**Aleš Drápal, Faculty of Mathematics and Physics,
Charles University, Prague**

# FROM MULTIPLICATION GROUPS TO CONJUGACY CLOSEDNESS

OUTLINE OF THE DOCTORAL THESIS

The thesis consists of 8 chapters based on nine papers that are listed below. Chapter I is based on two papers, otherwise each chapter corresponds to one paper. All the papers have only one author (i.e., Aleš Drápal):

Chapter I is based upon the papers
Multiplication groups of free loops I, II, *Czech. Math. J.* **46** (1996), 121–131 and 201–220.

Chapter II is based upon the paper
Multiplication groups of finite loops that fix at most two points, *J. Algebra* **235** (2001), 154–175.

Chapter III is based upon the paper
Multiplication groups of loops and projective semilinear transformations in dimension two, *J. Algebra* **251** (2002), 256–278.

Chapter IV is based upon the paper
Orbits of inner mapping groups, *Monatsh. Math.* **134** (2002), 191–206.

Chapter V is based upon the paper
Conjugacy closed loops and their multiplication groups, *J. Algebra* **272** (2004), 838–850.

Chapter VI is based upon the paper
On multiplication groups of left conjugacy closed loops, *Comment. Math. Univ. Carolinae* **45** (2004), 223–236.

Chapter VII is based upon the paper
Generating free groups by loop translations, *Europ. J. Combinatorics* **16** (1995), 561–565.

Chapter VIII is based upon the paper
On free Frobenius groups generated by left translations, *Rivista di Matematica Pura ed Applicata* **18** (1996), 107–119.

Further papers of the author that are relevant to the thesis:

1. (with T. Kepka) Alternating groups and Latin squares, *Europ. J. Combinatorics* **10** (1989), 175–180.
2. (with T. Kepka) Loops whose translations generate the alternating group, *Czech. Math. J.* **40** (1990), 128–136.
3. (with T. Kepka) Multiplication groups of quasigroups and loops I, *Acta Univ. Carolinae* **34/1** (1993), 85–99.
4. (with T. Kepka and P. Maršálek) Multiplication groups of quasigroups and loops II, *Acta Univ. Carolinae* **35/1** (1994), 9–29.

5. On multiplication groups of relatively free quasigroups isotopic to abelian groups, *Czech. Math. J.* (to appear).
6. Structural interactions of conjugacy closed loop (submitted).
7. On left conjugacy closed loops with a nucleus of index two, *Abh. Math. Sem. Univ. Hamburg* (to appear).

The subsequent text discusses results contained in the thesis. It starts from the definitions of loops and quasigroups, formulates the problems and explains, to some extent, their context. Results that are proved in the thesis appear in **bold**. The text is followed by a list of references, and by a short summary in Czech.

## 1. Loops

By a *quasigroup* one usually understands a binary system $Q(\cdot)$ such that the equations

$$a \cdot x = b \quad \text{and} \quad y \cdot a = b$$

have unique solutions $x$ and $y$ for all $a, b \in Q$. In such a situation one writes $x = a\backslash b$ and $y = b/a$. Both $\backslash$ and $/$ can be regarded as binary operations on $Q$, and an alternative way to define a quasigroup is to consider a system $Q(\cdot, \backslash, /)$ that satisfies the laws

$$x \cdot (x\backslash y) = y = x\backslash(x \cdot y) \quad \text{and} \quad (x \cdot y)/y = x = (x/y) \cdot y.$$

Both ways of definition are equivalent. We shall usually prefer the former approach, because of its brevity. Nevertheless, the standard notions of universal algebra (homomorphisms, subquasigroups, free quasigroups etc.) are always to be related to the definition with the three explicit binary operations.

There are two further laws that easily follow from the above ones and show the symmetric role of the three binary operations:

$$x/(y\backslash x) = y \quad \text{and} \quad (x/y)\backslash x = y.$$

A *loop* $Q = Q(\cdot, 1)$ is a quasigroup $Q(\cdot)$ that possesses a neutral element 1. Thus $x \cdot 1 = 1 \cdot x = x$ for all $x \in Q$, and hence $x/1 = x = 1\backslash x$.

When writing loop terms, one often uses the convention that an omitted multiplication has higher precedence than the explicit one. Thus $xy \cdot z$ is a shorter way of expressing $(x \cdot y) \cdot z$.

Multiplication tables of finite quasigroups are (finite) latin squares and vice versa. Loops correspond to latin squares in their normalized form. Such an analogy can be used in the infinite case as well, but there it is far less illuminating.

## 2. Free loops

Free loops were described by Evans [14] in 1952. The description is easy, but not without importance. It was one of the first free nonassociative objects for which an explicit description was obtained, and it later became a model example for term rewriting systems.

Like groups, free loops can be obtained as a set of irreducible elements in a looser free object. For a set $X$ consider an absolutely free algebra $W = W(\cdot, \backslash, /, 1)$ over $X$. Each element of $W$ is called a *loop term*. Such a term is called *irreducible* if it contains no subterm of one of the forms $u\backslash(u \cdot v), u \cdot (u\backslash v), (u \cdot v)/v, (u/v) \cdot v, u/(v\backslash u), (u/v)\backslash u$ and $u \cdot 1, 1 \cdot u, 1\backslash u, u/1$, where $u$ and $v$ are loop terms.

Each loop term can clearly be simplified to an irreducible one by substitutions that express loop identities. The relation corresponding to a simplifying step induces an equivalence that is the congruence, factor over which gives a free loop. A confluence argument can be employed to show that each congruence class contains exactly one irreducible loop term.

Free quasigroups can be obtained in the same way.

## 3. Multiplication groups

With each element $a$ of a loop $Q$ one associates its *left translation* $L_a$ and *right translation* $R_a$. They are defined by $L_a(x) = a \cdot x$ and $R_a(x) = x \cdot a$. The permutation group generated by all left translations is called *left multiplication group* and will be denoted by $\mathcal{L}(Q)$ or just $\mathcal{L}$. One defines similarly *right multiplication group* $\mathcal{R}$, and the *multiplication group* $\operatorname{Mlt} Q$ is generated by both left and right translations.

The stabilizer $(\operatorname{Mlt} Q)_1$ is called the *inner mapping group* and will be denoted by $\operatorname{Inn} Q$. An easy application of the standard way that is used to derive generators of a subgroup from the generators of a group gives a set of generators $L_{xy}^{-1} L_x L_y$, $R_{yx}^{-1} R_x R_y$ and $R_x^{-1} L_x$, where $x, y \in Q$.

The question which permutation group can be obtained as a multiplication group of a loop is called the *inverse problem* for multiplication groups. Another class of problems we shall address asks how a structure of $\operatorname{Inn} Q$ influences the structure of $Q$.

We shall pay special attention to permutations of types $L_{xa}^{-1} R_a L_x$ and $R_{ax}^{-1} L_a R_x$, where $a, x \in Q$. Each such permutation fixes points $a$ and 1. Suppose that $\operatorname{Mlt} Q$ is a Frobenius group (i.e., each nonidentity permutation fixes at most one point, and the group is transitive, but not regular). Then all such permutations have to be the identity mapping. However, if $L_{xa} = R_a L_x$ for all $a, x \in Q$, then $xa \cdot y = xy \cdot a$ for all $a, x, y \in Q$. It is easy to see that such identity holds if and only if $Q$ is an abelian group (indeed, setting $x = 1$ yields $ay = ya$, and hence $x \cdot ya = ya \cdot x = yx \cdot a = xy \cdot a$). Of course if $Q$ is an abelian group,

then $\operatorname{Mlt} Q \cong Q$ is a regular permutation group. We have proved that **multiplication group of a loop is never a Frobenius group**.

We shall say that a permutation group is a *Zassenhaus group* if it is transitive, but not regular or Frobenius, and if each nonidentity permutation fixes at most two points (some authors use the notion of Zassenhaus groups for a narrower class of groups). Since multiplication groups of loops cannot be Frobenius groups, it is natural to ask if they can be Zassenhaus groups. In Chapter I of the thesis one proves that **the multiplication group of a free loop is a Zassenhaus group** and Chapter II contains a proof that **the multiplication group of a finite loop is never a Zassenhaus group**. Subsequent sections explain (amongst others) where the difficulty of the proof rests.

## 4. Conjugacy closedness and Zassenhaus groups

Suppose first that $Q$ is a loop in which left translations are closed under composition, i.e., for all $a, b \in Q$ there exists $c \in Q$ such that $L_a L_b = L_c$. By applying both sides of the equation to 1 we see that $c = L_c(1) = L_a L_b(1) = ab$. Hence the equation gives the associative law $a \cdot bx = ab \cdot x$, and $Q$ is a group. Let us thus turn to a weaker condition.

Assume that the left translations of a loop $Q$ are closed under conjugation. Thus for all $a, b \in Q$ there exists $c \in Q$ such that $L_a L_b L_a^{-1} = L_c$. It follows $L_a L_b = L_c L_a$, $ab = ca$, and $c = (ab)/a = R_a^{-1} L_a(b)$. We shall write $T_a$ as a shortcut for $R_a^{-1} L_a$. Loops that are closed under conjugation are called *left conjugacy closed* (LCC) loops. The LCC law can be hence expressed as $L_a L_b L_a^{-1} = L_{T_b(a)}$ or

$$x \cdot (y \cdot z) = ((x \cdot y)/x) \cdot (x \cdot z).$$

This equation can also be written as $L_x R_z = R_{xz} R_x^{-1} L_x$ or $R_{xz}^{-1} L_x R_z = R_x^{-1} L_x$. Replacing $x$ by $a$, and $z$ by $x$ gives

$$R_a^{-1} L_a = R_{ax}^{-1} L_a R_x.$$

The mappings on the right are those that have been mentioned already in Section 3. In fact, the mapping on the left is of the same form, since $R_a^{-1} L_a = R_{a\cdot 1}^{-1} L_a R_1$. We see that the LCC law is equivalent to the fact that the mapping $R_{ax}^{-1} L_a R_x$ does not depend on the choice of $x \in Q$. This is how LCC loops are connected to the inverse problem for Zassenhaus groups. The discovery of this connection is described in Chapter II of the thesis, and we shall briefly explain it below.

Let us first mention that RCC loops are those in which mappings $L_{xa}^{-1} R_a L_x$ do not depend on the choice of $x$, by a mirror argument. Loops that are both LCC and RCC are called *conjugacy closed*.

Suppose now that $Q$ is a finite loop of $n$ elements such that $\operatorname{Mlt} Q$ is a Zassenhaus group. Suppose first that $\operatorname{Mlt} Q$ is not triply transitive. Fix $a \in Q$, $a \neq 1$. Let $C$ be an orbit of $(\operatorname{Mlt} Q)_{1,a} = (\operatorname{Inn} Q)_a$ (sets $\{1\}$

and $\{a\}$ are not regarded as orbits of $(\operatorname{Inn} Q)_a$). Denote the size of $C$ by $k$ and choose $c \in C$. Group $(\operatorname{Inn} Q)_a$ is semiregular and hence all its orbits are of the same size. There are at least two such orbits, because $\operatorname{Mlt} Q$ is assumed not to be triply transitive. Thus $k \leq (n-2)/2 < n/2$. Consider all mappings $R_{ax}^{-1} L_a R_x$, $x \in Q$. There are $n$ choices for $x$ and $k$ possible targets for $c$. Hence there exists $d \in C$ such that the number of $x$ with $R_{ax}^{-1} L_a R_x(c) = d$ is $\geq n/k > 2$. Therefore $a \cdot cx = d \cdot ax$ for at least three $x \in Q$. The mapping $L_a^{-1} L_d^{-1} L_a L_c$ fixes at least three $x \in Q$, and so it must be the identity. We thus see that the equality $a \cdot cx = d \cdot ax$ holds for all $x \in Q$, and so $L_a L_c L_a^{-1} = L_d$. A mirror argument yields RCC. We have proved that **if** $\operatorname{Mlt} Q$ **is a finite Zassenhaus group which is not triply transitive, then** $Q$ **must be conjugacy closed**.

In Section 7 we shall observe that $\operatorname{Mlt} Q$ is never a Zassenhaus group, if $Q$ is CC. This leaves open the case of triply transitive $\operatorname{Mlt} Q$. Of course, a triply transitive Zassenhaus group is sharply triply transitive. These groups have been classified by Zassenhaus [51], and they are isomorphic either to $PGL(2, q)$, or to its twisted version $M(q)$. This is where the real difficulty rests, and most of Chapter II is concerned with these two special cases.

## 5. Some standard loop notions

Let $Q$ be a loop. Each congruence on $Q$ is carried by a *normal subloop*, say $S$. A subloop $S$ is normal if and only if $x(yS) = (xy)S$, $(Sx)y = S(xy)$ and $xS = Sx$, for all $x, y \in Q$. This can be expressed also by an assertion that a subloop $S$ is normal if and only if $\operatorname{Inn} Q$ acts on $S$. Another way how to characterize normal subloops is to say that they coincide with those blocks of the permutation group $\operatorname{Mlt} Q$ that contain the element 1.

Elements $a \in Q$ that associate on the left form the *left nucleus* $N_\lambda = N_\lambda(Q) = \{a \in Q;\ a \cdot xy = ax \cdot y \text{ for all } x, y \in Q\}$. By shifting the position of $a$ to the right one gets the middle nucleus $N_\mu$ and the right nucleus $N_\rho$. It is not difficult to show that every nucleus forms a subloop. Such a subloop does not have to be necesarilly normal. The intersection $N = N(Q) = N_\lambda \cap N_\mu \cap N_\rho$ is called the *nucleus* of $Q$. Neither $N$ has to be normal.

A *centre* $Z(Q)$ of $Q$ is formed by all elements that associate and commute at every position. Thus $Z(Q) = \{a \in N(Q);\ ax = xa \text{ for all } x \in Q\}$. It can be observed immediately that $N_\rho$ is exactly the set of those $x \in Q$ that are fixed by every $\varphi \in \mathcal{L}_1$, that $N_\lambda$ are the fixpoints of $\mathcal{R}_1$, and that $Z(Q)$ corresponds to the points fixed by $\operatorname{Inn} Q$. Points fixed by a stabilizer always form a block of a permutation group, and so we see that $Z(Q)$ is always a normal subloop.

**Elements** $a \in Z(Q)$ **can also be characterized by the property that** $L_{xa}^{-1} R_a L_x$ **(or** $R_{ax}^{-1} L_a R_x$**) is the identity mapping for all** $x \in$

$Q$**.** Indeed, the claim states $xa \cdot y = xy \cdot a$ for all $x, y \in Q$. If $x = 1$, then $ya = ay$, and so $xy \cdot a = a \cdot xy = x \cdot ay = x \cdot ya$. The equality $a \cdot xy = ax \cdot y$ follows by symmetry, and the rest is easy. This observation appears as Lemma 1.1 of Chapter IV, and we shall say more about its consequences in Section 10.

An *autotopy* of a loop $Q$ is a triple $(\alpha, \beta, \gamma)$ such that $\alpha(x) \cdot \beta(y) = \gamma(xy)$ for all $x, y \in Q$. All autotopies form a group. The conditions $a \in N_\lambda$, $a \in N_\mu$ and $a \in N_\rho$ can be clearly expressed by assertions that the triples $(L_a, \mathrm{id}_Q, L_a)$, $(R_a^{-1}, L_a, \mathrm{id}_Q)$ and $(\mathrm{id}_Q, R_a, R_a)$ are autotopies, respectively.

The definition of LCC loops can be expressed by autotopies as well. We obtain that $Q$ is an LCC loop if and only $(T_x, L_x, L_x)$ is an autotopy for each $x \in Q$.

Note that a permutation $\alpha$ of $Q$ is an automorphism if and only if $(\alpha, \alpha, \alpha)$ is an autotopism. Our treatment of LCC loops by means of autotopisms will use the famous $\beta, \alpha$ *Lemma: If* $(\beta, \alpha, \alpha)$ *is an autotopism and* $\alpha(1) = 1$*, then* $\alpha = \beta \in \mathrm{Aut}(Q)$. The proof of the lemma immediately follows from $\beta(x)\alpha(1) = \alpha(x)$. Despite its easiness, the $\beta, \alpha$ Lemma can have striking applications.

## 6. Basic properties of LCC loops

Let $Q$ be an LCC loop and consider $a \in Q$. Then the composition $(R_a^{-1}, L_a, \mathrm{id}_Q)(L_a, \mathrm{id}_Q, L_a)$ equals $(T_a, L_a, L_a)$, which is an autotopism. Hence if one of the factors in the product is an autotopism, the other one has to be an autotopism as well. Since the factors express inclusion of $a$ to $N_\lambda$ or $N_\mu$, respectively, we see that $N_\lambda = N_\mu$ in all LCC loops. A similar argument applied to the equality $(\mathrm{id}_Q, R_a^{-1}, R_a^{-1})(T_a, L_a, L_a) = (T_a, T_a, T_a)$ gives $T_a \in \mathrm{Aut}\, Q \Leftrightarrow a \in N_\rho$.

By composition, $(T_{xy}^{-1} T_x T_y, L_{xy}^{-1} L_x L_y, L_{xy}^{-1} L_x L_y)$ is an autotopism for all $x, y \in Q$ (we still assume that $Q$ is LCC). Since $\beta, \alpha$ Lemma can be applied to this autotopism, we see that $T_{xy}^{-1} T_x T_y = L_{xy}^{-1} L_x L_y \in \mathrm{Aut}\, Q$ for all $x, y \in Q$. Since $\mathcal{L}_1$ is generated by the mappings of this form, we get $\mathcal{L}_1 \leq \mathrm{Aut}\, Q$. Such loops are called $A_\ell$-loops. We have thus proved that LCC loops are $A_\ell$-loops.

These facts (cf. [33]) were known before the paper [10] corresponding to Chapter VI was published. They are repeated in the beginning of the paper. New results start with Theorem 2.8, which we shall now set out.

It states that **there exists a unique homomorpism** $\Lambda : \mathcal{L} \to \mathrm{Inn}\, Q$ **such that each** $L_x$ **is mapped upon** $T_x$**. One has** $\Lambda(\varphi) = \varphi$ **for each** $\varphi \in \mathcal{L}_1$ **and** $\mathrm{Ker}\, \Lambda = Z(\Lambda) = \{R_x; x \in Q\} \cap \mathcal{L}$**.**

The proof is surprisingly easy, and uses again the $\beta, \alpha$ Lemma. We need to show that $L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n} = \mathrm{id}_Q$ implies $T_{x_1}^{\varepsilon_1} \dots T_{x_n}^{\varepsilon_n} = \mathrm{id}_Q$ for all $x_1, \dots, x_n \in Q$ and $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}$. The triples $(T_{x_i}^{\varepsilon_i}, L_{x_i}^{\varepsilon_i}, L_{x_i}^{\varepsilon_i})$ are

autotopisms for every $i$, $1 \leq i \leq n$, and hence

$$(T_{x_1}^{\varepsilon_1} \dots T_{x_n}^{\varepsilon_n}, L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n}, L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n})$$

is an autotopism as well. Since the two right-hand members of this triple are assumed to equal $\mathrm{id}_Q$, it follows that $T_{x_1}^{\varepsilon_1} \dots T_{x_n}^{\varepsilon_n} = \mathrm{id}_Q$, by the $\beta, \alpha$ Lemma.

We have $\Lambda(\varphi) = \varphi$ whenever $\varphi = L_{xy}^{-1} L_x L_y$ for some $x, y \in Q$, by $T_{xy}^{-1} T_x T_y = L_{xy}^{-1} L_x L_y$. Such mapping generate $\mathcal{L}_1$, and so $\Lambda(\varphi) = \varphi$ for all $\varphi \in \mathcal{L}_1$.

The part about the kernel can be obtained in a straightforward manner as well.

The existence of the homomorphism $\Lambda$ made the structure of LCC loops far more accessible than it had been hoped before. We shall mention two applications that can be found in Chapter VI of the thesis; far more applications appear in papers that have been submitted or are being developed and which are not subject of the thesis.

From the existence of $\Lambda$ one quickly derives that **LCC loops of prime order are abelian groups** (Theorem 2.11). (This does not mean there is a direct analogy with groups—there exists, e.g., a simple LCC loop of order 8).

For the other result we need to introduce the notion of an *associator subloop* $A(Q)$. By that we mean the least normal subloop $A$ of $Q$ such that $Q/A$ is a group. Theorem 3.5 of Chapter VI states:

**Let $Q$ be a left conjugacy closed loop. Denote by $\mathcal{L}$ and $\mathcal{R}$ the left and right multiplication group of $Q$, respectively. Then**

$$[\mathcal{L}, \mathcal{R}] = \langle \mathcal{R}_u;\ u \in Q \rangle \trianglelefteq \mathrm{Mlt}\, Q,$$

**and the orbits of $[\mathcal{L}, \mathcal{R}]$ coincide with the cosets modulo the associator subloop $A(Q)$.**

## 7. Conjugacy closed loops

Conjugacy closed loops were first defined by Soikis [41] in 1970 under the name of K-loops. (He called LCC loops LK-loops and RCC loops RK-loops.) Constructions involving CC loops were known already before, since each loop with a nucleus of index two is conjugacy closed. Soikis used different terminology than that one which was coined by Goodaire and Robinson in their paper [16] from 1982. They most probably were not aware of the work of Soikis. Even if they had been, they probably would have chosen the new name anyway, because they seemed to dislike the Soviet habit of denoting new classes of loops by combinations of capital letters. By irony, the only Soviet notation that became widely accepted is that of G-loops, which is exactly the class of loops that motivated Goodaire and Robinson to study conjugacy closed loops. A loop $Q$ is by definition a *G-loop* if and only if all loops isotopic to $Q$ are isomorphic to $Q$. Groups are G-loops, and CC loops

are (in some sense) the widest class of loops that are G-loops with naturally defined isotopies. G-loops are not a central notion of the thesis, and so this topic will not be explored here further. However, we shall say more about the problem that Goodaire and Robinson found as an obstacle for developing the structural theory of CC loops. The problem is whether every nontrivial CC loop $Q$ possesses a nontrivial nucleus.

This problem was solved by Basarab [3] in 1991. He does not seem to have been aware of results by Goodaire and Robinson, and his own result does not seem to have been noticed outside former Soviet Union up to 2002. He studied *universal LCC loops*, i.e. LCC loops $Q$ which have the property that every loop isotopic to $Q$ is an LCC loop as well. He proved that in such a case $Q/N_\lambda$ has to be an abelian group.

In a CC loop $N_\lambda = N_\mu = N_\rho$, by results of Section 6. A CC loop is a G-loop, and hence a universal LCC loop. Thus $Q/N$ is an abelian group whenever $Q$ is a CC loop. A proof of this fact, which is based on Basarab's paper, but uses a somewhat different argument, appears in Chapter V as Corollary 4.5. Theorem 5.5 of Chapter VI shows that Basarab's argument can be used in the converse direction as well. Hence **an LCC loop $Q$ is a universal LCC loop if and only if $Q/N_\lambda$ is an abelian group**.

Let us now return to arguments of Section 4. Let $Q$ be a CC loop such that $\mathrm{Mlt}\, Q$ is a Zassenhaus group, and let $N$ be the nucleus of $Q$. Each $L_{xy}^{-1} L_x L_y$, where $x, y \in Q$, fixes every element of $N$. If $|N| \geq 3$, then these mappings have to be the identity mappings, which means $L_{xy} = L_x L_y$ for all $x, y \in Q$. Such an equality expresses the associative law, and it is easy to see that $Q$ cannot be a group. (If $Q$ is a group, then $T_a$ fixes the elements of a subgroup generated by $a$. Hence each $a \in Q$ has to be of order two, and $Q$ is abelian of exponent two.) It remains to consider the case $|N| = 2$. Then each mapping of $\mathrm{Inn}\, Q$ has to move within the cosets modulo $N$, since $Q/N$ is abelian. It follows that $|\mathrm{Inn}\, Q| = 2$, and that the only nonidentity permutation of $\mathrm{Inn}\, Q$ exchanges the two elements of $xN$, for every $x \notin N$. It is easy to refute the existence of such a loop by elementary means. For the sake of brevity one can also employ a theorem discussed in Section 10, by which $\mathrm{Inn}\, Q$ is never a cyclic group. We have verified that **if $Q$ is a CC loop, then $\mathrm{Mlt}\, Q$ is not a Zassenhaus group**.

Lemma 2.4 of Chapter II proves the same fact only for loops that are finite, and proceeds by somewhat different means. The reason is that the paper corresponding to Chapter II was written without the knowledge of Basarab's result. However, the proof given in Chapter II is short as well. It is based on a separate proof that $\mathrm{Mlt}\, Q$ would have to be 2-transitive (the proof belongs to Niemenmaa and Kepka [23]) and on some basic properties of finite Frobenius groups.

The homomorphism $\Lambda$ was first discovered for CC loops (see Theorem 3.1 of Chapter V). An important difference when compared to

more general case of CC loops is the fact that **in a CC loop the homomorphism $\Lambda : \mathcal{L} \to \operatorname{Inn} Q$, $L_x \mapsto T_x$, is surjective**. Another claim of Chapter V states that **the left inner mapping group $\mathcal{L}_1$ coincides with the right inner mapping group $\mathcal{R}_1$ in every CC loop $Q$**. This property is rather rare in LCC loops, and when it takes place, then it has important consequences for the structure of a loop (see Section 4 of Chapter VI).

We conclude this section by stating a few of further results from Chapter V (cf. Corollary 3.9 and Proposition 4.4):

**Let $Q$ be a conjugacy closed loop. Then $Q/Z(N)$ is a group,**

$$[L_x, L_y^{-1}] = L_{x\backslash((yx)/y)} \quad \textbf{and} \quad [R_x, R_y^{-1}] = R_{(y\backslash(xy))/x},$$

**for all $x, y \in Q$. Furthermore, the elements $x\backslash((yx)/y)$ and $(y\backslash(xy))/x$ belong to the nucleus $N$.**

## 8. The case of linear fractional group

Results of Sections 4 and 7 show that if $Q$ is a finite loop such that $\operatorname{Mlt} Q$ is a Zassenhaus group, then $\operatorname{Mlt} Q$ has to be sharply triply transitive. Here we shall briefly discuss the method used to refute such a possibility. Let us first assume that $G = \operatorname{Mlt} Q$ is isomorphic to $PGL(2, q)$ (we shall be concerned here only with the natural representation of the latter group).

An important result of Vesanen states that $PSL(2, q)$ is never a multiplication group of a loop, for every representation of $PSL(2, q)$ (up to a finite number of special cases, which were left open in Vesanen's original papers [46] and [47], and which are said to have been refuted later by computer). The natural representation on $q+1$ elements is the one that seems to have required the greatest effort to refute. Chapters II, III and IV of the thesis point out several simplifications concerning Vesanen's work. The main one is based on observation that the natural representation of $PSL(2, q)$ on $q + 1$ points cannot be obtained as a multiplication group of a loop, by the general argument involving CC loops (see Sections 4 and 7). This follows from the fact that $PSL(2, q)$ is not triply transitive when $q$ is odd. Many pages of Vesanen's work can be omitted and replaced by this argument. However, that seems to help little to solve the case of $PGL(2, q)$. Still, to solve this case some ideas (while not many) from Vesanen's original approach turned out to be useful. The relationship to Vesanen's work is explained in detail in the introduction to Chapter II.

The proof that refutes $PGL(2, q)$ is quite long and technical. Nevertheless the starting idea is very simple. Suppose that we know the left translations $L_a$ and $L_b$, where $a \neq b$, and neither $a$ nor $b$ equals 1. Visualize the multiplication table of $Q$. Since the first row corresponds to the identity mapping, our knowledge of $L_a$ and $L_b$ means that we know three rows of the table. Since columns are assumed to come from

$PGL(2,q)$ as well, and since each permutation from $PGL(2,q)$ is determined by images of (any) three points, we see that the three rows determine all columns of the table. Because we can choose $a$ and $b$ in advance, we know the images of 1 by $L_a$ and $L_b$. These mappings are determined by three points as well, and so we see that the whole multiplication table is induced by four values. The idea of the proof is to treat them as unknowns and to formulate dependencies for each further row that express certain computed values of the multiplication tables. It turns out that these dependencies have a polynomial form, where the respective polynom is of degree at most 3. Since $q$ is in general much larger, the coefficients of the polynom have to vanish. This gives four identities (in Chapter II they appear as (1), (2), (3) and (4)), and after a number of quite technical computations one finally finds that these identities can be satisfied only when the rows and columns form the so called Singer cycle. The whole procedure works for infinite fields as well. The technique uses identification of $PGL(2,F)$ with the group of linear fractions $(ax+b)/(cx+d)$, where $ab-cd\neq 0$.

Note that the results state more than the fact that $PGL(2,F)$ cannot be realized as a multiplication group of a loop. By Theorems 6.1 and 6.2 of Chapter II we know that **if $Q$ is a loop such that** $\operatorname{Mlt} Q \leq PGL(2,F)$**, then $Q$ is an abelian group. If $F$ is finite of order $q\neq 3$, then $Q$ has to be cyclic.**

## 9. Semilinear fractions

The approach described in Section 8 does not fully express the content of Chapter II, as that chapter is concerned also with the case $\operatorname{Mlt} Q \leq M(q)$. The success of refutation of this possibility posed the natural question whether the case $\operatorname{Mlt} Q \leq P\Gamma L(2,q)$ can be excluded in its full generality (again, only the natural representation on $q+1$ points is considered).

It is proved in Chapter III that **if $Q$ is a loop with** $\operatorname{Mlt} Q \leq P\Gamma L(2,q)$ **and $q\neq 3,4$, then $Q$ has to be cyclic** (Theorem 5.1; the ensueing Theorem 5.2 gives a partial generalization for the case of an infinite $F$).

The cases $q\leq 3$ are of little interest since in such a case all loops of order $q+1$ are abelian. Assume $q\geq 4$. Group $G=P\Gamma L(2,q)$ contains $PGL(2,q)$ as a subgroup of index $r$, where $q=p^r$, $p$ a prime. For $q=4$ we get $|G|=5\,!$, which means $G\cong S_5$. Since $\operatorname{Mlt} Q\cong S_5$ for all nonassociative loops $Q$ of order 5, we see that the theorem cannot be extended to the case $q=4$. The next special case seems to be $q=8$, where the standard methods failed and the refutation was done by means of a computer. Cases $q=16$ and $q=64$ posed certain difficulty as well, but some sort of extension of standard methods turned out to be possible. The source of exceptional behaviout is the following statement which appears in Chapter III as Proposition 2.1:

**Let $q$ be a power of a prime, and let $F$ be a finite field of order $q^n$, $n \geq 2$. If $q = 2$, assume $n \notin \{2, 3, 4, 6\}$. Consider the number of elements of $F$ that are contained in a proper subfield which includes the subfield of order $q$. This number is less than $q^n/n - 1$.**

All proofs of Chapter III are rather technical, and we shall not explain them here. However, it seems to be worth to say more about the general approach. For a while denote $PGL(2, q)$ by $N$. With respect to the results of Section 8 we need to show the implication $\operatorname{Mlt} Q \leq G \Rightarrow \operatorname{Mlt} Q \leq N$. Denote by $U$ the set of all $a \in Q$ with $L_a \in N$ and by $V$ the set of all $b \in Q$ with $R_b \in N$. We wish to prove $U = Q$ and $V = Q$. The strategy used in Chapter III consists of three steps, and one can hope that these steps will prove to be useful in other similar situations when $|G : N|$ is relatively small when compared to $|Q|$. The strategy is as follows:

(1) From the size of $U$ deduce the existence of such an $S \subseteq U$ that the pointwise stabilizer $G_S$ is trivial, and the size of $S$ is the least possible.
(2) From the existence of $S \subseteq U$ with $G_S = 1$ and from the size of $V$ deduce that $V$ must be very large.
(3) Show that if $V \subseteq Q$ is very large, then $V$ has to equal $Q$.

In the application 'very large' means $|Q \setminus V| \leq 2$. The implication $|Q \setminus V| \leq 2 \Rightarrow Q = V$ is proved in a rather tricky way, and will not be commented here.

The condition $G_S = 1$ refers in no way to $N$, and so one can expect that some additional properties of $S$ will be used or required. For example one can assume the existence of an element $z \in S$ with $N_{S \setminus \{z\}} = 1$. This means that any $\varphi \in N$ is determined by its values $\varphi(a)$, $a \in S$, $a \neq z$.

Suppose now that $Q$ is a loop with $\operatorname{Mlt} Q \leq G$. For all $x \in Q$ construct the mapping $\varphi_x \in N$ (if it exists) by requiring $\varphi_x(a) = L_a(x) = R_x(a)$ for all $a \in S$, $a \neq z$, and denote $\varphi_x(z)$ by $f(x)$. Since $R_x \in G$ is determined by the values $R_x(a)$, $a \in S$, we see that $R_x$ belongs to $N$ (i.e., $x \in V$) if and only if $R_x(z) = f(x)$.

If $N = PGL(2, p^r)$, then $N$ is sharply triply transitive, $|S| = 4$, and $f$ is defined for all $x \in Q$. The equality $L_z(x) = f(x)$ leads to a polynomial identity of small degree, and $V$ is nearly always big enough to force this identity to be true everywhere. Since the connection between the polynomial identity and the equality $L_z(x) = f(x)$ allows the existence of (at most two) singular points, one obtains $|Q \setminus V| \leq 2$.

## 10. Orbits of inner mapping group

The penultimate paragraph of Section 3 proves that an element $a$ of a loop $Q$ belongs to its centre if and only if $R_{ax}^{-1} L_a R_x$ (or $L_{xa}^{-1} R_a L_x$) is

the identity mapping for all $x \in Q$. This simple fact is also a starting point for Chapter V. Theorem 1.2 of that chapter states that **if $\Gamma$ is such an orbit of** $\operatorname{Inn} Q$ **that** $\operatorname{Inn} Q$ **acts regularly on $\Gamma$, then $Q$ is an abelian loop.** Let us underscore that a regular action is assumed to be faithful. In a faithful action only the identity moves no element of the orbit. Orbits with a regular action should not be mixed with orbits upon which the image of the action is a regular permutation group.

The proof of the above mentioned theorem is easy: consider $a \in \Gamma$. Since all mappings $R_{ax}^{-1} L_a R_x$ fix $a$, the faithfulness implies that every such a mapping has to be the identity. Hence $a$ has to belong to the centre, and so $\Gamma = \{a\}$. The assumed faithfulness then implies the triviality of $\operatorname{Inn} Q$. Of course, $\operatorname{Inn} Q$ is trivial if and only if $Q$ is an abelian group.

There are few groups that cannot have a faithful action unless the action is regular on one of the orbits. Hence as an immediate corollary of the above theorem one sees that $\operatorname{Inn} Q$ **is never a cyclic $p$-group or a generalized group of quaternions**.

By blending together some group theory and the results on Zassenhaus groups (see Sections 3, 8 and 9), one can prove that **if $G$ is a finite permutation group such that $G_1$ acts faithfully on each of its orbits as a Frobenius group, then every loop $Q$ with** $\operatorname{Mlt} Q \leq G$ **has to be an abelian group**. This appears in Chapter V as Theorem 2.5.

This general theorem when associated with some elementary theorem of permutation groups (that is developed in Section 3 of Chapter V) can be applied to loops which have the inner mapping group of order $pq$, where $p$ and $q$ are two different primes. Theorem 4.5 of Chapter V states:

**Let $Q$ be a loop with $Z(Q) = 1$ such that $|\operatorname{Inn} Q| = pq$, $q < p$. Then $Q$ has a (unique) $p$-element normal subloop $S$ of order $p$, and $|Q/S| \leq q$. Both $S$ and $Q/S$ are abelian groups.**

From that one easily deduces that $\operatorname{Mlt} Q$ is a solvable group of order $p^2qk$, where $k = |G : S|$ (Theorem 4.6).

The structure of $Q$ does not change much when $Z(Q)$ is not trivial: in such a case $Q/Z(Q)$ is finite and $|\operatorname{Inn}(Q/Z(Q))| = pq$ as well. Hence $\operatorname{Mlt} Q$ **is solvable whenever** $\operatorname{Inn} Q$ **is of order $pq$.** This solves a question formulated by Niemenmaa, who gave earlier an answer to some partial cases (his methods are completely different and often rely on Classification of Finite Simple Groups), cf. Section 13.

The final section of Chapter V gives a new and shorter proof of an important theorem which was first proved by Kepka and Niemenmaa in [24] for the finite case, and later in [25] for the general case. The theorem states **if $Q$ is a loop which is not an abelian group, then** $\operatorname{Inn} Q$ **is not cyclic**.

## 11. Free loop terms

Chapter I contains more results than the fact that the multiplication group of a free loop is a Zassenhaus group. Some of them are not difficult, but some of them are highly technical.

Corollary 1.5 of Chapter I states that **if $Q$ is a free loop, then the groups $\mathcal{L}(Q)$, $\mathcal{R}(Q)$ and $\operatorname{Mlt} Q$ are free, and $\{L_a;\ a \in Q,\ a \neq 1\}$, $\{R_a;\ a \in Q,\ a \neq 1\}$ and $\{L_a, R_a;\ a \in Q,\ a \neq 1\}$ are free bases, respectively.** This is relatively easy. Theorem 5.1 which states that $\mathcal{L}(Q)$ **is a Frobenius group** is more difficult, and some nontrivial combinatorics on loop words is needed. The proof considers $\psi = \varphi_k \dots \varphi_1 \in \mathcal{L}(Q)$ that fixes two elements $a$ and $b$. Each of $\varphi_i$ is a left translation or an inverse of a left translation, and the result is obtained by considering the behaviour of $\varphi_i$ and $\varphi_{i-1}$ on $a_i = \varphi_i \dots \varphi_1(a)$ and $b_i = \varphi_i \dots \varphi_1(b)$, where $i$ is chosen so that $|a_i| + |b_i|$ is maximal. Here $|t|$ measures the size of a reduced loop term $t$.

To prove that $(\operatorname{Mlt} Q)_{a,b,c}$ consists only of identity, for any pairwise distinct $a, b, c \in Q$, one proceeds in a similar way. However, a number of complications arises, and a more abstract approach is needed to reduce the number of cases to be considered. One expresses $\psi$ as above, where each $\varphi_i$ can also be a right translation or its inverse. Denote by $e_i$ the element associated with $\varphi_i$, and consider the maximum of all $|e_i|$ in a situation when $\psi$ fixes $a$, $b$ and $c$ pointwise. It can be assumed that the maximum is attained for $i = 1$, since the situation allows for rotations. Then, roughly spoken, one proves that $\varphi_1$ causes shortening of each term $a$, $b$, $c$, and $\varphi_1^{-1}$ induces shortening of each of the terms $\varphi_1(a)$, $\varphi_1(b)$, $\varphi_1(c)$. Since operations $\cdot$, $/$ and $\backslash$ are binary, the number of shortenings is limited, and it turns out that the existence of three fixed points $a$, $b$ and $c$ would induce more ways than available how a term should be shortened.

The preceding description of the proof should be regarded as very approximative. The proof is full of gory details, and further explanatory efforts would require to descend to the level of exposition of the thesis. Only one further aspect will be mentioned here: It turned out that it is necessary to define $|t|$ as the number of occurences of a variable. Therefore a term produced by dividing 1 by a term $t$ does not change this value (e.g., $|t| = |1/t|$). When one needs a finer measure, one considers the size of the lifted term $\bar{t}$, in which all occurences of one are replaced by an extra dedicated variable. Of course, not all translations are compatible with such a lift, and then further considerations are needed. The proof would be thus simpler, if free quasigroups were considered.

The fact that $(\operatorname{Mlt} Q)_{a,b}$ contains no nonidentity $\psi$ that fixes some $c \notin \{a, b\}$ is proved in Section 8 of Chapter I. The remaining five sections of the Chapter serve to the purpose to characterize generators of

$(\operatorname{Mlt} Q)_{a,b}$. This is important, since in this way one gets for any loop $Q$ descriptions of permutations that are in $\operatorname{Mlt} Q$ and fix the points expressed by loop terms $a$ and $b$ (with respect to a fixed set of generators of $Q$). It turns out that $(\operatorname{Mlt} Q)_{a,b}$, $Q$ free, is generated by such combinations of translations that are basically the same as those that have been already considered. To be more precise, put

$$\mu_\varphi(x,y,z) = \varphi^{-1} R^{-1}_{\varphi(y)\backslash\varphi(z)} L_{\varphi(x)} L^{-1}_{\varphi(y)} R_{\varphi(x)\backslash\varphi(z)} \varphi \quad \text{and}$$
$$\nu_\varphi(x,y,z) = \varphi^{-1} L^{-1}_{\varphi(z)/\varphi(y)} R_{\varphi(x)} R^{-1}_{\varphi(y)} L_{\varphi(z)/\varphi(x)} \varphi,$$

for any $x, y, z \in Q$. Note that for $\varphi = \mathrm{id}_Q$ one gets

$$R^{-1}_{y\backslash z} L_x L^{-1}_y R_{x\backslash z} \quad \text{and} \quad L^{-1}_{z/y} R_x R^{-1}_y L_{z/x}.$$

Setting $y = 1$, $x = a$ and $z = ax$ (or $z = xa$) yields

$$R^{-1}_{ax} L_a R_x \quad \text{and} \quad L^{-1}_{xa} R_a L_x,$$

respectively, which are precisely the permutations that were repeatedly considered in Sections 3, 4 and 10.

Now, Theorem 14.4 of Chapter I states that **the double stabilizer $(\operatorname{Mlt} Q)_{a,b}$, $a \neq b$, $Q$ free, is generated by the set $\{\mu_\varphi(a,b,x)$, $\nu_\varphi(a,b,x)$; $\varphi \in \operatorname{Mlt} Q$ and $x \in Q\}$.** The proof is even more technical than that of the fact that each $\psi \in (\operatorname{Mlt} Q)_{a,b}$ fixes no element besides $a$ and $b$, unless $\psi = \mathrm{id}_Q$. One again expresses $\psi$ as $\varphi_k \dots \varphi_1$ and considers the behaviour of the respective translations when $|a_i| + |b_i|$ is maximal (the meaning of $\varphi_i$, $a_i$ and $b_i$ is the same as above).

## 12. Free groups of finite rank

Chapters VII and VIII contain constructions that give answers to natural questions induced by results of earlier chapters. Both constructions concern infinite loops and the corresponding results will be described only briefly since they do not seem to be important for further research. These chapters should be regarded as a sort of appendix to the previous text.

In Chapter VII there is proved that **for any integer $k \geq 1$ there exists a commutative loop $Q$ such that $\operatorname{Mlt} Q$ is a free group of rank $k$.** The construction is neither long, nor completely easy. Note that the multiplication group of a free loop is a free group of an infinite rank. Hence $Q$ constructed in Chapter VII has to be far from a free loop, and yet none of its term identifications can be extended to a series of term identifications that would make for an identification of two different group words in the free group generated by translations.

Chapter VIII contains a construction which is on one hand technically easier, and on the other hand more generic, allowing thus for modifications of parameters that imply additional properties. The construction describes the process of free completion of a set of partial permutations with respect to the requirement that these permutations

should be identified with (partial) loop translations. In this way one can show that **for any finite $k \geq 1$ there exists a loop $Q$ such that $\mathcal{L}(Q)$ is a free group of finite rank which is also a Frobenius group.** (Recall, that $\mathcal{L}(Q)$ is Frobenius and free when $Q$ is free, but that in such a case the rank is infinite.) By changing parameters one can prove that there is a large number of ways how such loops can be constructed. To be more precise, by Proposition 5.7 of Chapter VIII **there exist uncountably many non–isomorphic loops such that their left multiplication groups are simultaneously Frobenius groups and free groups of rank 2.**

## 13. Relationship to the work of other authors

Multiplication groups of loops started to be treated in a systematic way in the late seventies, with Smith, Kepka, Ihringer and Drápal being the principal investigators. J. D. H. Smith [42] published a paper in which he pointed out a connection to the representation theory. His further works are concerned more with quasigroups than loops, and in particular with central quasigroups [45], in connection with his well known treatise [43]. Smith has been always more interested in categorical than combinatorial aspects of multiplication groups, and for this reason he modified the standard definition of Mlt to get a functor from the category of loops (or quasigroups) to the category of groups [44]. When Mlt is defined in this way, then the connection to translations becomes far more complicated, and there is very little common ground with the theory described in the present thesis. In his work Smith was aided by his student J. D. Phillips [39]. However, a large part of Phillips' thesis is concerned with (standard) multiplication groups that admit triality [38]—an important topic that goes back to Glaubermann [15] and Doro [6] and which connects groups with Moufang loops. In his further works Phillips often cooperates with researchers from Prague, e.g. [32]. Smith's interest in connections with representation theory resulted in a large number of papers (many with K. W. Johnson) in which the original inspiration by multiplication groups is no more present (e.g., [21] [22]).

Drápal proved in his Diploma Thesis that the alternative group $A_n$ can be obtained as a multiplication group of a loop for every $n \geq 6$, but not for $n = 5$. These results were later published in two common papers [7] [8] with Kepka (who was Drápal's advisor). In the late seventies Kepka started to work with Markku Niemenmaa from Oulu, Finland. In their papers they decided to use the language of connected transversals instead of that of the left and right translations (cf. Section 1 of Chapter IV). There are two important results they have achieved: (1) if $\operatorname{Inn} Q$ is cyclic, then it is trivial [24] [25], and (2) if $\operatorname{Inn} Q$ is abelian, then $Q$ is nilpotent [26] [27]. Niemenmaa later concentrated

on the problem of proving the implication $|\operatorname{Inn} Q| = pq \Rightarrow Q$ is solvable. He published very many articles [35] [36] [37] [34] [4] [5] solving various partial cases, but did not succeed in solving the problem in its completeness. The solution appears in Chapter V of this thesis.

Results of Ari Vesanen have been mentioned in Section 8. Besides showing that $PSL(2, q)$ is never a multiplication group of a loop [46] [47], he proved an important fact that finite loops with soluble multiplication groups are soluble (as loops) [50]. His other results [48] [49] are deep as well.

The history of conjugacy closed loops is mentioned at the beginning of Section 7. Recently there has been an upsurge of interest in CC loops, which can be illustrated by works [31] [30] of Kunen et al. The main earlier source on left conjugacy closed loops is a paper by P. Nagy and Strambach [33]. However, the algebraic part of their paper does not go very far, and so the results of Chapter VI can be regarded as the real start for the theory of LCC loops. These results are also relevant for the theory of Bol loops, since a (left) Bol loop is an LCC loop if and only if $x^2 \in N_\lambda$ for every $x \in Q$. The main obstacle to classifying finite simple Bol loops seems to be the lack of understanding of the involutorial Bol loops (which satisfy $x^2 = 1$ for all $x \in Q$). There are quite a few authors working on Bol loops, and the connection with LCC loops is very promising (see, e.g., [28] [29]). However, it will not be presented here, since it goes beyond the results published in the thesis.

## 14. Reflexions on loop theory

Many people in the past seem to have been fascinated by nonassociative binary structures. In particular, at the time when the trend towards the abstract approach to algebraic structures was at its peak it looked very attractive to hope that one could develop a new mathematical world based on nonassociative operations. The origins of this hope go back to the discovery of quaternions and the ensueing Cayley numbers. The present perspective seems to be a bit different, since the number of classification results has shown that the abstract approach led to discovery of very few concrete structures that were not known before. Nevertheless, the state of theory of loops and quasigroups seems to be now much healthier than at any point in the last fifty years. There are more reasons for this fact, and one of them is a (hopefully widespread) realization of the interdisciplinary nature of the theory. Connections to combinatorics, geometry, group theory, mathematical physics, cryptography and logic are increasingly regarded as the main vehicle for the development of the theory.

The thesis is concerned mainly with connections to group theory. However, LCC loops have been considered also in the context of automatic theorem proving and there is a potential for applications in

cryptography (public keys based on the difficulty of the conjugation problem).

Regarding multiplication groups, the relationship to general group theory is quite peculiar. There is still very little understanding for the general character of permutation groups that can be realized by multiplication groups of loops. The experience seems to show that such permutation groups show little of strange behaviour that makes classification of groups a very difficult task (e.g., an easy observation shows that multiplication groups are never quasiprimitive [40]). This experience is emphasized by the fact that all important theorems on multiplication groups that were first proved by deeper results of finite group theory seem to have proofs using only elementary means.

The connection between loops and groups has been historically more important than the conventional mathematical knowledge seems to recognize. Zassenhaus used loops that appear in quasifields in his original approach to classification of sharply triple transitive groups [51]. Quasifields also are important for sharply two transitive groups and for the associated theory of nondesarguesian projective planes [18]. Fischer's finding of three sporadic simple groups that started in the early sixties a chain of such discoveries was based on investigations of left distributive quasigroups (a nice exposition can be found in [2]. The final sporadic group, the Monster, has several descriptions, the most elementary of which is based on the Parker loop [17] [1], a Moufang loop which is elementary abelian 2-group over a 2-element centre. The connection to groups with trialities was already mentioned above. Recently I have found that some group theorists (like Ch. Praeger) find the properties of multiplication groups of conjugacy closed loops quite appealing. Such groups possess two transitive proper normal subgroups, each of which has the stabilizer as its image. It seems quite difficult to construct such groups without using a loop.

There are other connections to groups, but that would take us too far from the topic of the thesis. The text is at its end.

## References

[1] M. Aschbacher, *Sporadic groups*, Cambridge University Press 1994.
[2] M. Aschbacher, *3-transposition groups*, Cambridge University Press 1997.
[3] A. S. Basarab, Klass LK-lup, *Matematicheskie issledovanija* **120** (1991), 3–7.
[4] P. Csörgö and M. Niemenmaa, Solvability conditions for loops and groups, *J. Algebra* **232** (2000), 336–342.
[5] P. Csörgö and M. Niemenmaa, On connected transversals to nonabelian subgroups, *European J. Combin.* **23** (2002), 179–185.
[6] S. Doro, Simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* **83** (1978), 377–392
[7] A. Drápal and T. Kepka, Alternating groups and Latin squares, *Europ. J. Combinatorics* **10** (1989), 175–180.
[8] A. Drápal and T. Kepka, Loops whose translations generate the alternating group, *Czech. Math. J.* **40** (1990), 128–136.

[9] A. Drápal, Conjugacy closed loops and their multiplication groups, *J. Algebra*, **272** 2004, 838–850.
[10] A. Drápal, On multiplication groups of left conjugacy closed loops, *Comment. Math. Univ. Carolinae* **45** (2004), 223–236.
[11] A. Drápal, Multiplication groups of finite loops that fix at most two points, *J. Algebra*, **235** (2001), 154–175.
[12] A. Drápal, Multiplication groups of loops and projective semilinear transformations in dimension two, *J. Algebra*, **251** (2002), 256–278.
[13] A. Drápal, Orbits of inner mapping groups, *Monatsh. Math.*, **134** (2002), 191–206.
[14] T. Evans, On multiplicative systems defined by generators and relations. I. Normal form theorem, *Proc. Cambridge Philos. Soc.* **47** (1951), 637–649.
[15] G. Glaubermann, On loops of odd order II, *J. Algebra* **8** (1968), 393–414.
[16] E. G. Goodaire and D. A. Robinson, A class of loops which are isomorphic to all loop isotopes, *Canad. J. Math.* **34** (1982), 662–672.
[17] R. L. Griess, Jr., Code loops, *J. Algebra* **100** (1986), 224–234.
[18] M. Hall, *The theory of groups*, The Macmillan Company, New York 1959.
[19] Th. Ihringer, On multiplication groups of quasigroups, *European J. Combin.* **5** (1984), 137–141.
[20] Th. Ihringer, Quasigroups, loops and centraliser rings, *Contributions to general algebra* **3** (Vienna, 1984), 211–224.
[21] K. W. Johnson and J. D. H. Smith, Characters of finite quasigroups, *European J. Combin.* **5** (1984), 43–50.
[22] K. W. Johnson, J. D. H. Smith and S. Y. Song, Characters of finite quasigroups, VI. Critical examples and doubletons. *European J. Combin.* **11** (1990), 267–275.
[23] T. Kepka and M. Niemenmaa, On conjugacy classes in finite loops, *Bull. Austral. Math. Soc.* **38** (1988), 171–176.
[24] T. Kepka and M. Niemenmaa, On multiplication groups of loops, *J. Algebra,* **135**(1990), 112–122.
[25] T. Kepka and M. Niemenmaa,On loops with cyclic inner mapping groups *Arch. Mat. (Basel)*, **60** (1993), 233–236.
[26] T. Kepka and M. Niemenmaa, On connected transversals to abelian subgroups, *Bull. Austral. Math. Soc.* **49** (1994), 121–128.
[27] T. Kepka, On the abelian inner permutation groups of loops, *Comm. Alg.* **26** (1998), 857–861.
[28] G. P. Nagy, Group invariants of certain Burn loop classes, *Bull. Belg. Math. Soc.* **5** (1998), 403–415.
[29] H. Kiechle and G. P. Nagy, On the extension of involutorial Bol loops, *Abh. Math. Sem. Univ. Hamburg*, **72** (2002), 235–250.
[30] M. K. Kinyon, K. Kunen and J. D. Phillips, Diassociativity in Conjugacy Closed Loops, *Communications in Algebra*, **32** (2004), 767–786.
[31] K. Kunen, The structure of conjugacy closed loops, *Trans. Amer. Math. Soc.*, **352** (2000), 2889–2911.
[32] T. Kepka and J. D. Phillips, Connected transversals to subnormal subgroups, *Comment. Math. Univ. Carolin.* **38** (1997), 223–230.
[33] P. Nagy and K. Strambach, Loops as invariant sections in groups, and their geometry, *Canad. J. Math.*, **46** (1994), 1027–1056.
[34] K. Myllylä and M. Niemenmaa, On the solvability of commutative loops and their multiplication groups, *Comment. Math. Univ. Carolinae* **40** (1999), 209–214.

[35] M. Niemenmaa, On loops which have dihedral 2-groups as inner mapping groups, *Bull. Austral. Mat. Soc.* **52** (1995), 153–160.
[36] M. Niemenmaa, On connected transversals to subgroups whose order is a product of two primes, *European J. Comb.* **18** (1997), 915–919.
[37] M. Niemenmaa, On the solvability of loops and their multiplication groups, in: *Groups—Korea '98* (Pusan), 291–296, de Gruyter, Berlin, 2000.
[38] J. D. Phillips, Moufang loop multiplication groups with triality, *Rocky Mountain J. Math.* **29** (1999), 1483–1490.
[39] J. D. Phillips and J. D. H. Smith, The endocenter and its applications to quasigroup representation theory, *Commentat. Math. Univ. Carol.* **41** (2000), 251–259.
[40] J. D. Phillips and J. D. H. Smith, Quasiprimitivity and quasigroups., *Bull. Austral. Math. Soc.* **59** (1999), 473–475.
[41] L. R. Soikis, O specialnych lupach, in *Voprosy teorii kvazigrupp i lup* (V. D. Belousov, ed.), Akademia Nauk Moldav. SSR, Kishinev, 1970, pp. 122–131.
[42] J. D. H. Smith, Centraliser rings of multiplication groups on quasigroups, *Math. Proc. Camb. Philos. Soc.* **79** (1976), 427–431.
[43] J. D. H. Smith, *Mal'cev varieties*, Springer, 1976.
[44] J. D. H. Smith, *Representation theory of infinite groups and finite quasigroups*, Les Presses de l'Université de Montréal, Montréal, 1986.
[45] J. D. H. Smith, Centrality, in *Quasigroups and loops: theory and applications*, Sigma Ser. Pure Math. 8, 95-114, Heldermann Verlag, 1990.
[46] A. Vesanen, On connected transversals in $PSL(2,q)$, *Ann. Acad. Sci. Fenn., Ser. A, I. Mathematica, Dissertationes,* **84** (1992).
[47] A. Vesanen, The group $PSL(2,q)$ is not the multiplication group of a loop, *Comm. Algebra,* **22** (1994), 1177–1195.
[48] A. Vesanen, On $p$-groups as loop groups, *Arch.-Math. (Basel)*, **61** (1993), 1–6.
[49] A. Vesanen, Finite classical groups and multiplication groups of loops, *Math. Proc. Cambridge Philos.Soc.* **117** (1995), 425–429.
[50] A. Vesanen, Solvable groups and loops, *J. Algebra* **180** (1996), 862–876.
[51] H. Zassenhaus, Kennzeichnung endlichen linearen Gruppen als Permutationsgruppen *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 17–44.