathscr{R}(a)^{-1} \in \mathbf{C}_G(G_l) = \mathbf{C}_S(G_l) \subseteq G_r$ $(\mathscr{L}(b)\mathscr{L}(a)^{-1} \in \mathbf{C}_G(G_r) = \mathbf{C}_S(G_r) \subseteq G_l)$.

(v) $\mathscr{R}(b)\mathscr{R}(a)^{-1} = R(xb)\mathscr{R}(xa)^{-1}$ *for every* $x \in Q$ $(\mathscr{L}(b)\mathscr{L}(a)^{-1} = \mathscr{L}(bx)\mathscr{L}(ax)^{-1}$ *for every* $x \in Q)$.

Proof. Similar to that of 2.6 (see 1.5(i), (ii)).

2.9 Proposition. *Let $a \in Q$ and $f \in G_l$ $(f \in G_r)$. The following conditions are equivalent:*

(i) $f \in \mathbf{N}_{G_l}(H_l(a))$ $(f \in \mathbf{N}_{G_r}(H_r(a)))$.

(ii) $H_l(f(a)) = H_l(a)$ $(H_r(f(a)) = H_r(a))$.

(iii) $f \in (\mathbf{C}_G(G_l)\, H(a)) \cap G_l$ $(f \in (\mathbf{C}_G(G_r)\, H(a)) \cap G_r)$.

Proof. (i) implies (ii). Let $g \in H_l(a)$. Then $f^{-1}gf \in H_l(a)$ and $g \in H_l(f(a))$. By 2.8, $H_l(a) = H_l(f(a))$.

(ii) implies (iii). By 2.8, $k = \mathscr{R}(f(a))\mathscr{R}(a)^{-1} \in \mathbf{C}_G(G_l)$. Further, if $a = ba$, then $f(a) = bf(a)$ and $f^{-1}k \in H(a)$.

(iii) implies (i). Let $f = gh$, $g \in \mathbf{C}_G(G_l)$, $h \in H(a)$ and let $k \in H_l(a)$. Then $f^{-1}kf(a) = f^{-1}kg(a) = f^{-1}gk(a) = h^{-1}(a) = a$, and so $f^{-1}kf \in H_l(a)$.

2.10 Corollary. (i) $\mathbf{N}_G(H(a)) = H(a)$ *iff* $\mathbf{Z}(G) = 1$.

(ii) *If* $\mathbf{C}_G(G_l) = 1$, *then* $\mathbf{N}_{G_l}(H_l(a)) = H_l(a)$.

(iii) *If* $\mathbf{C}_G(G_r) = 1$, *then* $\mathbf{N}_{G_r}(H_r(a)) = H_r(a)$.

3. The stability congruence

3.1 We continue here immediately the preceding two sections.

Put $s = s(Q) = \Phi(\mathbf{Z}(G))$ (see 1.10(i)). Then s is a cancellative congruence of Q (the stability congruence introduced by Smith in [4]) and $(a, b) \in s$ iff $a, b \in Q$ and $b = f(a)$ for some $f \in \mathbf{Z}(G)$.

3.2 Lemma. *Let $a, b \in Q$. The following conditions are equivalent:*

(i) $(a, b) \in s$.

(ii) $H(a) = H(b)$ *(see 2.6).*

(iii) $\mathscr{L}(b)\mathscr{L}(a)^{-1} \in \mathbf{Z}(G)$.

(iv) $\mathscr{R}(b)\mathscr{R}(a)^{-1} \in \mathbf{Z}(G)$.

In this case $\mathscr{L}(b)\mathscr{L}(a)^{-1} = \mathscr{R}(b)\mathscr{R}(a)^{-1}$ *and* $\mathscr{L}(b)\mathscr{L}(a)^{-1}(a) = b$.

Proof. (i) implies (ii). This implication is easy.

(ii) implies (iii) and (iv). See 2.6.

(iii) implies (i). Let $c \in Q$ be such that $a = ac$. Then $\mathscr{L}(b)\,\mathscr{L}(a)^{-1}(a) = \mathscr{L}(b)\,\mathscr{L}(a)^{-1}\,\mathscr{R}(c)^{-1}(a) = \mathscr{R}(c)^{-1}\,\mathscr{L}(b)\,\mathscr{L}(a)^{-1}(a) = \mathscr{R}(c)^{-1}(bc) = b$.

(iv) implies (i). We can proceed similarly.

The rest is clear from 2.6.

3.3 Corollary. (i) $\mathrm{card}(Q) = \mathrm{card}(\mathbf{Z}(G)) \cdot (\mathrm{card}(Q/s)$.

(ii) $s = \mathrm{id}_Q$ *iff* $\mathbf{Z}(G) = 1$.

(iii) $s = Q \times Q$ *iff* Q *is an abelian group.*

3.4 For every ordinal number $\alpha \geqq 0$, define a cancellative congruence $s(\alpha) = s(Q, \alpha)$ of Q as follows: $s(0) = \mathrm{id}_Q$; if $\alpha \geqq 0$ then $s(\alpha + 1)$ is the uniquely determined cancellative congruence of Q such that $s(\alpha) \subseteqq s(\alpha + 1)$ and $s(\alpha + 1)/s(\alpha) = s(Q/s(\alpha))$; if $\alpha > 0$ is limit, then $s(\alpha) = \bigcup s(\beta)$, $0 \leqq \beta \leqq \alpha$.

The quasigroup Q is said to be stably nilpotent of class at most α if $s(\alpha) = Q \times Q$.

The quasigroup is said to be stably nilpotent if it is stably nilpotent of a finite class.

Clearly, Q is stably nilpotent of class at most 0 iff it is trivial and Q is stably nilpotent of class at most 1 iff it is an abelian group.

3.5 (i) For every $\alpha \geqq 0$, let $L(\alpha) = \Psi(s(\alpha))$ (see 1.10(ii)). Then $L(\alpha)$ is a normal subgroup of G and Q is stably nilpotent of class at most α iff $L(\alpha) = G$ (this follows from 1.12).

(ii) For $a \in Q$ and $\alpha \geqq 0$, let $H(a, \alpha) = L(\alpha) \cap H(a)$.

Let $\psi\colon Q \to Q/s(\alpha) = P$ denote the natural projection. By 2.3(i), $\mathscr{I}(P, \psi(a)) \cong \cong H(a)/H(a, \alpha)$.

3.6. Lemma. (i) $L(0) = 1$.

(ii) $L(1) = \mathbf{L}_G(H(a)\,\mathbf{Z}(G))$, $a \in Q$.

(iii) *For every* $n \geqq 0$, $L(n + 1) = \mathbf{L}_G(H(a)\,K_n)$, $a \in Q$, *where* $K_n \in \mathscr{N}$ *is such that* $L(n) \subseteqq K_n$ *and* $K_n/L(n) = \mathbf{Z}(G/L(n))$.

Proof. (i) This is obvious.

(ii) $L(1) = \Psi(s) = \Psi\Phi(\mathbf{Z}(G)) = \mathbf{L}_G(H(a)\,\mathbf{Z}(G))$ by 1.11(i).

(iii) We shall proceed by induction on n. For $n = 0$, the result is proved in (ii). Now let $n \geqq 1$, $P = Q/s(n)$, $\psi\colon Q \to P$ and $\varrho\colon G \to G/L(n)$ be the natural projection and let $\varphi\colon G \to \mathscr{M}(P)$ be by 1.13(ii). Now, we are going to show that $s(n + 1) = \Phi(K_n)$.

First, let $f \in K_n$, $a \in Q$. We have $L(n) = \mathrm{Ker}(\varphi)$, so that $\varphi = \sigma\varrho$ for an isomorphism $\sigma\colon G/L(n) \to \mathscr{M}(P)$, and then $\varphi(F) = \sigma\varrho(f) \in \mathbf{Z}(\mathscr{M}(P))$, $(\psi(a), \varphi(f)\,(\psi(a))) = (\psi(a), \psi(f(a))) \in s(P)$ and $(a, f(a)) \in s(n + 1)$. We have proved that $\Phi(K_n)$ is contained in $s(n + 1)$.

Now, let $(a, b) \in s(n + 1)$, i.e. $(\psi(a), \psi(b)) \in s(P)$. Then there is $f \in K_n$ such that $\psi(b) = \varphi(f)\,(\psi(a)) = \psi(f(a))$. However, then $(a, f(a)) \in \Phi(K_n)$ and $(f(a), b) \in s(n)$. Since $L(n) \subseteqq K_n$, we have $s(n) = \Phi(K_n)$, and hence $(a, b) \in \Phi(K_n)$.

We have proved that $s(n+1) = \Phi(K_n)$. Now, by 1.11(i), $L(n+1) = \Psi(s(n+1)) = \Psi\Phi(K_n) = \mathbf{L}_G(H(a)\, K_n)$.

3.7 Proposition. *Let $n \geqq 1$. The following conditions are equivalent:*

(i) *Q is stably nilpotent of class at most n.*

(ii) $L(n) = G$.

(iii) $G' \subseteq H(a)\, K_{n-2}$ *(see 3.6;* $K_{-1} = 1$*).*

(iv) $H(a)\, K_{n-2}$ *is normal in G.*

(v) $H(a) \subseteq L(n-1)$.

(vi) $H(a) = H(a, n-1)$.

Proof. Easy (combine 3.4, 3.5 and 3.6).

3.8 Proposition. ([4]) *Let $n \geqq 1$. The following conditions are equivalent:*

(i) *Q is stably nilpotent of class at most n.*

(ii) *For every $a \in Q$, $H(a)$ is subnormal of depth at most n in G.*

(iii) *There exists $a \in Q$ such that $H(a)$ is subnormal of depth at most $n \in G$.*

Proof. (i) implies (ii). By induction on n. If $n = 1$, then $H(a) = 1$ is normal in G, i.e., subnormal of depth at most 1.

Let $n \geqq 2$ and $P = Q/s(1)$. Then P is stably nilpotent of class at most $n-1$, and so $\mathscr{I}(P, \Psi(a)) \cong L(1)\, H(a)/L(1)$ is subnormal of depth at most $n-1$ in $\mathscr{M}(P) \cong G/L(1)$ (here, $\psi\colon Q \to P$ denotes the natural projection). This implies that $L(1)\, H(a)$ is subnormal of depth at most $n-1$ in G. However, $H(a) \subseteq L(1)\, H(1) = \mathbf{Z}(G)\, H(a)$, so that $H(a)$ is normal in $L(1)\, H(a)$.

(ii) implies (iii). This is trivial.

(iii) implies (i). Again by induction on n. If $n = 1$, then the result follows from 1.17(iii). Let $n \geqq 2$ and $P = Q/s(1)$. We have $\mathscr{I}(P, \psi(a)) \cong L(1)\, H(a)/L(1) = \mathbf{N}_G(H(a))/L(1)$. However $\mathbf{N}_G(H(a))$ is subnormal of depth at most $n-1$ in $\mathscr{M}(P)$, P is stably nilpotent of class at most $n-1$ and Q is stably nilpotent of class at most n.

3.9 Corollary. *If the multiplication group G is nilpotent of class at most $n \geqq 0$, then the quasigroup Q is stably nilpotent of class at most n.*

3.10 Put $j(Q) = \mathrm{card}(Q/s)$. By 2.7(i) and 3.2, we have $j(Q) = [G\colon \mathbf{N}_G(H(a))] = [G\colon H(a)\, \mathbf{Z}(G)]$. By 3.3(i), $\mathrm{card}(Q) = \mathrm{card}(\mathbf{Z}(G)) \cdot j(Q)$. Consequently $\mathrm{card}(G) = i(Q) \cdot j(Q) \cdot \mathrm{card}(\mathbf{Z}(G))$.

3.11 Lemma. (i) *$L(1)$ can be imbedded into the cartesian product of $j(Q)$ copies of $\mathbf{Z}(G)$; in particular, $L(1)$ is abelian.*

(ii) *For every $a \in Q$, $H(a, 1)$ can be imbedded into the cartesian product of $j(Q) - 1$ copies of $\mathbf{Z}(G)$ (here, $j(Q) - 1 = j(Q)$ for $j(Q)$ infinite).*

Proof. (i) For every $a \in Q$, $\mathbf{N}_G(H(a))$ is the direct product of $H(a)$ and $\mathbf{Z}(G)$. Hence, let $\pi_a\colon \mathbf{N}_G(H(a)) \to \mathbf{Z}(G)$ denote the natural projection. Now, let $\{a_i\}$ be a set

of representatives of the blocks of $s = s(1)$. Since $L(1) = \mathbf{L}_G(\mathbf{N}_G(H(a)))$ for every $a \in Q$, we can define a homomorphism $\varphi: L(1) \to \Pi_i \mathbf{Z}(G)$ by $\varphi(f) = (\pi_{a_i}(f))$, $f \in L(1)$. If $\varphi(f) = 1$, then $f \in H(a_i)$ for every i and then $f \in \bigcap_a H(a) = \mathrm{id}_Q$. Thus φ is injective.

(ii) Take $a \in Q$ and define $\psi: H(a, 1) \to \Pi \mathbf{Z}(G)$ by $\psi(f) = (\pi a_i(f))$, $a_i \notin H(a)$. Again, ψ is injective.

3.12 Corollary. *For every $n \geqq 0$, $L(n+1)/L(n)$ can be imbedded into the cartesian product of $j(Q/s(n))$ copises of $\mathbf{Z}(G)/L(n)$).*

3.13 Corollary. ([4]) *If Q is stably nilpotent of class at most $n \geqq 1$, then the multiplication group G is soluble of class at most n.*

3.14 Corollary. *If Q is stably nilpotent of class at most 2, then $H(a)$ (for each $a \in Q$) can be imbedded into the cartesian product of $j(Q) - 1$ copies of $\mathbf{Z}(G)$. In particular, $H(a)$ is an abelian group.*

3.15 Proposition. *Suppose that Q is finite and of prime-power order. The following conditions are equivalent:*

(i) *Q is stably nilpotent.*

(ii) *G is a p-group.*

(iii) *G is nilpotent.*

Proof. (i) implies (ii). For every $n \geqq 0$, the centre $\mathbf{Z}(G/L(n))$ is isomorphic to the centre $\mathbf{Z}(\mathscr{M}(Q/s(n))$. However, the order of $Q/s(n)$ is a power of a prime p, and hence $\mathbf{Z}(G/L(n))$ is a p-group (see 3.10). Now, by 3.12, $L(n+1)/L(n)$ is a p-group, too.

(ii) implies (iii). This is clear.

(iii) implies (i). See 3.9.

3.16 Lemma. (i) *If $a, b \in Q$ belong to the same block of s, then $ab = ba$.*

(ii) *If Q is commutative and $a, b, c \in q$ belong to the same block of s, then $a \cdot bc = ab \cdot c$.*

Proof. (i) $b = f(a)$ for some $f \in \mathbf{Z}(G)$, and so $ab = af(a) = f(aa) = f(a)\, a = ba$.

(ii) $b = f(a)$, $c = g(a)$, $f, g \in \mathbf{Z}(G)$ and $a \cdot bc = a \cdot f(a)\, g(a) = g(a \cdot f(a)\, a) = g(a \cdot f(aa)) = gf(a \cdot aa) = fg(a \cdot aa) = fg(aa \cdot a) = ab \cdot c$.

3.17 Proposition. ([4]) *If Q is stably nilpotent, then Q contains a unique idempotent element e. The block of s containing e is an abelian subgroup of Q.*

Proof. We shall proceed by induction on the class n of Q. If $n = 0$, then Q is trivial and the result is clear. Let $n \geqq 1$ and $P = Q/s$. Then P is stably nilpotent of class at most $n - 1$ and P contains just one idempotent element. The block R of $s(Q)$ corresponding to this element is a subquasigroup of Q. By 3.16, R is an abelian

subgroup of Q, and so the neutral element e of R is an idempotent in Q. On the other hand, if $e' \in Q$ is idempotent, then $e' \in R$ (since P contains just one idempotent) and necessarily $e' = e$.

3.18 If Q is a loop, then the stability congruence coincides with the congruence corresponding to the centre $\mathbf{Z}(Q)$ of Q. Thus Q is stably nilpotent (of a class) iff Q is (centrally) nilpotent (of the same class) in the usual sense.

3.19 Lemma. *Suppose that Q is a loop but not an abelian group. Then $j(Q) \geqq 3$.*

Proof. If $j(Q) = 1$, then $s = Q \times Q$ and Q is an abelian group. Now, let $j(Q) = 2$. Then Q is (stably) nilpotent of class 2, $Q = \mathbf{Z}(Q) \cup a\,\mathbf{Z}(Q)$ for any $a \in Q - \mathbf{Z}(Q)$. If b, c in $\mathbf{Z}(Q)$, then $bc = cb$, $b \cdot ac = ac \cdot b$, $ab \cdot ac = (ab \cdot a)\,c = (a^2 b)\,c = a^2 \cdot bc = a^2 \cdot cb = ac \cdot ab$ and we have checked that Q is commutative. Similarly, if $b, c, d \in \mathbf{Z}(Q)$, then $(ab)(ac \cdot ad) = (a \cdot a^2)(bcd) = (a^2 \cdot a)(bcd) = (ab \cdot ac)(ad)$ and it is clear that Q is an abelian group; then $j(Q) = 1$, a contradiction.

4. The loop-kernel

4.1 Again, this is an immediate continuation of the preceding three sections.

(i) Let $a, b \in Q$, $f = \mathscr{R}(a)$, $g = \mathscr{L}(b)$ and $x * y = f^{-1}(x)\, g^{-1}(y)$ for all $x, y \in Q$. Then $Q(*)$ is a loop, ba is its neutral element and $xy = f(x) * g(y)$ for all $x, y \in Q$. The loop $Q(*)$ is a principal isotope of Q and every principal loop isotope of Q is of this form.

(ii) Let $Q(*)$ be a loop which is principal isotope of the quasigroup Q, i.e., there exist $f, g \in S$ such that $xy = f(x) * g(y)$ for all $x, y \in Q$. Then $f = \mathscr{R}(g^{-1}(e))$, $g = \mathscr{L}(f^{-1}(e))$, where e denotes the neutral element of $Q(*)$, and $G_l = \langle \mathscr{M}_l(Q(*)), g \rangle$, $G_r = \langle \mathscr{M}_r(Q(*)), f \rangle$, $G = \langle \mathscr{M}(Q(*)), f, g \rangle$.

(iii) Let $Q(*)$ and $Q(\circ)$ be loops which are both principal isotopes of Q. Then $Q(\circ)$ is a principal isotope of $Q(*)$, and so $M_l(Q(\circ)) \leqq M_l(Q(*))$, $M_r(Q(\circ)) \leqq M_r(Q(*))$, $M(Q(\circ)) \leqq M(Q(*))$. Similarly the converse inequalities and thus we have $\mathscr{M}_l(Q(\circ)) = M_l(Q(*))$, $\mathscr{M}_r(Q(\circ)) = M_r(Q(*))$ and $M(Q(\circ)) = M(Q(*))$.

The uniquely determined subgroup $\mathscr{M}(Q(*))$ of $G = \mathscr{M}(Q)$ will be called the loop-kernel of G in the sequel and will be denoted by $\tilde{G} = \tilde{\mathscr{M}}(Q)$.

For every $a \in Q$, $H(a) \cap \tilde{G} = \mathscr{I}(Q, a) \cap \tilde{G} = \mathscr{I}(Q(*), a) = \mathscr{I}(Q(\circ), a)$; we put $\tilde{H}(a) = \tilde{\mathscr{I}}(Q, a) = H(a) \cap \tilde{G}$.

4.2 Lemma. (i) $\mathscr{L}(a)\,\mathscr{L}(b)^{-1} \in \tilde{G}$ *for all* $a, b \in Q$.

(ii) $\tilde{G} = \langle \mathscr{L}(x)\,\mathscr{L}(a)^{-1}, \mathscr{R}(x)\,\mathscr{R}(b)^{-1}; x \in Q \rangle$ *for all* $a, b \in Q$.

(iii) $G = \langle \tilde{G}, \mathscr{L}(a)\,\mathscr{R}(b) \rangle$ *for all* $a, b \in Q$.

Proof. See 4.1.

4.3 Lemma. $G = \tilde{G} \cdot H(a) = H(a) \cdot \tilde{G}$ *for every* $a \in Q$.

Proof. Let $f \in G$, $b, c \in Q$, $a = ba$, $f(a) = ca$. Then $f = \mathscr{L}(c)\,\mathscr{L}(b)^{-1} \cdot \mathscr{L}(b)\,\mathscr{L}(c)^{-1} f$, $\mathscr{L}(c)\,\mathscr{L}(b)^{-1} \in \tilde{G}$ and $\mathscr{L}(b)\,\mathscr{L}(c)^{-1} f \in H(a)$.

4.4 Lemma. (i) $\mathbf{Z}(G_l) \leqq \tilde{G}$ *and* $\mathbf{Z}(G_r) \leqq \tilde{G}$.

(ii) $\mathbf{Z}(G) \leqq \mathbf{L}_G(\mathbf{Z}\tilde{G}))$.

Proof. (i) This follows from 1.5(i), (ii) and 4.2(i).

(ii) By (i) and 1.5(iv), $\mathbf{Z}(G) \leqq \tilde{G}$. Hence $\mathbf{Z}(G) \leqq \mathbf{Z}(\tilde{G})$ and, moreover, $\mathbf{Z}(G) \leqq \mathbf{L}_G(\mathbf{Z}(\tilde{G}))$.

4.5 Proposition. *The following conditions are equivalent:*

(i) Q *is isotopic to abelian group.*

(ii) $\tilde{G}$ *is an abelian group.*

(iii) $\tilde{H}(a) = 1$.

(iv) $\tilde{H}(a)$ *is a cyclic group.*

Proof. (i) implies (ii). Let $Q(*)$ be a principal loop isotope of Q. Then $Q(*)$ is an abelian group, and so $Q(*) \cong \mathscr{M}(Q(*)) = \tilde{G}$.

(ii) implies (iii). We have $\tilde{H}(a) = \mathscr{I}(Q(*), a) = 1$.

(iii) implies (iv). This is trivial.

(iv) implies (i). $Q(*)$ is a loop whose inner permutation group is cyclic. By [3], $Q(*)$ is an abelian group.

4.6 Corollary. *Suppose that* $H(a)$ *is cyclic. Then* Q *is isotopic to abelian group.*

4.7 Proposition. *Suppose that* $H(a)$ *is abelian and* Q *is isotopic to abelian group. Then* $G'' = 1$.

Proof. By 4.5, $\tilde{G}$ is abelian. However, $G = \tilde{G} \cdot H(a)$ and we can use the well-known Ito theorem.

4.8 Let $Q(*)$ be a principal loop isotope of Q and let e denote the neutral element of $Q(*)$. There are $f, g \in S$ such that $xy = f(x) \cdot g(y)$ for all $x, y \in Q$.

(i) Put $a = f(e)$ and $f_1 = \mathscr{R}(Q(*), a)^{-1} f \in S$. Then $f_1(e) = e$, so that $f_1 \in H(e)$, and $f(x) = f_1(x) * a$ for every $x \in Q$. Similarly, if $b = g(e)$ and $g_1 = \mathscr{R}(Q(*), b)^{-1} g$, then $g_1(e) = e$, $g_1 \in H(e)$ and $g(x) = g_1(x) * b$ for every $x \in Q$. Now, $xy = (f_1(x) * a) * (g_1(x) * b)$ for all $x, y \in Q$.

(ii) We have $\mathbf{Z}(\tilde{G}) = \{\mathscr{L}(Q(*), u);\ u \in \mathbf{Z}(Q(*))\}$. Now, put $R = \{u \in \mathbf{Z}(Q(*));\ \mathscr{L}(Q(*), u) \in \mathbf{L}_G(\mathbf{Z}(\tilde{G}))\}$. Then R is a subgroup of $\mathbf{Z}(Q(*))$.

(iii) Let $u \in R$ and $h \in H(e)$. Then $\mathscr{L}(*, u) \in \mathbf{L}_G(\mathbf{Z}(\tilde{G}))$, and so $h\mathscr{L}(*, u)\,h^{-1} = \mathscr{L}(*, v)$ for suitable $v \in R$. Then also $h(u) = h(u * e) = v * h(e) = v$, so that $h\mathscr{L}(*, u) = \mathscr{L}(*, h(u))\,h$ and $h(u * x) = h(u) * h(x)$ for every $x \in Q$.

(iv) For each $h \in H(e)$, $h|R$ is an automorphism of the abelian group $R(*)$. In particular, $f_1|R$ and $g_1|R$ are automorphisms of $R(*)$.

(v) $G = \langle \tilde{G}, f_1, g_1 \rangle$. Now, define a binary operation $\triangle$ on Q by $x \triangle y = f_1(x) * g_1(y)$. Then $Q(\triangle)$ is a guasigroup, it is a principal isotope of Q and $\mathcal{M}(Q(\triangle)) = G = \mathcal{M}(Q)$, $\tilde{\mathcal{M}}(Q(\triangle)) = \tilde{G} = \tilde{\mathcal{M}}(Q)$. Moreover, $e \triangle e = e$.

(vi) If $\tilde{G}$ is abelian and normal in G, then $Q(*)$ is an abelian group and f_1, g_1 are its automorphisms. In that case, $xy = f_1(x) * g_1(y) * c$, $c = a * b$, for all $x, y \in Q$.

5. Quasigroups linear over abelian groups

5.1 A quasigroup Q will be called linear (more precisely, linear over abelian group) in the sequel if there exists an abelian group $Q(+)$, $f, g \in \mathrm{Aut}(Q(+))$ and $w \in Q$ such that $xy = f(x) + g(y) + w$ for all $x, y \in Q$. Now, assume that Q is such a quasigroup.

(i) $\mathcal{L}(Q, a) = \mathcal{L}(Q(+), f(a) + w)\, g$ and $\mathcal{R}(Q, a) = \mathcal{L}(Q(+), g(a) + w)\, f$ for every $a \in Q$.

(ii) $\mathcal{M}_l(Q) = \langle \mathcal{M}(Q(+)), g \rangle$, $\mathcal{M}(Q(+))$ is a normal subgroup of $\mathcal{M}_l(Q)$, $\mathcal{M}(Q(+)) \cap \langle g \rangle = 1$ and $\mathcal{M}_l(Q) = \mathcal{M}(Q(+)) \cdot \langle g \rangle$.

(iii) $\mathcal{M}_r(Q) = \langle \mathcal{M}(Q(+)), f \rangle$, $\mathcal{M}(Q(+))$ is a normal subgroup of $\mathcal{M}_r(Q)$, $\mathcal{M}(Q(+)) \cap \langle f \rangle = 1$ and $\mathcal{M}_r(Q) = \mathcal{M}(Q(+)) \cdot \langle f \rangle$.

(iv) $\mathcal{M}(Q) = \langle \mathcal{M}(Q(+)), f, g \rangle$, $\mathcal{M}(Q(+))$ is a normal subgroup of $\mathcal{M}(Q)$, $\mathcal{M}(Q(+)) \cap \langle f, g \rangle = 1$ and $\mathcal{M}(Q) = \mathcal{M}(Q(+)) \cdot \langle f, g \rangle$.

(v) $\mathcal{I}_l(Q, 0) = \langle g \rangle$, $\mathcal{I}_r(Q, 0) = \langle f \rangle$ and $\mathcal{I}(Q, 0) = \langle f, g \rangle$.

(vi) $\tilde{\mathcal{M}}(Q) = \mathcal{M}(Q(+)) \cong Q(+)$.

(vi) $\mathbf{Z}(\mathcal{M}_l(Q)) = \{\mathcal{L}(Q(+), a);\ g(a) = a\}$, $\mathbf{Z}(\mathcal{M}_r(Q)) = \{\mathcal{L}((Q(+), a);\ f(a) = a\}$ and $\mathbf{Z}(\mathcal{M}(Q)) = \{\mathcal{L}(Q(+), a); f(a) = g(a) = a\}$.

5.2 Proposition. *The following conditions are equivalent for a group G:*

(i) *G is isomorphic to the multiplication group of a linear quasigroup.*

(ii) *G contains subgroups K, H such that $G = KH$, K is a normal abelian subgroup of G, H can be generated by at most two elements and $\mathbf{L}_G(H) = 1$.*

Proof. (i) implies (ii). If $G = \mathcal{M}(Q)$, then $K = \tilde{\mathcal{M}}(Q)$ and $H = \mathcal{I}(Q, 0)$ (see 5.1).

(ii) implies (i). First, define a mapping $\varphi\colon H \to \mathrm{Aut}(K)$ by $\varphi(a)(x) = axa^{-1}$ for all $a \in H$, $x \in K$. Then φ is a homomorphism and $\mathrm{Ker}(\varphi) = H \cap \mathbf{C}_G(K) \subseteq \mathbf{L}_G(H) = 1$, so that φ is injective. Further, denote by P the subgroup of $\mathcal{S}(K)$ generated by $\mathcal{M}(K) \cup \varphi(H)$ and define a mapping $\psi\colon G \to P$ by $\psi(xa) = \mathcal{L}(K, x)\, \varphi(a)$ for all $x \in K$ and $a \in H$ (we have $K \cap H \subseteq \mathbf{L}_G(H) = 1$, and so ψ is well defined). Now, for $x, y \in K$ and $a, b \in H$, we have $\psi(xa)(\psi(yb)(z)) = xaybzb^{-1}a^{-1} = xaya^{-1} \cdot abzb^{-1}a^{-1} = \psi(xaya^{-1} \cdot ab)(z) = \psi(xayb)(z)$. We have checked that ψ is a homomorphism of G into the permutation group P. Since $\psi(K) = \mathcal{M}(K)$ and $\psi(H) = \varphi(H)$, we have $\psi(G) = P$. Moreover, if $\psi(xa) = 1$, then $xaz = za$ for

every $z \in K$, and hence $x = 1$ and $a \in H \cap \mathbf{C}_G(K) = 1$. Thus ψ is an isomorphism of G onto P. Finally, let u, v generate H. Define a binary operation $*$ on K by $x * y = \varphi(u)(x) \cdot \varphi(v)(y) = uxu^{-1}vyv^{-1}$ for all $x, y \in K$. Then $K(*)$ is a linear quasigroup and $\mathscr{M}(K(*)) = P$ (see 5.1).

5.3 Remark. Let G be a group such that $G = KH$, where K is a normal abelian subgroup of G and H is a subgroup of G. Then $\mathbf{L}_G(H) = 1$ iff $\mathbf{C}_G(K) = K$ and $K \cap H = 1$.

5.4 Proposition. *A quasigroup Q is linear iff $\tilde{\mathscr{M}}(Q)$ is abelian and normal in $\mathscr{M}(Q)$.*

Proof. Combine 5.1 and 4.8(viii).

5.5 Proposition. *Let Q be a linear quasigroup. Then Q is stably nilpotent of class at most 2 iff the multiplication group $\mathscr{M}(Q)$ is nilpotent of class at most 2.*

Proof. Put $G = \mathscr{M}(Q)$, $K = \tilde{\mathscr{M}}(Q)$ and $H = \mathscr{I}(Q, 0)$ (see 5.1). If G is nilpotent of class at most 2, then Q is stably nilpotent of class at most 2 by 3.9. Now, assume that Q is stably nilpotent of class at most 2. Then $\mathbf{Z}(G)H$ is normal in G. Since Q is linear,, K is normal in G and we have $[K, K] \subseteq [K, \mathbf{Z}(G)H] \subseteq K \cap \mathbf{Z}(G)H$. On the other hand, $\mathbf{L}_G(H) = 1$, and so $\mathbf{C}_G(K) = K$, $\mathbf{Z}(G) \subseteq K$ and $K \cap H = 1$. Consequently, $K \cap \mathbf{Z}(G)H = \mathbf{Z}(G)$, $[K, H] \subseteq \mathbf{Z}(G)$ and $G/\mathbf{Z}(G)$ is abelian (take into account H is abelian by 3.14).

5.6 Consider the situation from 5.1 and put $P = \{a \in Q; f(a) = g(a) = a\}$ (see 5.1(vii)), so that P is a subgroup of $Q(+)$. Then $Q$is stably nilpotent of class at most 2 iff $f(a) - a$, $g(a) - a \in P$ (or, equivalently, $f^2(a) - 2f(a) + a = g^2(a) - 2g(a) + a = fg(a) - g(a) - f(a) + a = gf(a) - f(a) - g(a) + a = 0$) for every $a \in Q$. In that case, $fg = gf$, and so the quasigroup Q is medial (i.e., it satisfies the identity $xy \cdot uv = xu \cdot yv$).

6. The centre congruence

6.1 Throughout this section, we use the same notation as in the first five sections.

Put $t = t(Q) = \Phi(\mathbf{L}_G(\mathbf{Z}(\tilde{G})))$ (see 1.10(i) and 4.1). Then t is a cancellative congruence of Q (the centre congruence introduced by Smith in [4]) and $(a, b) \in t$ iff $a, b \in Q$ and $b = f(a)$ for some $f \in \mathbf{L}_G(\mathbf{Z}(\tilde{G}))$.

By 4.4(ii), $\mathbf{Z}(G) \subseteq \mathbf{L}_G(\mathbf{Z}(\tilde{G}))$, and hence $s = s(Q) = \Phi(\mathbf{Z}(G)) \subseteq \Phi(\mathbf{L}_G(\mathbf{Z}(\tilde{G})) = t(Q) = t$. Thus, the stability congruence is contained in the centre congruence. If Q is a loop, then $G = \tilde{G}$, $\mathbf{Z}(G) = \mathbf{L}_G(\mathbf{Z}(\tilde{G}))$ and $s = t$ (see also 3.18).

By 1.11(i), $\Psi(t) = \mathbf{L}_G(\mathbf{L}_G(\mathbf{Z}(\tilde{G})) \cdot H(a))$.

6.2 Consider the situation from 4.8. Then, for $x, y \in Q$, $(x, y) \in t$ iff $y = x * u$ for some $u \in R$. Further, $R(\triangle)$ is a subquasigroup of $Q(\triangle)$ and $R(\triangle)$ is a linear quasigroup (see 5.1). Now, define a mapping $\varphi: t \to R$ by $\varphi(x, y) = u$, where

$(x, y) \in t$, $u \in R$ and $y = x * u$ (u is determined uniquely by the pair (x, y)). The congruence t (as a subset of $Q^{(2)}$) is also a subquasigroup of the cartesian square $Q^{(2)}$ of the quasigroup Q and we will show that φ is a homomorphism of this quasigroup t onto the linear quasigroup $R(\triangle)$. Indeed, let $y = x * u$, $z = w * v$, $x, y, w \in Q, u, v \in R$. Then $(x, y)(w, z) = (xv, yz)$, $xw = (f_1(x) * a) * (g_1(y) * b)$, $yz = (f_1(x * u) *) * (g_1(w * v) * b) = ((f_1(x) * a) * g_1(w) * b) * (f_1(u) * g_1(v)) = (xw) * (u \triangle v)$, and hence $\varphi((x, y)(w, z)) = u \triangle v = \varphi(x, y) \triangle \varphi(w, z)$.

Clearly, $\varphi(t) = R$ and the identity congruence id_Q is just one of the blocks of $\mathrm{Ker}(\varphi)$; in fact, $\mathrm{id}_Q = \varphi^{-1}(e)$, e being the neutral element of $Q(*)$. That means, that id_Q (as a quasigroup) is a normal subquasigroup of t.

6.3 Proposition. *Q is a linear quasigroup iff $t(Q) = Q \times Q$.*

Proof. If Q is linear, then $\tilde{G}$ is a normal abelian subgroup of G, and therefore $\mathbf{L}_G(\mathbf{Z}(\tilde{G})) = \tilde{G}$, $\Psi(t) = \mathbf{L}_G(\tilde{G}H(a)) = \mathbf{L}_G(G) = G$ and $t = \Psi\Phi(G) = \Phi(G) = Q \times Q$. Conversely, if $t = Q \times Q$, then $R = Q$ (see 6.2), $Q(*)$ is an abelian group and Q is linear by 4.8.

6.4 For every ordinal number $\alpha \geqq 0$, define a cancellative congruence $t(\alpha) = t(Q, \alpha)$ of Q as follows: $t(0) = \mathrm{id}_Q$; if $\alpha \geqq 0$, then $t(\alpha + 1)$ is the uniquely determined cancellative congruence of Q such that $t(\alpha) \subseteqq t(\alpha + 1)$ and $t(\alpha + 1)/t(\alpha) = t(Q/t(\alpha))$; if $\alpha > 0$ is limit, then $t(\alpha) = \bigcup t(\beta)$, $0 \leqq \beta < \alpha$. The quasigroup Q is said to be centrally nilpotent of class at most α if $t(\alpha) = Q \times Q$. The quasigroup is said to be centrally nilpotent if it is centrally nilpotent of a finite class.

Q is centrally nilpotent of class at most 0 iff it is trivial and Q is centrally nilpotent of class at most 1 iff it is linear (see 6.3).

From 4.4(iv) it follows easily that $s(Q, \alpha) \subseteqq t(Q, \alpha)$ for every $\alpha \geqq 0$. In particular, if Q is stably nilpotent of class at most α, then Q is centrally nilpotent of class at most α. If Q is a loop, then $s(Q, \alpha) = t(Q, \alpha)$ for every $\alpha \geqq 0$ (see 3.18).

6.5 Proposition. *Suppose that Q is centrally nilpotent of class at most n (n finite) and let $Q(*)$ be a loop isotopic to Q. Then $Q(*)$ is nilpotent of class at most n.*

Proof. We shall proceed by induction on n. The result is clear for $n \leqq 1$. Generally, $t(Q) \subseteqq t(Q(*)) = s(Q(*))$, $t(Q)$ is a congruence of $Q(*)$ and $Q/t(Q)$ is isotopic to $Q(*)/t(Q)$ (ve assume that $Q(*)$ is a principal isotope of Q).

6.6 Proposition. *Let Q be centrally nilpotent. If $H(a)$ is soluble, then G is so.*

Proof. By induction on the nilpotence class of Q. We have $\mathcal{M}(Q/t) \cong G/L$, where $L = \mathbf{L}_G(\mathbf{L}_G(\mathbf{Z}(\tilde{G})) \cdot H(a))$. If $H(a)$ is soluble, the $H(a) \cdot \mathbf{L}_G(\mathbf{Z}(\tilde{G}))$ is so and conseuqently L is soluble.

7. Quasigroups isotopic to abelian groups

7.1 Let Q be a quasigroup isotopic to abelian group, i.e., there exists an abelian group $Q(+)$ and $f, g \in \mathscr{S}(Q)$ such that $xy = f(x) + g(y)$ for all $x, y \in Q$.

(i) $\mathscr{L}(Q, a) = \mathscr{L}(Q(+), f(a))\, g$ and $\mathscr{R}(Q, a) = \mathscr{R}(Q(+), g(a))\, f$ for every $a \in Q$.

(ii) $\mathscr{M}_l(Q) = \langle \mathscr{M}(Q(+)), g\rangle$, $\mathscr{M}_r(Q) = \langle \mathscr{M}(Q(+)), f\rangle$ and $\mathscr{M}(Q) = \langle \mathscr{M}(Q(+)), f, g\rangle$.

(iii) $\mathscr{M} = \mathscr{M}(Q(+)) \cong Q(+)$.

(iv) $\mathscr{M}(Q) = \mathscr{M}(Q(+)) \cdot \mathscr{I}(Q, a)$ and $\mathscr{M}(Q(+)) \cap \mathscr{I}(Q, a) = 1$ for every $a \in Q$.

(v) Let $f_1, g_1 \in I(Q, 0)$ be as in 4.8(i). Then $\mathscr{M}(Q) = \langle \mathscr{M}(Q(+)), f_1, g_1\rangle$ (see 4.8(v)).

7.2 Let G be a group such that $G = KH$, where K is an abelian subgroup and H is a subgroup of G. Suppose further that $\mathbf{L}_G(H) = 1$ and that there are $u, v \in H$ with $G = \langle K, u, v\rangle$.

7.2.1 Lemma. $H \cap K = 1$.

Proof. $H \cap K \subseteqq \mathbf{L}_G(H) = 1$.

7.2.2 Lemma. *For all $a \in H$ and $x \in K$, there are transformations q_a of K and p_x of H such that $ax = a_a(x)\, p_x(a)$.*

Proof. $G = KH = HK$.

7.2.3 Lemma. (i) $q_{ab} = q_a q_b$ *for all* $a, b \in H$.

(ii) $p_x(ab) = p_{q_b(x)}(a)\, p_x(b)$ *for all* $a, b \in H$, $x \in K$.

(iii) $p_{xy} = p_y p_x$ *for all* $x, y \in K$.

(iv) $q_a(xy) = q_a(x)\, q_{p_x(a)}(y)$ *for all* $x, y \in K$, $a \in H$.

Proof. (i) and (ii). $q_{ab}(x)\, p_x(ab) = abx = aq_b(x)\, p_x(b) = q_a(q_b(x))\, p_{q_b(x)}(a)\, p_x(b)$ and the result follows from the fact that $H \cap K = 1$.

(iii) and (iv). Similar.

7.2.4 Lemma. *The mapping $a \to q_a$ is an injective homomorphism of the group H into the symmetric group $\mathscr{S}(K)$.*

Proof. By 7.2.3(i), $q_a q_{a^{-1}} = q_{a^{-1}} q_a = q_1 = \mathrm{id}_K$, and so $q_a \in \mathscr{S}(K)$. By 7.2.3(i) again, $a \to q_a$ is a homomorphism. The kernel of this homomorphism is $\mathbf{L}_{G(H)} = 1$.

7.2.5 Lemma. *The mapping $x \to p_{x^{-1}}$ is a homomorphism of K into $\mathscr{S}(H)$ and its kernel is $\mathbf{L}_G(K)$.*

Proof. Similar to that of 7.2.4.

7.2.6 Define a mapping $\varphi: G \to \mathscr{S}(K)$ by $\varphi(xa) = \mathscr{L}(K, x)\, q_a$ for all $x \in K$, $a \in H$.

7.2.7 Lemma. (i) φ *is an injective homomorphism of G into $\mathscr{S}(K)$.*

(ii) $\varphi(x) = \mathscr{L}(K, x)$ *for every* $x \in K$.

(iii) $\varphi(a) = q_a$ *for every* $a \in H$.

Proof. Let $x, y \in K$ and $a, b \in H$. Then $xayb = xq_a(y)\, p_y(a)\, b$ and $\varphi(xayb) = \mathscr{L}(K, xq_a(y))\, q_{p_y(a)b} = \mathscr{L}(K, x)\, \mathscr{L}(K, q_a(y))\, q_{p_y(a)}q_b = \mathscr{L}(K, x)\, q_a\, \mathscr{L}(K, y)\, q_b = \varphi(xa)\, \varphi(yb)$ (by 7.2.3(iv), $\mathscr{L}(K, q_a(y))\, q_{p_y(a)} = q_a \mathscr{L}(K, y)$). We have checked that φ is a homomorphism.

Finally, let $\varphi(xa) = \mathrm{id}_K$. Then $xq_a(y) = y$ for every $y \in K$, $x = xq_a(1) = 1$, $q_a = \mathrm{id}_K$, $a = 1$, $xa = 1$. Thus $\mathrm{Ker}(\varphi) = 1$ and φ is injective.

7.2.8 Lemma. *The exists a homomorphism $\psi\colon G \to \mathscr{S}(H)$ such that:*

(i) $\mathrm{Ker}(\psi) = \mathbf{L}_G(K)$.

(ii) $\psi(a) = \mathscr{L}(H, a)$ *for every* $a \in H$.

Proof. This is dual to 7.2.7.

7.2.9 Lemma. *If H is finite and* $\mathrm{card}(K) > (\mathrm{card}(H) - 1)!$, *then* $\mathbf{L}_G(K) \neq 1$.

Proof. This follows immediately from 7.2.8.

7.2.10 Lemma. *If* $n = \mathrm{card}(K)$ *is finite, then H is finite and* $\mathrm{card}(H) \leqq (n - 1)!$.

Proof. This follows immediately from 7.2.7(i).

7.2.11 Define a binary operation $*$ on K by $x * y = q_u(x)\, q_v(y)$ for all $x, y \in K$. Then $K(*)$ is a quasigroup (isotopic to K) and $\mathscr{M}(K(*)) = \varphi(G) \cong G$, $\tilde{\mathscr{M}}(K(*))\, \mathscr{M}(K) \cong K$, $\mathscr{I}(K(*), 1) = \varphi(H) \cong H$.

7.3 Proposition. *The following conditions are equivalent for a group G:*

(i) *G is isomorphic to the multiplication group of a quasigroup isotopic to abelian group.*

(ii) *G contains subgroups K, H such that $G = KH$, K is abelian,* $\mathbf{L}_G(H) = 1$ *and there exist $u, v \in H$ with $G = \langle K, u, v\rangle$.*

Proof. Combine 7.1 and 7.2.

7.4 Proposition. *Let Q be a non-trivial finite quasigroup isotopic to abelian group. If* $\mathrm{card}(Q) > (\mathrm{i}(Q) - 1)!$, *then* $t(Q) \neq \mathrm{id}_Q$.

Proof. Put $G = \mathscr{M}(Q)$, $K = \tilde{\mathscr{M}}(Q)$, $H = \mathscr{I}(Q, 0)$ (see 7.1). We must show that $\mathbf{L}_G(K) \neq 1$. However, $\mathrm{card}(K) = \mathrm{card}(Q)$, $\mathrm{card}(H) = \mathrm{i}(Q)$ and the result follows from 7.2.9.

8. Characterizations of the multiplication groups of quasigroups and loops

8.1 Let H be a subgroup of a group G such that $\mathbf{L}_G(H) = 1$ and let $Q = G/H = \{xH; x \in G\}$ denote the set of left cosets modulo H. Then we have an injective homomorphism π of G into the symmetric group $\mathscr{S}(Q)$ defined by $\pi(x)(yH) = xyH$ for all $x, y \in G$. Put $P = \pi(G)$, so that P is a subgroup of $\mathscr{S}(Q)$ and $P \cong G$. Moreover, $\pi(H) = \mathrm{St}(P, Q, H)$. Further, let A be a stable transversal to H in G. For

every $x \in G$, there is just one $f(x) \in A$ such that $f(x)\,H = xH$ (or, $x^{-1}f(x) \in H$). Now, we shall define a binary operation $*$ on Q by $(xH) * (yH) = f(x)\,yH$ (clearly, this definition is correct).

(i) $\mathscr{L}(Q(*), xH) = \pi(f(x)) \in P$ for every $x \in G$. In particular, $Q(x)$ is a left quasigroup.

(ii) $Q(*)$ is a quasigroup.

It remains to show that $Q(*)$ is a right quasigroup. For, let $(x_1H) * (yH) = (x_2H) * (yH)$. Then $f(x_1)\,yH = f(x_2)^{-1}f(x_1) \in yHy^{-1}$, $f(x_2) = f(x_1)$ (since A is stable) and $x_1H = x_2H$. We have shown that $Q(*)$ is right cancellative. Finally, let $y, z \in H$. Since A is stable, A is also a transversal to yHy^{-1} in G and there is $x \in G$ such that $f(x) \in zy^{-1} \cdot yHy^{-1}$. Then $f(x)\,y \in zH$, i.e. $(xH) * (yH) = zH$.

(iii) $Q(*)$ is a right loop (H is a right neutral element); $Q(*)$ is a loop iff $1 \in A$.

(iv) $\pi(\langle A\rangle) = \mathscr{M}_r(Q(*)) \subseteq P$; $\mathscr{M}_r(Q(*)) = P$ iff $G = \langle A\rangle$.

(v) Suppose that there is a transversal B to H in G such that $[A, B] \subseteq H$ (i.e., A, B are H-conneted). Then, for every $x \in G$, there is uniquely determined $g(x) \in B$ with $xH = g(x)\,H$, i.e. $x^{-1}g(x) \in H$. Now, $(xH) * (yH) = f(x)\,yH = f(x)\,g(y)\,H = g(y)\,f(x)\,H = g(y)\,xH$, since $g(y)^{-1}f(x)^{-1}\,g(y)\,f(x) \in H$. From this, $\mathscr{R}(Q(*)), yH) = \pi(g(y)) \in P$. Consequently, $\pi(\langle B\rangle) = \mathscr{M}_r(Q(*)) \subseteq P$ and $(\langle A, B\rangle) = \mathscr{M}(Q(*)) \subseteq P$. Clearly, $\mathscr{M}_r(Q(*)) = P$ iff $G = \langle B\rangle$ and $\mathscr{M}(Q(*)) = P$ iff $G = \langle A, B\rangle$.

(vi) $Q(*)$ is commutative iff $[A, A] \subseteq H$ (i.e., A is H-selfconnected). In that case, $Q(*)$ is a loop and $\mathscr{M}(Q(*)) \subseteq P$.

(vii) $\mathscr{I}_l(Q(*), H) \subseteq \pi(H)$; if $\mathscr{M}_l(Q(*)) = P$, then $\mathscr{I}_l(Q(*), H) = H$.

(viii) $\pi(H) \cap \mathscr{M}(Q(*)) = \mathscr{I}(Q(*), H) \cap P$. If $\mathscr{M}(Q(*)) = P$, then $\mathscr{I}(Q(*), H) = \pi(H)$.

8.2 Corollary. *Let H be a subgroup of a group G. The following conditions are equivalent:*

(i) $\mathbf{L}_G(H) = 1$ *and there exists a stable transversal A to H in G such that* $G = \langle A\rangle$.

(ii) *there exists a quasigroup Q with a right neutral element e and an isomorphism* $\varphi\colon \mathscr{M}_l(Q) \to G$ *such that* $\varphi(\mathscr{I}_l(Q, e)) = H$.

(iii) *There exist a quasigroup Q and an isomorphism* $\varphi\colon \mathscr{M}_l(Q) \to G$ *such that* $\varphi(\mathscr{I}_l(Q, a)) = H$ *for some* $a \in Q$.

8.3 Corollary. *Let H be a subgroup of a group G. The following conditions are equivalent:*

(i) $\mathbf{L}_G(H) = 1$ *and there exists a stable transversal A to H in G such that* $1 \in A$ *and* $G = \langle A\rangle$.

(ii) *There exist a loop Q and an isomorphism* $\varphi\colon \mathscr{M}(Q) \to G$ *such that* $\varphi(\mathscr{I}_l(Q, 1)) = H$.

8.4 Corollary. *Let H be a subgroup of a group G. The following conditions are equivalent:*

(i) $\mathbf{L}_G(H) = 1$ *and there exist H-connected transversals A, B to H in G such that* $G = \langle A, B\rangle$.

(ii) *There exist a loop A and an isomorphism* $\varphi: \mathscr{M}(Q) \to G$ *such that* $\varphi(\mathscr{I}(Q)) = H$.

8.5 Let G be a transitive permutation group on a non-empty set Q. Take $a \in Q$ and put $H = \mathrm{St}(G, Q, a)$ and $Q_1 = G/H$ (the left cosets – see 8.1). We have a bijection $\varphi: Q \to Q_1$ such that $\varphi(x) = fH, x \in Q, f \in G, x = f(a)$. Moreover, since G is transitive, $\mathbf{L}_G(H) = 1$, $\pi: G \to P \subseteq \mathscr{S}(Q_1)$ is an isomorphism (see 8.1) and $\varphi f(x) = \pi(f)\,\varphi(x)$ for all $x \in Q$ and G. The permutation groups G (on Q) and P (on Q_1) are similar.

Now, suppose that there is defined a binary operation $*$ on Q_1 such that $Q_1(*)$ is a quasigroup. Define $\circ$ on Q by $x \circ y = \varphi^{-1}(\varphi(x) * \varphi(y))$. Then $\varphi: Q(\circ) \to Q_1(*)$ is an isomorphism. Obviously, $\mathscr{M}_l(Q(\circ)) = G$ $(\mathscr{M}(Q(\circ)) = G)$ iff $\mathscr{M}_l(Q_1(*)) = P$ $(\mathscr{M}(Q_1(*)) = P)$.

8.6 Corollary. *Let G be a permutation group on a non-empty set Q, $a \in Q$ and $H = \mathrm{St}(G, Q, a)$. The following conditions are equivalent:*

(i) *G is transitive on Q and there exists a stable transversal A to H in G such that $g = \langle A\rangle$ (and $\mathrm{id}_Q \in A$).*

(ii) *There exists a quasigroup (loop) $Q(*)$ such that $\mathscr{M}_l(Q(*)) = G$, $\mathscr{I}_l(Q(*), a) = H$ (and $a = 1$).*

8.7 Corollary. *Let G be a permutation group on a non-empty set Q, $a \in Q$, $H = \mathrm{St}(G, Q, a)$. The following conditions are equivalent:*

(i) *G is transitive on Q and there exist H-connected transversals A, B to H in G such that* $G = \langle A, B\rangle$.

(ii) *There exists a loop $Q(*)$ such that $\mathscr{M}(Q(*)) = G$, $a = 1$ and $\mathscr{I}(Q(*)) = H$.*

8.8 Let H_1 be a subgroup of a group G such that $\mathbf{L}_G(H_1) = 1$ and let A_1, B_1 be H_1-semiconnected stable transversals to H_1 in G. Take $u \in A_1$, $v \in B_1$ and put $A = A_1u^{-1}$, $B = B_1v^{-1}$. Then there is $x \in G$ such that A, B are H-connected transversals to H in G, $H = H_1^x$.

Now, let Q, π, P, $*$ have the same meaning as in 8.1; $Q(*)$ is a loop and $\mathscr{M}(Q(*)) \subseteq P \cong G$. By 8.1(v), $\mathscr{M}(Q(*)) = \pi(\langle A, B\rangle)$.

Define permutations α and β of Q by $\alpha(xH) = uxH$ and $\beta(xH) = vxH$, resp., and put $(xH) \circ (yH) = \alpha(xH) * \beta(yH) = (uxH) * (vyH) = f(ux)\,vyH$. Then $Q(\circ)$ becomes a quasigroup.

Clearly, $\mathscr{L}(Q(\circ), xH) = \pi(f(ux))\,\pi(v)$, and so $\mathscr{M}_l(Q(\circ)) = \pi(\langle A, v\rangle) = \langle \mathscr{M}_l(Q(*)), \pi(v)\rangle \subseteq P$. Further, $(xH) \circ (yH) = f(ux)\,vyH = g(vy)\,f(ux)\,H = g(vy)\,uxH$ (see 8.1(v)), and hence $\mathscr{R}(Q(\circ), yH) = \pi(g(vy))\,\pi(u)$, $\mathscr{M}_r(Q(\circ)) =$

$= \pi(\langle B, v\rangle) = \langle \mathcal{M}_r(Q(*), \pi(u)\rangle \subseteq P$. Finally, $\mathcal{M}(Q(\circ)) = \pi(\langle A, B, u, v\rangle) =$
$= \pi(\langle A_1, B_1\rangle) \subseteq P$ and $\mathcal{M}(Q(\circ)) = P$ iff $\langle A_1, B_1\rangle = G$.

8.9 Corollary. *Let H be a subgroup of a group G. The following conditions are equivalent:*

(i) $\mathbf{L}_G(H) = 1$ *and there exist H-semiconnected stable transversals A, B to H in G such that $G = \langle A, B\rangle$.*

(ii) $\mathbf{L}_G(H) = 1$ *and there exist H-connected transversals C, D to H in G and elements $u, v \in G$ such that $G = \langle C, D, u, v\rangle$.*

(iii) *There exist a quasigroup Q and an isomorphism $\varphi: \mathcal{M}(Q) \to G$ such that $\varphi(\mathcal{I}(Q, a)) = H$ for some $a \in Q$.*

References

[1] Belousov V. D., Foundations of the theory of quasigroups and loops, Nauka Moscow 1967.

[2] Drápal A., Kepka T., Multiplication groups of quasigroups and loops I. (to appear).

[3] Kepka T., Niemenmaa M., On loops with cyclic inner mapping groups, Arch. Math. 60 (1983), 233–236.

[4] Smith J. D. H., Multiplication groups of quasigroups, Preprint 603, Technische Hochschule Darmstadt, 1981.