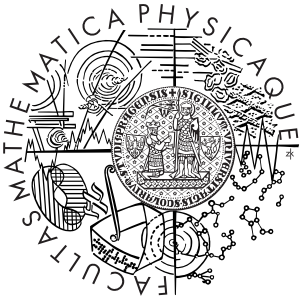
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Jan Vlachý

Malé levodistributivní kvazigrupy

Katedra algebry

Vedoucí bakalářské práce: RNDr. David Stanovský, Ph.D.
Studijní program: Matematika, Obecná matematika

2010

Chtěl bych poděkovat svému vedoucímu, Davidu Stanovskému, za mnoho podnětných připomínek a za jeho podporu během tvorby této práce.

Dále mé díky patří otci a babičce za připomínky k formální stránce tohoto textu; též ovšem za veškerou podporu, kterou mi poskytovali během dosavadního studia.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne Jan Vlachý

Contents

Název práce: Malé levodistributivní kvazigrupy
Autor: Jan Vlachý
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: RNDr. David Stanovský, Ph.D.
e-mail vedoucího: stanovsk@karlin.mff.cuni.cz

Předložená práce se zabývá konečnými levodistributivními (LD) kvazigrupami. V kapitole 1 předkládáme podrobně rozpracovaný obsah dvou článků V. M. Galkina. V kapitole 2 pomocí Galkinovy teorie klasifikujeme všechny LD kvazigrupy až do řádu 15. V obecném (nemediálním) případě se nejprve věnujeme jednoduchým LD kvazigrupám. Poté popíšeme obecný postup, kterým se pomocí normální podkvazigrupy dají získat informace o struktuře dané LD kvazigrupě. Tento postup rozpracujeme podrobněji pro kvazigrupy splňující jisté další podmínky. Ukážeme, že tyto podmínky musí platit pro libovolnou LD kvazigrupu na 9, 12 nebo 15 prvcích, z čehož vyvodíme hlavní výsledky práce. Dále v kapitole 3 explicitně sestrojíme jediné dvě nemediální LD kvazigrupy na 15 prvcích.

Klíčová slova: kvazigrupa, levá distributivita, levá multiplikativní grupa

Title: Small left distributive quasigroups
Author: Jan Vlachý
Department: Department of Algebra
Supervisor: RNDr. David Stanovský, Ph.D.
Supervisor's e-mail address: stanovsk@karlin.mff.cuni.cz

In this work we study finite left distributive (LD) quasigroups. In Chapter 1, we compile and thoroughly analyze two papers by V. M. Galkin. In Chapter 2, we apply Galkin's theory to classify all the LD quasigroups of orders up to 15. In the general (non-medial) case, we first consider simple quasigroups. Afterwards, we sketch a general procedure how to use a normal subquasigroup to investigate the quasigroup structure. This procedure is elaborated under additional conditions on the LD quasigroup, which are shown to hold for LD quasigroups on 9, 12 and 15 elements. This leads to the main conclusions. Furthermore, in Chapter 3, the only two non-medial LD quasigroups of order 15 are explicitly constructed.

Keywords: quasigroup, left distributivity, left multiplication group

Introduction

Quasigroups are non-associative generalizations of groups. Finite quasigroups correspond to Latin squares and thus have an inherently combinatorial character. Therefore, when studying quasigroups, additional conditions are imposed. In this thesis, we study finite left distributive quasigroups (for precise definitions, see 1.1).

Many quasigroup properties are determined by its multiplication group (i.e. the group generated by all the left and right translations). In general, this group may be very wild. In the case of left distributive quasigroups, though, the subgroup of the multiplication group generated by just the left translations is rather tame, since it is contained in the automorphism group of the quasigroup.

This thesis has two principal goals. The first one is to compile the results of two articles ([7], [6]) by Galkin and to provide comments and clarify the proofs therein. The second goal is to classify all left distributive quasigroups up to order 15. This is accomplished by application of Galkin's results.

The original motivation for this work was the discovery of the smallest (of order 15) non-medial left distributive quasigroup [13, Chapter IV]. This was done by brute force searching (using a model builder) for all quasigroups satisfying left distributivity, but not mediality. It then seemed natural to look for a more theoretical argument that would explain the nonexistence of any smaller quasigroups of this kind.

Certain arguments in this thesis still rely on computer verification, yet only in a minor way. Nothing more but a few computations in small groups is needed.

Chapter 1 consists of Galkin's results (with the exceptions of some basic notions in 1.1; other exceptions are explicitly indicated). The author of this thesis provided a few clarifying remarks (apart from Galkin's own - rather scarce - remarks) and also expanded the proofs - in the original articles, some proofs were mere sketches.

Chapter 2 begins by enumeration (up to isomorphism) of the medial quasigroups up to order 15. In the larger part of the chapter, the author then considers the non-medial left distributive (non-M LD) quasigroups. First, a few observations are made ruling out the existence of non-M LD quasigroups of orders 2, 3, 4, 5, 6, 7, 8, 10, 11, 13 and 14. Then, under additional assumptions (which are satisfied for small quasigroups), restrictive conditions concerning the left multiplication groups of non-M LD quasigroups are derived. These conditions are then applied to rule out the existence of non-M LD quasigroups of orders 9 and 12 (and to determine the properties of such quasigroups on 15 elements).

In chapter 3, we provide explicit constructions for the two existing non-M LD quasigroups on 15 elements.

Chapters 2 and 3 consist of the author's original work, any exceptions being indicated.

Appendix A is provided for the reader's convenience, mentioning some results in the group and quasigroup theory needed to follow the text.

Appendix B lists left multiplication groups for several small LD quasigroups.

Chapter 1

Galkin's theorems

1.1 Basic notions

Definition 1.1.1 *A* quasigroup *$(Q, \cdot, /, \backslash)$ is a set Q with three binary functions ("multiplication", "right division", "left division"), satisfying:*

$$\begin{aligned} y\backslash(y \cdot x) &= x \\ (x \cdot y)/y &= x \\ y \cdot (y\backslash x) &= x \\ (x/y) \cdot y &= x \end{aligned} \tag{1.1}$$

From this, the usual notions of universal algebra follows - such as homomorphism (and its kernel), subquasigroup, congruence, quotient quasigroup and so on (cf. [3]).

Given a quasigroup as above, we may equivalently view it as a groupoid $(Q, \cdot)$, with multiplication defined as in $(Q, \cdot, /, \backslash)$, but instead of division functions and axioms (1.1), we require that for every $a,\ b \in Q$, the equations

$$\begin{aligned} a \cdot x &= b \\ y \cdot a &= b \end{aligned} \tag{1.2}$$

have unique solutions $x_{(a,b)}, y_{(a,b)}$ in Q or, equivalently, that for every $a \in Q$, the left and right translations $\lambda_a : x \mapsto a \cdot x$, $\rho_a : x \mapsto x \cdot a$ are bijections of Q (their surjectivity is referred to as left, respectively right, divisibility; the injectivity is referred to as left, respectively right, cancellation).

Indeed, if $(Q, \cdot, /, \backslash)$ with (1.1) is given, $x = a\backslash b$ and $y = b/a$ are the unique solutions of (1.2). On the other hand, given $(Q, \cdot)$ with (1.2), we

may define $a\backslash b,\ a/b$ (for any $(a,b) \in Q \times Q$) as the respective unique solutions $x_{(a,b)}, y_{(a,b)}$ in (1.2) and $(Q, \cdot, /, \backslash)$ then satisfies (1.1).

Now, given $(Q, \cdot)$, congruences and subquasigroups need not correspond to those in $(Q, \cdot, /, \backslash)$. They do, though, in the finite case, as $/, \backslash$ are definable using just iterated multiplication: $b/a = \rho_a^{-1}(b) = \rho_a^{n_{a,b}}(b),\ a\backslash b = \lambda_a^{-1}(b) = \lambda_a^{m_{a,b}}(b)$ for some $n_{a,b},\ m_{a,b} \in \mathbb{N}$.

For more on this topic, see [12, Chapter 1.2].

Definition 1.1.2 *We say that a quasigroup $(Q, \cdot)$ is*

- left distributive *(LD), if* $z(xy) = (zx)(zy)$,
- right distributive *(RD), if* $(xy)z = (xz)(yz)$,
- distributive, *if it is both left and right distributive,*
- idempotent, *if* $xx = x$,
- medial, *if* $(xy)(zw) = (xz)(yw)$,

for all $x, y, z, w \in Q$.

Since the above properties are given by equalities, the homomorphic images and substructures of Q will again exhibit those properties, if Q does.

Choosing $y = x$ (respectively $y = w$) in the equation of mediality, we see that a medial idempotent quasigroup is distributive.

Proposition 1.1.3 (Basic properties) *Let Q be a LD quasigroup. Then:*

1. *$x \cdot x = x$ for all $x \in Q$ (idempotency)*
2. *λ_a is an automorphism of Q for all $a \in Q$*

Proof.

1. From (LD) we have $x(xx) = (xx)(xx)$. From right cancellation we have $x = (xx)$.
2. λ_a is a bijection, since Q is a quasigroup. The fact that λ_a is an endomorphism of Q is just a rephrasing of the LD property.

□

Remark. In the text, we will always assume that the quasigroups mentioned are finite (unless indicated otherwise) - under this assumption, we need not distinguish substructures and congruences of $(Q, \cdot)$ from those of $(Q, \cdot, /, \backslash)$. In particular in the finite case, the substructures are exactly those subsets closed to multiplication and a mapping between two quasigroup is a homomorphism, exactly when it respects the multiplication.

Suppose there is a nontrivial congruence $\sim$ of a LD quasigroup Q, let Q_0 be its block. Then Q_0 is a subquasigroup, because of idempotency (if $x, y \in Q_0$, then $[xy]_\sim = [x]_\sim[y]_\sim = [x]_\sim[x]_\sim = [x]_\sim$, that is $x \cdot y \sim x$ and $x \cdot y \in Q_0$). All the blocks are subquasigroups isomorphic to Q_0, because those are images of Q_0 under appropriate left translations (for B a block of the congruence with $b \in B$, we choose any $a \in Q_0$ and we get $x \in Q$ with $xa = b$ from left divisibility. Then $\lambda_x(Q_0)$ is a subquasigroup isomorphic to Q_0, containing b. Moreover $xa' \sim b = xa$, $\forall a' \in Q_0$, because $\sim$ is a congruence. That is, $\lambda_x(Q_0) = B$ if Q was finite. See also Proposition 2.3.2.).

Definition 1.1.4 *We say that $Q_0 \leq Q$ is a* normal subquasigroup *of Q, if it is a block of some congruence on Q.*

Proposition 1.1.5 *Let Q be a LD quasigroup with Q_1 being its proper subquasigroup. Then $|Q_1| \leq |Q|/3$. If the equality holds, then Q_1 is normal.*

Proof. Pick $a \notin Q_1$, $b \in Q_1$ and put $Q_2 := \lambda_a(Q_1)$, $Q_3 := \lambda_b \circ \lambda_a(Q_1)$. The three subquasigroups are then isomorphic (and so $|Q_1| = |Q_2| = |Q_3|$).

We want to show, that all Q_i $(i = 1, 2, 3)$ are mutually disjoint. $Q_1 \cap Q_2 = \emptyset$: If not, pick $q_1 \in Q_1 \cap Q_2$, then $q_1 = (q_1/q)\ q = aq$ for some $q \in Q_1$ and $q_1/q \in Q_1$, because Q_1 is a subquasigroup. This contradicts the injectivity of ρ_q. Now, because $b \notin Q_2$, we have $Q_2 \cap Q_3 = \emptyset$ (arguing the same as for $Q_1 \cap Q_2$). Also $Q_1 \cap Q_3 = \emptyset$: for if $b(aq) = q'$ with $q, q' \in Q_1$, then $a = (b\backslash q')/q \in Q_1$, contradicting the selection of a.

Thus $3|Q_1| = |Q_1| + |Q_2| + |Q_3| = |Q_1 \cup Q_2 \cup Q_3| \leq |Q|$ and the first claim holds.

If $x_i \in Q_i, x_j \in Q_j$ (with $i \neq j$), then $x_i \cdot x_j \notin Q_i \cup Q_j$ (else we would come to contradiction with cancellation - for instance, if $x_i \cdot x_j = y_j \in Q_j$, then also $y_j = (y_j/x_j) \cdot x_j$ and $Q_i \ni x_i \neq (y_j/x_j) \in Q_j$, contradicting the injectivity of ρ_{x_j}). If $Q = Q_1 \cup Q_2 \cup Q_3$, then the product must lie in the remaining subquasigroup, so the three subquasigroups induce a congruence on Q (the induced multiplication $\tilde{\cdot}$ on $\{Q_1, Q_2, Q_3\}$ is then defined as in Table 1.1). $\square$

$\cdot$	Q_1	Q_2	Q_3
Q_1	Q_1	Q_3	Q_2
Q_2	Q_3	Q_2	Q_1
Q_3	Q_2	Q_1	Q_3

Table 1.1: Cayley table of the 3-element LD quasigroup

1.2 About the left multiplication group

Let $(Q, \cdot)$ be a LD quasigroup. Denote by $\mathbf{L}(Q) = \mathrm{LMlt}(Q)$ the subgroup of $\mathrm{Aut}(Q)$ generated by all left translations $\lambda_a : x \mapsto a \cdot x$ (for any $a, x \in Q$); we will write just $\mathbf{L}$, when Q is clear from the context. For any group G acting on Q, we denote the stabilizer of $a \in Q$ as G_a.

For $\alpha \in \mathrm{Aut}(Q)$ we have $\alpha(a \cdot x) = \alpha(a) \cdot \alpha(x)$, so

$$\begin{aligned} \alpha\lambda_a &= \lambda_{\alpha(a)}\alpha \quad \text{and} \\ \lambda_{\alpha(a)} &= \alpha\lambda_a\alpha^{-1}. \end{aligned} \tag{1.3}$$

In particular $\lambda_{a \cdot b} = \lambda_a\lambda_b\lambda_a^{-1}$.

Consider a group G with $\mathbf{L} \leq G \leq \mathrm{Aut}(Q)$. The following holds:

Theorem 1.2.1 (Properties of automorphism groups of a LD quasigroup)

1. *$\{\lambda_a;\ a \in Q\}$ form a conjugacy class in G.*
2. *The center of G is trivial.*
3. *G is transitive on Q.*

   The subgroups $\{G_a;\ a \in Q\}$ are conjugated in G.

   $G_a = N_G(G_a)$.
4. *Every left coset of G_a in G contains exactly one left translation; $[G : G_a] = |Q|$*

Proof.

1. $\lambda_{\alpha(a)} = \alpha\lambda_a\alpha^{-1}$, so $\{\lambda_a\}_{a \in Q}$ is conjugation-invariant. The conjugation action of G is transitive on $\{\lambda_a\}_{a \in Q}$: given $x, y \in Q$, choose a with $y = a \cdot x$, then $\lambda_y = \lambda_a\lambda_x\lambda_a^{-1}$.

2. Since $\mathbf{L} \leq G$, the mappings from the center $Z(G)$ commute with all the left translations, so - from (1.3) - they fix all Q. Thus $Z(G) = \{id\}$.

3. Given $q_0, q_1 \in Q$, choose $\lambda_{q_1/q_0} \in \mathbf{L} \leq G$, then $\lambda_{q_1/q_0}(q_0) = q_1$, so G acts transitively on Q.

   Because $\alpha G_a \alpha^{-1} = G_{\alpha(a)}$, the transitivity gives the second statement.

   For $\alpha \in N_G(G_a)$ we have $G_{\alpha(a)} = \alpha G_a \alpha^{-1} = G_a$, so $\lambda_{\alpha(a)}$ centralizes λ_a. Then $\lambda_{\alpha(a)} = \lambda_a \lambda_{\alpha(a)} \lambda_a^{-1} = \lambda_{a \cdot \alpha(a)}$, thus $\alpha(a) = a \cdot \alpha(a)$ and $\alpha(a) = a$ (as $\alpha(a) \cdot \alpha(a) = \alpha(a)$ and we have cancellation). This means $\alpha \in G_a$.

4. $[G : G_a] = [G : N_G(G_a)] = |\{G_b;\ b \in Q\}| = |Q|$ (the second equality is because of transitivity; the third because $G_a \neq G_b$, when $a \neq b$, as λ_a lies in the former, but not in the latter). If $b \neq c$, then $\lambda_b^{-1}\lambda_c$ has no fixed points (if $\lambda_b^{-1}\lambda_c(a) = a$, then $c \cdot a = b \cdot a$ and $c = b$ from right cancellation), so λ_b and λ_c lie in different cosets by G_a. The number of cosets is the same as the number of the translations, so every coset contains exactly one translation.

□

Remark.

- From the theorem, $\mathbf{L}$ is invariant to conjugations within $\mathrm{Aut}(Q)$; that means $\mathbf{L}(Q) \trianglelefteq \mathrm{Aut}(Q)$.

- $\mathbf{L}'$ is generated by $\{\lambda_a \lambda_b^{-1}; a, b \in Q\}$

  $$(\text{because } \lambda_x^{-1}\lambda_y^{-1}\lambda_x\lambda_y = \lambda_x^{-1}\lambda_{y\backslash x} = \lambda_{x\backslash(y\backslash x)}\lambda_x^{-1}\ )$$

  and so $\mathbf{L}\,/\,\mathbf{L}'$ is cyclic, generated by $\lambda_a\,\mathbf{L}'$.

- $\mathbf{L}'$ is also transitive on Q - for given $a, b \in Q$, we have $\lambda_a\lambda_b^{-1}(b) = a$.

- This theorem holds - with the same proof - even for Q infinite (except for the last point).

1.3 Galkin's representation

Suppose G is a finite group with an automorphism ϕ, T being the subgroup of elements fixed by ϕ.
Let G/T denote the family of left cosets of T in G. The coset containing $x \in G$ will be denoted xT.
Define a binary operation on G/T by

$$xT \circ yT = x\phi(x^{-1}y)T \tag{1.4}$$

Proposition 1.3.1

1. *The definition* (1.4) *is correct.*
2. $(G/T, \circ)$ *is a LD groupoid with left divisibility.*
3. $(G/T, \circ)$ *is a quasigroup if and only if*

$$x\phi(x^{-1}) \in sTs^{-1} \Rightarrow x \in T, \text{ for every } x, s \in G \tag{1.5}$$

Proof.

1. If $x' = xs,\ y' = yt$ for some $x, x', y, y' \in G,\ s, t \in T$, then we have

$$\begin{aligned}&\phi(t) = t, \phi(s) = s, \text{ so}\\ &x'T \circ y'T = x'\phi(x'^{-1}y')T = xs\phi(s^{-1})\phi(x^{-1}y)\phi(t)t^{-1}T =\\ &= x\phi(s)\phi(s^{-1})\phi(x^{-1}y)tt^{-1}T = x\phi(x^{-1}y)T = xT \circ yT.\end{aligned}$$

2. Left distributivity: on one hand:

$$xT \circ (yT \circ zT) = xT \circ y\phi(y^{-1}z)T = x\phi(x^{-1}y)\phi^2(y^{-1}z)T$$

   On the other hand:

$$\begin{aligned}&(xT \circ yT) \circ (xT \circ zT) = x\phi(x^{-1}y)T \circ x\phi(x^{-1}z)T =\\ &= x\phi(x^{-1}y)\phi(\phi(y^{-1}x)x^{-1}x\phi(x^{-1}z))T = x\phi(x^{-1}y)\phi^2(y^{-1}z)T\end{aligned}$$

   Left divisibility: Given a and b in the equation $aT \circ xT = bT$. Taking xT with $x = a\phi^{-1}(a^{-1}b)$ solves it (since $aT \circ xT = a\phi(a^{-1}x)T$).

3. Assume (1.5). Since G/T is finite, the left divisibility gives also the left cancellation and $(G/T, \circ)$ is already a left quasigroup.

   For the bijectiveness of right translations, it is enough (again from finiteness) to check right cancellation. Given the equation

   $$x_1T \circ aT = x_2T \circ aT \tag{1.6}$$

   in G/T, put $x := x_1^{-1}x_2$ and choose $s \in G$, such that $a = x_1\phi^{-1}(s)$. Using this, rewrite the equation (1.6):

   $$\begin{aligned} x_1T \circ aT &= x_2T \circ aT \\ x_1\phi(x_1^{-1}a)T &= x_2\phi(x_2^{-1}a)T \\ x_1sT &= x_2\phi(x_2^{-1}x_1)sT \\ sT &= x\phi(x^{-1})sT. \end{aligned}$$

   Therefore we have $x\phi(x^{-1}) \in sTs^{-1}$ and (1.5) gives $x = x_1^{-1}x_2 \in T$ and $x_1T = x_2T$.

   Now assume that $(G/T, \circ)$ is a quasigroup, $x, s \in G$, and $t \in T$. Let $x\phi(x^{-1}) = sts^{-1}$ as in (1.5). Rewrite it as $x\phi(x^{-1}\phi^{-1}(s)) = \phi(\phi^{-1}(s))t$, this means $xT \circ \phi^{-1}(s)T = 1T \circ \phi^{-1}(s)T$ in $(G/T, \circ)$. Cancelling $\phi^{-1}(s)T$, we get $xT = 1T$ and so $x \in T$.

□

Example. Take $G := (\mathbb{Z}, +)$ and

$$\begin{aligned} &\phi \in \mathrm{Aut}(\mathbb{Z}, +) \\ &\phi : x \mapsto -x. \end{aligned}$$

Then $T = \{0\}$ and ϕ satisfies (1.5) - if $x\phi(-x) = 2x = 0$, then already $x = 0$.

By the above process, we obtain a groupoid $(\mathbb{Z}, \circ)$ with $x \circ y = 2x - y$. This is a LD left quasigroup, however it is not a quasigroup, since right translations are not surjective.

This example shows that the finiteness condition for G is not redundant.

Once we restrict ourselves to finite structures, every LD quasigroup can be represented in the above form. Let Q be a LD quasigroup, $\mathbf{L} := \mathrm{LMlt}(Q)$. Fix $e \in Q$ and define the automorphism ϕ on $\mathbf{L}$ by $\phi(\alpha) = \lambda_e\alpha\lambda_e^{-1}$, its fixed points (that is, the centralizer of λ_e in $\mathbf{L}$) are exactly $\mathbf{L}_e = \{u \in \mathbf{L} \mid u(e) = e\}$ (recall Equation (1.3)). Now, $(\mathbf{L} \,/\, \mathbf{L}_e, \circ)$ is a LD quasigroup as in 1.3.1.

Theorem 1.3.2 (Galkin's representation)
There is the isomorphism of quasigroups: $(Q,\cdot) \simeq (\mathbf{L}\,/\,\mathbf{L}_e, \circ)$

Proof. Consider the mapping

$$\begin{aligned} \psi : (Q,\cdot) &\to (\mathbf{L}\,/\,\mathbf{L}_e, \circ) \\ q &\mapsto \lambda_{q/e}\,\mathbf{L}_e\,. \end{aligned}$$

This is a bijective mapping (there are $|Q|$ cosets according to 1.2.1 and the right division by e is bijective).

For finite quasigroups it is enough to verify, that ψ respects the multiplication: Let

$$\lambda_{q_1/e}\,\mathbf{L}_e \circ \lambda_{q_2/e}\,\mathbf{L}_e = \lambda_{q/e}\,\mathbf{L}_e, \text{ for some } q \in Q. \tag{1.7}$$

We want to show $q_1 \cdot q_2 = q$. We have (from the definition of $\circ$ and from (1.3)):

$$\lambda_{q_1/e}\,\mathbf{L}_e \ \circ \lambda_{q_2/e}\,\mathbf{L}_e = \lambda_{q_1/e}\ \lambda_e \lambda^{-1}_{q_1/e}\ \lambda_{q_2/e}\ \lambda_e^{-1}\,\mathbf{L}_e = \lambda_{q_1}\ \lambda_{q_2/e}\ \lambda_e^{-1}\,\mathbf{L}_e\ . \tag{1.8}$$

Evaluating arbitrary representatives of cosets in (1.7) and (1.8) in the point e and equating them gives:

$$q/e \cdot e = \lambda_{q_1}\ \lambda_{q_2/e}(e)\ ,$$

which is just a complicated way to write $q_1 \cdot q_2 = q$. □

The presentation in form $(G/T, \circ)$ is not unique and it is convenient to look for the presentation with G as small as possible.

Assume now, that $H \leq G$ is a ϕ-subgroup (i.e. $\phi(H) = H$). If not indicated otherwise, we will assume the quasigroup structure on $H/H \cap T$ with the automorphism $\phi\restriction_H$.

On the other hand, observe that the cosets HT/T form a subquasigroup of G/T. We have the following:

Proposition 1.3.3 ("Diamond isomorphism theorem")
The following isomorphism of quasigroups holds:

$$HT/T \simeq H/H \cap T.$$

Proof. Take the representatives of left cosets HT/T in the form $hT, h \in H$ and consider the mapping

$$\psi : hT \mapsto h(H \cap T).$$

Its bijectiveness is easily verified.

As for respecting multiplication, we have (for $h, h' \in H$):

$$\psi(hT) \diamond \psi(h'T) = h(H \cap T) \diamond h'(H \cap T) =$$
$$= h\phi(h^{-1}h')(H \cap T) = \psi(h\phi(h^{-1}h')T) = \psi(hT \circ h'T),$$

where $\circ$, respectively $\diamond$, denotes the binary operation on HT/T, respectively $H/H \cap T$. □

In case of $\phi(N) = N$ with N a normal subgroup in G, we may consider the quotient group $\tilde{G} := G/N$ with the automorphism $\tilde{\phi}$ induced by ϕ (i.e. $\tilde{\phi}(gN) := \phi(g)N$ for $gN \in G/N$).

We may introduce the quasigroup structure on $\tilde{G}$ using $\tilde{\phi}$ in the same way as was shown in the beginning of Section 1.3. We claim that the distinguished subgroup of fixed elements of $\tilde{\phi}$ in $\tilde{G}$ (denote the set by $\tilde{T}$) is exactly the subgroup TN/N.

If $xN \in TN/N$, choose $x' \in xN$ with $x' \in T$. Then $\tilde{\phi}(xN) = \tilde{\phi}(x'N) = \phi(x')N = x'N = xN$, so $TN/N \subset \tilde{T}$

On the other hand, if $xN \in \tilde{T}$, then $xN = \phi(x)N$, so $x\phi(x^{-1}) \in N$. Thus $xT \circ 1T = x\phi(x^{-1})T \in NT/T$. Because NT/T is a subquasigroup of G/T containing $1T$, the result of cancelling $1T$ from $xT \circ 1T$ lies again in NT/T, i.e. $xT \in NT$ and $x \in NT$. But this means $xN \in (NT)/N = (TN)/N$, so $\tilde{T} \subset (TN)/N$, which we wanted to show.

Lemma 1.3.4

The map

$$\pi : G/T \to \tilde{G}/\tilde{T}$$
$$xT \mapsto xNT,$$

induced by the canonical projection of G on $\tilde{G}$, is a quasigroup epimorphism.

Furthermore if $N \leq T$, then π is an isomorphism.

Proof. It is clearly a surjection.

It respects multiplication:

$$\pi(xT \circ yT) = \pi(x\phi(x^{-1}y)T) = x\phi(x^{-1}y)NT =$$
$$= xNT \diamond yNT = \pi(xT) \diamond \pi(yT).$$

Elements $xT, yT \in G/T$ are projected in the same coset of $\tilde{G}/\tilde{T}$ if and only if $x^{-1}y \in NT$. For $N \leq T$ this means $xT = yT$, so π is injective. □

Lemma 1.3.5 *Let Q be a LD quasigroup with Galkin's representation $Q \simeq G/T$ and assume G has no normal subgroups contained in T. Then there is an embedding of G in* $\mathrm{Aut}(Q)$.

Proof. Consider the group mapping

$$\begin{aligned} \psi : G &\to \mathrm{Aut}(Q) \\ g &\mapsto \psi_g : xT \mapsto gxT. \end{aligned}$$

ψ_g is easily seen to be a bijection of G/T. It indeed respects the multiplication of Q:

$$\begin{aligned} &\psi_g(xT \circ yT) = \psi_g(x\phi(x^{-1}y)T) = gx\phi(x^{-1}y)T = \\ &= gx\phi((gx)^{-1}gy)T = gxT \circ gyT = \psi_g(xT) \circ \psi_g(yT) \end{aligned}$$

This means that ψ is correctly defined.

It follows easily that ψ is actually a group homomorphism. Its kernel is

$$\begin{aligned} &\{g \in G \ ; \ xT = gxT \quad \forall x \in G\} = \{g \in G \ ; \ xgx^{-1} \in T \quad \forall x \in G\} = \\ &= \bigcap_{x \in G} xTx^{-1}, \end{aligned}$$

and thus a normal subgroup of G contained in T. This subgroup is trivial from the assumption and so ψ is indeed injective. □

Remark. The homomorphism ψ, when considered as just a homomorphism between G and the symmetric group on the cosets G/T, is commonly known as *action of G on left cosets* - see also [4, Example 1.3.4].

Theorem 1.3.6 (Minimal represesentation)

If G/T is a minimal representation (in the sense that the order of G is the smallest possible) of a LD quasigroup Q, then $G \simeq \mathbf{L}'$.

Proof. The presentation with $G \simeq \mathbf{L}'$ exists: we have $\mathbf{L} \simeq \mathbf{L}'\mathbf{L}_e$ (as in the discussion after 1.2.1). Thus we get the quasigroup isomorphism

$$\mathbf{L} \,/\, \mathbf{L}_e \simeq \mathbf{L}' \,/ \mathbf{L}' \cap \mathbf{L}_e$$

from 1.3.3.

Consider an arbitrary minimal presentation G/T. Then G satisfies the condition of 1.3.5 (if not and $N \leq T$ is a normal subgroup of G, we have an isomorphism of quasigroups $G/T \simeq (G/N)/(NT/N)$ as in 1.3.4

- this contradicts the minimality of G) . Lemma 1.3.5 then gives a group monomorphism

$$\begin{aligned} \psi : G &\to \mathrm{Aut}(G/T, \circ) \\ u &\mapsto (\ xT \mapsto uxT\ ). \end{aligned}$$

Yet any generator of $\mathrm{LMlt}(G/T, \circ)'$ (of the form $\lambda_{aT}\lambda_{bT}^{-1}$) lies in $\psi(G)$ (i.e. it is of the form ($xT \mapsto uxT$)) - namely $\lambda_{aT}\lambda_{bT}^{-1} = (\ xT \mapsto a\phi(a^{-1})\phi(b)b^{-1}xT\ )$. This means $\mathrm{LMlt}(G/T, \circ)' \leq \psi(G)$ (in particular $\mathrm{LMlt}(G/T, \circ)'$ has smaller or equal order), from minimality of G we have $\mathrm{LMlt}(G/T, \circ)' = \psi(G) \simeq G$.

□

Remark (On determination of subquasigroups in Galkin's representation).

Let a LD quasigroup $Q \simeq G/T$ be given.

- Suppose we want to find a subquasigroup. Proposition 1.3.3 guarantees one for any ϕ-subgroup $H \leq G$ (still it may be trivial, if $H = H \cap T$).

  Such subgroups then clearly include the following: characteristic subgroups, normalizers of ϕ-subgroups, "iterated" subgroups of fixed elements $\{x \in G;\ \phi^k(x) = x\}$.

- Let a subquasigroup $Q_0 \leq Q$ be given. We may assume $e \in Q_0$ (else we take the isomorphic - via left translations - subquasigroup, which already includes e). Take the subgroup H generated by $\{\lambda_a; a \in Q_0\}$, it is ϕ-invariant (as $\phi(\lambda_a) = \lambda_e\lambda_a\lambda_e^{-1} = \lambda_{e\circ a} \in H$, since $e \circ a \in Q_0$ for $a \in Q_0$). The mapping $(\lambda_a \mapsto \lambda_a \restriction_{Q_0})$ extends to a surjective homomorphism from H on $\mathbf{L}(Q_0)$. Its kernel consists of the elements of H fixing Q_0 pointwise, which is exactly the center of H (indeed: $\mathbf{L}(Q_0)$ is generated by $\{\lambda_a; a \in Q_0\}$ and $\alpha\lambda_a\alpha^{-1} = \lambda_{\alpha(a)}$, so the central elements are just those fixing all $a \in Q_0$).

1.4 Isogroups

Let G/T be the minimal representation of a LD quasigroup, ϕ being the corresponding automorphism, and suppose that $T = \{1_G\}$. From 1.3.1 follows $\phi(x) = x \Rightarrow x = 1$, which means exactly that ϕ has no nontrivial fixed points.

Then the underlying sets of the quasigroup and the corresponding group G coincide and the quasigroup operation is defined by $x * y = x\phi(x^{-1}y)$.

Such a LD quasigroup $(G, *)$ will be called an *isogroup*. The above discussion shows that it is isotopic to the group $(G, \cdot)$, the isotopy being (ψ, ϕ, id_G) (With $\psi : x \mapsto x\phi(x^{-1})$. The map ψ is injective because of regularity of ϕ [indeed, let $x\phi(x^{-1}) = y\phi(y^{-1})$. Then $x^{-1}y = \phi(x^{-1}y)$, from regularity $x = y$.] As we are talking about finite structures, ψ is also surjective). (For the definition of isotopy, see A.2.1).

The property of being isotopic to a group even characterizes isogroups among LD quasigroups (see [2, Teorema 9.2] for the proposition; it includes even the infinite case).

Proposition 1.4.1 *Let $(G, \circ)$ be an isogroup. A subset $X \subset G$ forms a subquasigroup if and only if X is a left coset of a ϕ-invariant subgroup H in G (that is $X = aH$ for some $a \in G$).*

Proof. Let $X = aH,\ x, y \in H$. Then $ax \circ ay = ax\phi(x^{-1}y) \in aH$, thus $(aH, \circ)$ is a subquasigroup of $(G, \circ)$.

On the other hand, let $(H, \circ)$ be a subquasigroup. First assume $1 \in H$. For $x, y \in H$ choose $x_1, y_1 \in H$ such that $x = x_1 \circ 1,\ y = 1 \circ y_1$, then $x \cdot y = (x_1\phi(x_1^{-1} \cdot 1)) \cdot (1 \cdot \phi(1 \cdot y_1)) = x_1\phi(x_1^{-1}y_1) = x_1 \circ y_1 \in H$, so $(H, \cdot)$ is a subgroup, actually a ϕ-subgroup: we have $\phi(x) = 1 \circ x \in H$ for any $x \in H$.

If $1 \notin H$, consider $H_1 := a \circ H = \lambda_a(H)$ with a chosen so that $1 \in H_1$. $H_1 \simeq H$ as quasigroups, but H_1 is also a ϕ-subgroup, as proved in the above paragraph. Now $H_1 = a\phi(a^{-1})\phi(H)$, so $H = a\,\phi^{-1}(a^{-1})H_1$ (using the ϕ-invariance of H_1). That means H is a left coset by H_1. □

Corollary 1.4.2 (Lagrange's theorem for isogroups)
The order of a subquasigroup in an isogroup divides the order of the latter.

Proposition 1.4.3 *A subquasigroup and a homomorphic image of an isogroup forms again an isogroup.*

Proof.

- The group structure $(G, \cdot)$ on an isogroup $(G, \circ)$ is given by

$$x \cdot y = (x/1) \circ (1\backslash y) \tag{1.9}$$

If we have the epimorphism of quasigroups $\pi : (G, \circ) \to (\tilde{G}, \tilde{\circ})$, define (correctly) the quasigroup structure $(\tilde{G}, \tilde{\cdot})$ on $\tilde{G}$ by

$$\pi(x) \mathbin{\tilde{\cdot}} \pi(y) := (\pi(x) \tilde{/} \pi(1)) \tilde{\circ} (\pi(1) \tilde{\backslash} \pi(y))$$

(so $(\tilde{G}, \tilde{\circ})$ will be isotopic to a group, if we show $(\tilde{G}, \tilde{\cdot})$ is a group).

Now it is enough to verify the equations of associativity for $(\tilde{G}, \tilde{\cdot})$ (because of A.2.2) and these hold: rewrite the equation of associativity for $(G, \cdot)$ using (1.9) and apply π to them (π respects / and $\backslash$ - see the discussion before 1.1.3).

- A subquasigroup Q of an isogroup is isomorphic to a subquasigroup Q_1 containing 1_G and this set is already a group (with the group operation inherited from G). This means Q_1 is isotopic to a group and so an isogroup (and $Q \simeq Q_1$ is thus also an isogroup).

□

Definition 1.4.4 *Let $(Q, \circ)$ be a finite quasigroup, $|Q| = p^k m$, p prime with $p \nmid m$. If Q_0 is a subquasigroup of Q with $|Q_0| = p^k$, then we say Q_0 is a* Sylow p-subquasigroup.

Proposition 1.4.5 *Let $(G, \circ)$ be an isogroup, p a prime dividing $|G|$. Then $(G, \circ)$ has a Sylow p-subquasigroup.*

Proof. Take H a Sylow p-subgroup of $(G, \cdot)$. Then $\phi(H)$ is also a Sylow p-subgroup, therefore $\phi(H) = x_0^{-1} H x_0$ for some $x_0 \in G$ (see A.1.4). Pick x_1 with $x_0 = x_1 \circ 1$, then $x_0 = x_1 \phi(x_1^{-1})$. For such x_1 we have

$$\begin{aligned} &\phi(x_1^{-1} H x_1) = \phi(x_1^{-1}) \phi(H) \phi(x_1) = \phi(x_1^{-1}) x_0^{-1} H x_0 \phi(x_1) = \\ &= \phi(x_1^{-1}) \phi(x_1) x_1^{-1} H x_1 \phi(x_1^{-1}) \phi(x_1) = x_1^{-1} H x_1. \end{aligned}$$

This means that $(x_1^{-1} H x_1, \cdot)$ is a ϕ-invariant Sylow p-subgroup and so $(x_1^{-1} H x_1, \circ)$ is a (Sylow p-) subquasigroup from 1.4.1. □

Definition 1.4.6 Minimal quasigroup *is a quasigroup containing no proper subquasigroups.*

It is possible to characterize minimal isogroups:

Theorem 1.4.7 *A minimal isogroup $(G, \circ)$ is isomorphic to $(\mathbb{F}, \circ)$, where $(\mathbb{F}, +, -, 0, \cdot, 1)$ is a finite field and $u \circ v = \mu u + \nu v$ for some $\nu, \mu \in F$ with $\mu + \nu = 1$, $\nu \neq 0, 1$.*

Proof. From 1.4.5 and minimality, $|G| = p^k$ for some prime p. Let $(G, +)$ be the group corresponding to the isogroup $(G, \circ)$. Consider 1.4.1 and minimality. The center Z of $(G, +)$ is characteristic, it is nontrivial from A.1.3, so it is all G (if not, then $(Z, \circ)$ is a proper subquasigroup). In an abelian group, the elements of order p (and 1) form a characteristic subgroup. Again, it must be all G. That is, $(G, +)$ is isomorphic to the direct product of $\mathbb{Z}_p$ (in particular $(G, +)$ is a vector space over $\mathbb{Z}_p$).

If ϕ is of order m, consider the (finite, commutative) ring $R := \mathbb{Z}_p[x]/(x^m\mathbb{Z}_p[x])$. We may consider $(G, +)$ as a R-module G_R (indeed, a finite $\mathbb{Z}_p$ algebra generated by $\bar{1}, \bar{x} \dots \bar{x}^{m-1}$ over $\mathbb{Z}_p$), with action of $x(x^m\mathbb{Z}_p[x]) =: \bar{x}$ given by $\bar{x}(u) := \phi(u)$ for $u \in G$.

Consider any nontrivial submodule of G_R. It is a ϕ-invariant subspace of G_R, that is - a nontrivial ϕ-invariant subgroup of $(G, +)$. Taking into consideration 1.4.1, this would contradict the minimality of $(G, \circ)$.

This means G_R is a simple R-module, so $G_R \simeq R/\mathcal{I}$ for some maximal ideal $\mathcal{I}$ of $R = \mathbb{Z}_p[x]/(x^m\mathbb{Z}_p[x])$. From the isomorphism theorems, $G_R \simeq \mathbb{Z}_p[x]/(\mathcal{I} + x^m\mathbb{Z}_p[x])$ and $\mathcal{I} + x^m\mathbb{Z}_p[x]$ is a maximal ideal in $\mathbb{Z}_p[x]$. From this, G_R is actually (isomorphic to) a finite field $\mathbb{F}$ and $\phi(u) = \bar{x}(u) = \nu \cdot u$ for some $\nu \in \mathbb{F}$ (if $u \in G$ is considered as an element of $\mathbb{F}$).

We have $\nu \notin \{0, 1\}$, because ϕ was a regular automorphism. Put $\mu := 1 - \nu$, we then have (for $u, v \in G$) $u \circ v = u + \phi(-u + v) = u + \nu \cdot (-u + v) = (1 - \nu)u + \nu v = \mu u + \nu v$, as desired.

On the other hand, if $\mathbb{F}$ is the algebraic field extension $\mathbb{Z}_p(\nu)$, then $(\mathbb{F}, \circ)$ this is indeed a minimal quasigroup (as $\lambda_0 : v \mapsto \nu v$ acts transitively on $G\backslash\{0\}$, so 0 doesn't lie in any proper subquasigroup).

□

Remark. The construction of a R-module representing the action of ϕ as in the proof is a standard one - see for instance [9, chapter XIV].

1.5 More theorems

It was Stein who originally proved the following thoerem, the proof given here is Galkin's.

Theorem 1.5.1 (Stein's theorem)
There are no LD quasigroups of order $4k + 2$, $k \in \mathbb{N}$.

Proof. Assume Q is the smallest quasigroup of order $4k + 2$ and G/T its minimal presentation.

Write $|G| = 2^l m$ with $2 \nmid m$ and observe that $2^{l-1} \mid |T|$ (this is from $|G| = [G:T]|T| = (4k+2) \cdot |T|$).

First we show $l = 1$. Assume for contradiction that $l > 1$. Then there is a nontrivial Sylow 2-subgroup T_2 in T (A.1.4). The normalizer $N_G(T_2)$ is thus a nontrivial ϕ-subgroup. Let G_2 be a Sylow 2-subgroup of G containing T_2. Then $[G_2 : T_2] = 2^l/2^{l-1} = 2$. In particular T_2 is normal in G_2 as a subgroup of index 2, that is $G_2 \leq N_G(T_2)$. $N_G(T_2)$ is not all G in view of the minimality of the presentation (see 1.3.4 - T_2 would be a normal subgroup contained in T). In view of this, $N_G(T_2)T/T \simeq (N_G(T_2)/T_2)/(T/T_2)$ is a proper subquasigroup of order $4k'+2$ (it is divisible by 2, as $[N_G(T_2) : T_2] = [N_G(T_2) : G_2] \cdot [G_2 : T_2] = 2[N_G(T_2) : G_2]$, while $[T : T_2]$ is not divisible by 2; it is not divisible by 4, as $[N_G(T_2)T : T]$ divides $[G : T] = 4k+2$). This contradicts Q being the smallest counterexample.

Thus $l = 1$ and $|T|$ is odd. It follows that a Sylow-2 subgroup (necessarily isomorphic to $\mathbb{Z}_2$, so cyclic) in G has a normal complement N (A.1.10). From this we have $G' < G$ (as G' is the smallest subgroup of G such that G/G' is abelian, so $G' \leq N$).

Then we can consider the induced quasigroup structure on G/G' from 1.3.4 - the quasigroup has order $4k'+2$: Its order is not divisible by 4, as G/T, of which it is an epimorphic image, has order not divisible by 4 - see the discussion before 1.1.4). Its order is divisible by 2, as $|(G/G')/(G'T/G')| = \frac{[G:G']}{[G'T:G']}$ and while $[G'T : G']$ is not divisible by 2 (since $|T|$ is odd), $[G : G'] \geq [G : N] = 2$ is even.

In view of the minimality of $|Q|$, we have $G' = \{1\}$. Now G is abelian, so Q is an isogroup and the Sylow subquasigroup is of order 2 from 1.4.5 - but LD quasigroups of order 2 do not exist. □

We will now obtain some more results on minimal quasigroups. Let Q be a LD quasigroup with the representation $\mathbf{L} \,/\, \mathbf{L}_e$.

Theorem 1.5.2 *Every minimal quasigroup is an isogroup.*

Proof. Let $Q_0 \subseteq Q$ be the elements invariant to automorphisms from $\mathbf{L}_a \cap \mathbf{L}_b$. Q_0 is closed with respect to multiplication, thus a subquasigroup (nontrivial - it contains at least a and b). We have $Q_0 = Q$ from minimality, so $\mathbf{L}_a \cap \mathbf{L}_b = \{id\}$ for $a \neq b$. This means that every mapping in $\mathbf{L}$ fixes at most 1 point, moreover the left translations fixes exactly one point - thus $\mathbf{L}$ is a Frobenius group (see A.1.7). Consider its Frobenius kernel K, we have $\mathbf{L} = K\,\mathbf{L}_e$, and K is a ϕ-subgroup (as K is normal and ϕ is a conjugation of $\mathbf{L}$) . From 1.3.3 we have the following quasigroup

isomorphisms:

$$Q \simeq \mathbf{L}\,/\,\mathbf{L}_e = (K\,\mathbf{L}_e)/\,\mathbf{L}_e \simeq K/(K \cap \mathbf{L}_e) = K/1,$$

which shows that Q is an isogroup. □

Remark. This classifies (together with 1.4.7) the minimal finite LD quasigroups. In particular, they are all medial.

Theorem 1.5.3 ("Weak Lagrange property") *Let Q a LD quasigroup, Q_0 its minimal subquasigroup. The orders of Q_0 and Q cannot be relatively prime.*

First, a lemma:

Lemma *Assume G is a group, Z its center and G/Z a p-group. Then the Sylow p-subgroup $G_p \leq G$ is normal in G.*

Proof. Consider the subgroup $Z_0 \leq Z$ of elements with order coprime to p. Then $Z_0 \cap G_p = \{1\}$, Z_0 commutes with G_p and $G = Z_0 G_p$. Thus $G \simeq Z_0 \times G_p$ and $G_p \trianglelefteq G$. □

Proof of 1.5.3. If Q_0 is trivial, then the statement holds. Hence suppose that $|Q_0| > 1$.

We may assume $e \in Q_0$ (else take a subquasigroup isomorphic to Q_0 - via a left translation - which already contains e).

Consider $H := \langle \lambda_a; a \in Q_0 \rangle \leq \mathbf{L}(Q)$, H is ϕ-invariant and $H/Z(H) \simeq \mathbf{L}(Q_0)$ (cf. the discussion after 1.3.6). $|\,\mathbf{L}(Q_0)'| = |Q_0|$, because Q_0 is minimal (therefore an isogroup) and because of 1.3.6. Thus, from 1.4.7, $|\,\mathbf{L}(Q_0)'| = p^k$ for some prime p.

$\mathbf{L}(Q_0)'$ is $\tilde{\phi}$-invariant in $\mathbf{L}(Q_0)$ (where $\tilde{\phi}$ is the same as in the discussion before 1.3.4; this is the same situation, with $G := H,\ N := Z(H)$) and so is the preimage (by the canonical projection $\pi_{Z(H)} : H \to \mathbf{L}(Q_0)$) of $\mathbf{L}(Q_0)'$ in H (denote it by $\hat{H}$) ϕ-invariant in H. $\hat{H}/Z(\hat{H})$ is a p-group (we have $|\hat{H}/Z(\hat{H})| \leq |\hat{H}/(Z(H) \cap \hat{H})| = |\pi_{Z(H)}(\hat{H})| = p^k$). Therefore, by the preceding lemma, $\hat{H}_p$ is normal in $\hat{H}$ - then it is the unique Sylow p-subgroup of $\hat{H}$ (A.1.4), therefore ϕ-invariant (in fact, even characteristic).

For contradiction, assume $p \nmid |Q|$. From $|\,\mathbf{L}(Q)| = |Q| \cdot |\,\mathbf{L}(Q)_e|$, we have that the order of Sylow p-subgroups of $\mathbf{L}(Q)_e$ is the same as the order of the Sylow p-subgroups of $\mathbf{L}(Q)$. This implies that the Sylow p-subgroups of $\mathbf{L}(Q)_e$ form a subset of the Sylow p-subgroups of $\mathbf{L}(Q)$ (in particular, they are all mutually conjugated in $\mathbf{L}(Q)$).

Let $\hat{P}$ be a Sylow p-subgroup, containing $\hat{H}_p$ (this is possible, since $\hat{H}_p$ is a p-group of $\mathbf{L}(Q)$). Choose P to be any Sylow p-subgroup in $\mathbf{L}(Q)_e$, $\hat{P} = s_0 P s_0^{-1}$ for some $s_0 \in \mathbf{L}(Q)$ (as discussed in the preceding paragraph). In particular, we can write any $h \in \hat{H}_p$ as

$$h = s_0 y s_0^{-1}, \quad y \in \mathbf{L}(Q)_e$$

$\hat{H}_p$ is ϕ-invariant, so $h\phi(h^{-1}) \in H$ and we may write

$$h\phi(h^{-1}) = s_0 z s_0^{-1}, \quad z \in \mathbf{L}(Q)_e$$

That is, $h\phi(h^{-1}) \in s_0 \mathbf{L}(Q)_e s_0^{-1}$ and from 1.3.1, $h \in \mathbf{L}(Q)_e$. Since h in $\hat{H}_p$ was arbitrary, we have $\hat{H}_p \leq \mathbf{L}(Q)_e$. This means ϕ acts trivially on $\hat{H}_p$ and consequently $\tilde{\phi}$ acts trivially on $\pi_{Z(H)}(\hat{H}_p) \simeq \pi_{Z(H)}(\hat{H}) \simeq \mathbf{L}(Q_0)'$, that is $\mathbf{L}(Q_0)' = \mathbf{L}(Q_0)'_e = \{1\}$ (since Q_0 is an isogroup) and $|\mathbf{L}(Q_0)'| = |Q_0| = 1$. Q_0 is a trivial subquasigroup, a contradiction. Thus p divides $|Q|$.

□

Finally, we proceed to the structure theorem for *distributive* quasigroups, which will prove useful in the classification.

We need the following result of Smith [11, p.39]:

Theorem 1.5.4 *Assume that $(Q, \circ)$ is a finite distributive quasigroup. Then* $\mathrm{LMlt}(Q)'$ *is a direct product of an abelian group of order prime to 3 and of a 3-group. In particular,* $\mathrm{LMlt}'(Q)$ *is nilpotent.*

Remark. The last theorem in turn stems from the structure theorems concerning commutative Moufang loops.

Theorem 1.5.5 (Structure theorem for distributive quasigroups) *Let Q be a distributive quasigroup of order $n = 3^k m$ where $k, m \in \mathbb{N}$ and $3 \nmid m$. Then $Q \simeq Q_A \times Q_3$, where Q_A is a medial idempotent quasigroup of order m and Q_3 is a distributive quasigroup of order 3^k.*

Proof. Write $Q \simeq \mathbf{L}' / \mathbf{L}'_e$. The Smith's result applies to get the direct decomposition: $\mathbf{L}' \simeq G_A \times G_3$ and the corresponding decomposition $\mathbf{L}'_e \simeq (G_A)_e \times (G_3)_e$. Both G_A and G_3 are ϕ-invariant (from coprimality) and ϕ induces the quasigroup structure on each. Consider the mapping

$$\begin{aligned} \psi : \quad & \mathbf{L}' / \mathbf{L}'_e \to G_A/(G_A)_e \times G_3/(G_3)_e \\ & g\,\mathbf{L}'_e = g_A g_3\,\mathbf{L}'_e \mapsto (g_A(G_A)_e, g_3(G_3)_e) \qquad g_A \in G_A,\ g_3 \in G_3. \end{aligned}$$

ψ is a quasigroup isomorphism: It is correctly defined, as $g = g_A g_3$ uniquely. It is clearly surjective. It is injective - either from surjectivity and finiteness or by direct calculation. It is a homomorphism of quasigroups (from finiteness, it is enough to verify that ψ respects multiplication):

$$\begin{aligned}\psi(g\,\mathbf{L}'_e \circ h\,\mathbf{L}'_e) &= \psi(g\phi(g^{-1}h)\,\mathbf{L}'_e) = \psi(g_A\phi(g_A^{-1}h_A)g_3\phi(g_3^{-1}h_3)\,\mathbf{L}'_e) = \\ &= (g_A\phi(g_A^{-1}h_A)(G_A)_e,\ g_3\phi(g_3^{-1}h_3)(G_3)_e) = \\ &= (g_A \circ_A h_A(G_A)_e,\ g_3 \circ_3 h_3(G_3)_e) = \\ &= (g_A(G_A)_e, g_3(G_3)_e) \diamond (h_A(G_A)_e, h_3(G_3)_e) = \\ &= \psi(g\,\mathbf{L}'_e) \diamond \psi(h\,\mathbf{L}'_e)\end{aligned}$$

(the second equality is justified by that G_A and G_3 commute with each other and they are ϕ-invariant).

From the Smith's result, G_A is abelian. Since

$$Q \simeq \mathbf{L}' \,/\, \mathbf{L}'_e \simeq G_A/(G_A)_e \times G_3/(G_3)_e$$

was the minimal presentation, we already have $(G_A)_e = \{1\}$ (else $(G_A)_e \times \{1\}$ would be normal, contained in $(G_A)_e \times (G_3)_e$ and nontrivial). Now it is enough to put $Q_A := G_A/(G_A)_e = G_A/1,\ Q_3 := G_3/(G_3)_e$.

Mediality of Q_A is easily verified (we have $x \circ_A y = x\phi(x^{-1}y)$ for $x, y \in G_A$):

$$\begin{aligned}(x \circ_A y) \circ_A (z \circ_A w) &= x\phi(x^{-1}y)\phi^2(y^{-1}x)\phi(x^{-1}z)\phi^2(z^{-1}w) \\ \text{and: } (x \circ_A z) \circ_A (y \circ_A w) &= x\phi(x^{-1}z)\phi^2(z^{-1}x)\phi(x^{-1}y)\phi^2(y^{-1}w).\end{aligned}$$

Both expressions are equal from the commutativity of G_A. □

Remark.

- According to Galkin, the smallest distributive 3-quasigroup which is not medial has 3^4 elements.
- In general, assume that a LD quasigroup $Q \simeq G/G_e$ and $G \simeq G_1 \times \ldots \times G_k$, with G_i having mutually coprime orders (so that every G_i is characteristic and thus ϕ-invariant). Then we may consider a quasigroup isomorphism

$$\begin{aligned}G/G_e &\to G_1/(G_1)_e \times \ldots \times G_k/(G_k)_e \\ g_1 g_2 \ldots g_k G_e &\mapsto (g_1(G_1)_e, \ldots, g_k(G_k)_e) \qquad g_i \in G_i\end{aligned}$$

as in the theorem.

In particular, if $\mathrm{LMlt}'(Q)$ is nilpotent (which need not be the case - it is not, for example, for the two LD non-RD quasigroups constructed in 3.1), we can obtain the decomposition in a direct product of p-quasigroups (because $\mathrm{LMlt}'(Q)$ is then isomorphic to a direct product of its Sylow p-subgroups from A.1.5). However, we can say nothing more about the structure of these p-quasigroups.

- One consequence: Given $Q_A \simeq G_A/1$ from the theorem in the minimal presentation, we can decompose the abelian G_A in a direct product of its p_i-primary components (with p_i primes): $G_A \simeq G_{p_1} \times \ldots \times G_{p_k}$. This then gives a decomposition of Q_A in p-quasigroups: $Q_A \simeq G_{p_1}/1 \times \ldots \times G_{p_k}/1$.

  Putting it all together, we may formulate Structure theorem 1.5.5 in the form which appeared in the Galkin's article:

  Corollary 1.5.6 (Structure theorem - a reformulation) *Let Q be a distributive quasigroup. Let $|Q| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ where $k, \alpha_1, \ldots, \alpha_k \in \mathbb{N}$ and $p_1, \ldots, p_k$ are distinct primes. Then $Q \simeq Q_1 \times \cdots \times Q_k$, where Q_i is a quasigroup of order $p_i^{\alpha_i}$. Q_i is medial for $p_i \neq 3$.*

Chapter 2

Classification of small LD quasigroups

2.1 Introduction and basic considerations

In this chapter, we provide the classification of LD quasigroups of order up to 15.

The first step will be to characterize the medial idempotent (recall that left distributivity implies idempotence) quasigroups of order up to 15.

Second, we show that all LD quasigroups of order less than 14 are medial. Actually, there exist non-medial LD quasigroups already of order 15, as was demonstrated in [13, p.29]. In section 3.1, we construct them explicitly using the Galkin's representation.

2.2 Medial case

First we make several remarks concerning any finite quasigroup (not just the small ones).

As medial idempotent (MI) quasigroups are both left and right distributive, we can use the Structure theorem 1.5.6 and it follows that it is enough to classify quasigroups Q such that $|Q| = p^k,\ k \in \mathbb{N},\ p$ prime.

It is known, how do all medial quasigroups arise (for the original Toyoda's article, see [14]):

Theorem 2.2.1 (Toyoda's theorem) *A quasigroup $(Q, \cdot)$ is medial if and only if there exists an Abelian group $(Q, +)$, its automorphisms $\alpha, \beta \in$*

$Aut(Q,+)$ and $c \in Q$ such that α and β commute and

$$x \cdot y = \alpha(x) + \beta(y) + c \quad \textit{for all } x, y \in Q \tag{2.1}$$

Proof. See [5, p.12-14] . □

Remark. Suppose $(Q, \cdot)$ is also idempotent. Let 0 denote the neutral element in $(Q, +)$. Applying (2.1) with $x = 0,\ y = 0$ yields $c = 0$. Moreover, choosing arbitrary $a \in Q$, applying (2.1) to $x = a, y = a$ and using idempotency we obtain $\alpha + \beta = 1$ in the endomorphism ring of $(Q, +)$.

Also note that in the idempotent case $\alpha = \rho_0,\ \beta = \lambda_0$ and Toyoda's representation coincides with the Galkin's representation (with $\phi = \beta$, we have $x \cdot y = x + \phi(-x + y)$ and ϕ have no fixed points except for 0, i.e. medial idempotent quasigroups are special cases of isogroups).

Therefore, from Toyoda's theorem, every MI quasigroup arise as follows: it is enough to consider an abelian group G of respective order and to such group we assign (α, β) as a pair of automorphisms of G, such that $\alpha\beta = \beta\alpha$ and $\alpha + \beta = 1,\ \alpha, \beta \notin \{0, 1\}$ in the ring of endomorphisms of the respective group. Denote the corresponding quasigroup as (G, α) (as β is uniquely determined by α). When do two quasigroups (G, α) and (G', α') turn out to be isomorphic?

First, if G and G' are not isomorphic, then neither are the quasigroups isomorphic. (Indeed, if the quasigroups $Q = (G, \alpha)$ and $Q' = (G', \alpha')$ are isomorphic, then they are in particular isotopic; next Q is isotopic to G, Q' is isotopic to G'. But the isotopy relation is an equivalence, so G and G' are also isotopic. Now, two isotopic groups are already isomorphic [12, Proposition 1.4]).

Now let $G = G'$. We turn our attention to the automorphisms inducing the quasigroup structure (that is, α and β in the medial idempotent case and, more generally, ϕ in the case of the Galkin's representation of an arbitrary finite isogroup).

Proposition 2.2.2 *Let $(G, \cdot)$ be a group and let $(G, *)$ and $(G, \odot)$ be isogroups such that*

$$x * y = x\phi(x^{-1}y) \tag{2.2}$$

$$x \odot y = x\phi'(x^{-1}y) \tag{2.3}$$

(with $\phi, \phi' \in \mathrm{Aut}(G, \cdot)$, such that their unique fixed point is 1_G).

Suppose that $(G, *) \simeq (G, \odot)$. Then there is an isomorphism κ of them, such that κ is also an automorphism of $(G, \cdot)$. Moreover,

$$\tilde{\phi} = \kappa\phi\kappa^{-1}. \tag{2.4}$$

Proof. Observe that

$$x \cdot y = \psi^{-1}(x) * \phi^{-1}(y) = \tilde{\psi}^{-1}(x) \odot \tilde{\phi}^{-1}(y), \tag{2.5}$$

where

$$\psi(x) = x\phi(x^{-1}), \qquad \tilde{\psi}(x) = x\tilde{\phi}(x^{-1})$$

are bijections of G (because injectivity of ϕ, respectively $\tilde{\phi}$ implies injectivity of ψ, respectively $\tilde{psi}$ and finiteness then gives the surjectivity).

Let ζ be an isomorphism of the two quasigroups. First assume that $\zeta(1) = 1$. Then it is enough to take $\kappa = \zeta$. Indeed $\zeta(\psi(x) \cdot \phi(y)) = \zeta(x * y) = \zeta(x) \odot \zeta(y) = \tilde{\psi}(\zeta(x)) \cdot \tilde{\phi}(\zeta(y))$ for all $x, y \in G$, so plugging $x = 1$ gives $\zeta(\phi(y)) = \tilde{\phi}(\zeta(y))$ for all $y \in G$, which means (2.4). Also note, that similarly putting $y = 1$ gives $\tilde{\psi} = \zeta\psi\zeta^{-1}$.

Next (by (2.5) and since from the last paragraph we deduce $\tilde{\phi}^{-1}\zeta = \zeta\phi^{-1}$ and $\tilde{\psi}^{-1}\zeta = \zeta\psi^{-1}$) we get $\zeta(x) \cdot \zeta(y) = \tilde{\psi}^{-1}(\zeta(x)) \odot \tilde{\phi}^{-1}(\zeta(x)) = \zeta(\psi^{-1}(y)) \odot \zeta(\phi^{-1}(y)) = \zeta(\tilde{\psi}^{-1}(x) * \tilde{\phi}^{-1}(y)) = \zeta(x \cdot y)$, so $\zeta \in \mathrm{Aut}(G, \cdot)$ (it is a bijection as a quasigroup automorphism).

In case $\zeta(1) \neq 1$, choose $a \in G$, such that $a \odot \zeta(1) = 1$; this is possible, because $(G, \odot)$ is a quasigroup. Then $\kappa = \lambda_a^{\odot}\zeta$ satisfies $\kappa(1) = 1$ and κ is an isomorphism of $(G, *)$ and $(G, \odot)$ (as $\lambda_a^{\odot} \in \mathrm{Aut}(G, \odot)$), so $\kappa \in \mathrm{Aut}(G, \cdot)$ follows from the first part of the proof. □

From this the desired conclusion for MI quasigroups immediately follows:

Corollary 2.2.3 *Let $(G, +)$ be an abelian group and let $(G, *)$ and $(G, \odot)$ be MI quasigroup such that*

$$x * y = \alpha(x) + \beta(y)$$
$$x \odot y = \tilde{\alpha}(x) + \tilde{\beta}(y)$$

$$x, y \in G, \quad \alpha, \beta, \tilde{\alpha}, \tilde{\beta} \in \mathrm{Aut}(G, +);$$
$$\alpha\beta = \beta\alpha, \ \tilde{\alpha}\tilde{\beta} = \tilde{\beta}\tilde{\alpha}, \ \alpha + \beta = id, \ \tilde{\alpha} + \tilde{\beta} = id.$$

Suppose that $(G, *) \cong (G, \odot)$. Then there is an isomorphism κ of them, such that κ is also an automorphism of $(G, +)$. Moreover,

$$\tilde{\alpha} = \kappa\alpha\kappa^{-1}, \ \tilde{\beta} = \kappa\beta\kappa^{-1}.$$

Proof. This is immediate from 2.2.2 and from the above note about the equivalence of Toyoda's and Galkin's presentations for MI quasigroups.

Following the proof of 2.2.2, we have $\beta = \phi$, $\alpha = \psi = id - \beta$. But in the abelian case, $id - \beta$ is already an automorphism of $(G, +)$ and β and $id - \beta$ commutes (and similarly for the tilded mappings). □

A kind of stronger converse to Proposition 2.2.2 holds:

Proposition 2.2.4 *Assume $(G/T, \phi), (G/T', \phi')$ are two quasigroups in Galkin's representation:*

$$xT * yT = x\phi(x^{-1}y)T \tag{2.6}$$
$$xT' \odot yT' = x\phi'(x^{-1}y)T' \tag{2.7}$$

and $\phi' = \kappa\phi\kappa^{-1}$ for some $\kappa \in \mathrm{Aut}(G)$. Then $(G/T, \phi) \cong (G/T', \phi')$.

Proof. If T are the fixed points of ϕ and T' are the fixed points of ϕ', then necessarily $\kappa(T) = T'$. Define

$$f : (G/T, \phi) \to (G/T', \phi')$$
$$xT \mapsto \kappa(x)T'.$$

Correctness of the definition follows from $\kappa(T) = T'$. The mapping f is obviously a bijection. It is a quasigroup homomorphism:

$$f(xT) \odot f(yT) = \kappa(x)T' \odot \kappa(y)T' = \kappa(x)\phi'(\kappa(x^{-1}y))T' =$$
$$= \kappa(x)\kappa(\phi(x^{-1}y))\kappa(T) = \kappa(x\phi(x^{-1}y)T) = f(xT * yT).$$

Therefore, f is the desired isomorphism of $(G/T, \phi)$ and $(G/T', \phi')$. □

Remark.

- In the context of this chapter, we use this proposition with G abelian and $T = \{0\}$, with Toyoda's presentation coinciding with the Galkin's one (with $\phi = \beta = id - \alpha,\ \phi' = \beta' = id - \alpha'$). Furthermore, the proposition will prove useful in Section 3.1.

- The proposition essentially says, that when considering possible $\phi \in \mathrm{Aut}(G, \cdot)$, it is enough to consider just one arbitrary representative in every conjugacy class of $\mathrm{Aut}(G, \cdot)$.

  We should verify that this is actually independent of the choice of ϕ in the given conjugacy class $\mathcal{C}$ of $\mathrm{Aut}(G, \cdot)$ (i.e. if one representative ϕ gives $(G/T, \phi)$ being a LD quasigroup, then every automorphism in $\mathcal{C}$ does): Indeed, for ϕ, ϕ', assume $(G/T, \phi)$ is a LD quasigroup. Now $(G/T', \phi')$ is a groupoid. But in the proof of 2.2.4, we have actually exhibited a groupoid isomorphism of $(G/T, \phi)$ and $(G/T', \phi')$. Now, since $(G/T, \phi)$ is finite and $(G/T', \phi')$ is a (groupoid) homomorphic image of it, $(G/T', \phi')$ must be already a LD quasigroup.

- We may ask if the stronger generalization of 2.2.2 also holds:

  Question: *Assume* $(G/T, \phi)$ *and* $(G/T', \phi')$ *are two quasigroups in Galkin's representation:*

$$xT * yT = x\phi(x^{-1}y)T$$
$$xT' \odot yT' = x\phi'(x^{-1}y)T'.$$

  Assume $(G/T, \phi) \simeq (G/T', \phi')$. *Is there* $\kappa \in \mathrm{Aut}(G)$, *such that* $\phi' = \kappa\phi\kappa^{-1}$? (Then necessarily κ induces an automorphism of the quasigroups as in the proof of 2.2.4.)

  If the answer is positive, we believe it may be proved by a suitable generalization of proof of 2.2.2.

Using 2.2.3 and 2.2.4, we see that to classify medial quasigroups up to some order, it is enough to list (for every $(G, +)$ abelian up to the order) all suitable pairs $(\alpha, id - \alpha)$ of automorphisms of $(G, +)$, with at most one automorphism α for every conjugacy class in $\mathrm{Aut}(G, +)$. This is done, up to order 15, below.

Remark. It is perhaps worth noting that there are no medial quasigroups isotopic to abelian groups having direct decomposition $G \cong \mathbb{Z}_{2^k} \times \prod_{i=1}^{n} C_i$ ($\{C_i, i = 1 \ldots n\}$ cyclic not containing $\mathbb{Z}_{2^k}$, $k \geq 1$), as elements $g := \langle 2^{k-1}, a_1, \ldots, a_n \rangle$ maps by any automorphsim α to an element of the same type, thus $\alpha(g) + (id - \alpha)(g) \neq g$, since it has 0 in the first position.

The classification. Of the abelian groups of order up to 15, we may, by the preceding remark, omit some even without counting automorphisms: $\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_{10}, \mathbb{Z}_2 \times \mathbb{Z}_6, \mathbb{Z}_{14}$.

We start with the prime numbers (Table 2.1). Note that there always has to be $p - 2$ non-isomorphic quasigroups, with one left symmetric (i.e. $x * (x * y) = y$ for every $x, y \in Q$), one right symmetric and one commutative. Groups are assumed to be represented as numbers modulo p.

The situation in cyclic groups of prime power order is similar (Table 2.2), except that there are relatively fewer automorphisms.

Consider elementary abelian groups (see Table 2.3; we assume the representation of elements of $\mathbb{Z}_p^n$ as vectors over $\mathbb{Z}_p$). In every case, some conjugacy classes of automorphisms contain more then one mapping - the automorphisms α listed in Table 2.3 were chosen arbitrarily. In brackets, the number of appropriate conjugacy classes in $\mathrm{Aut}(G)$ is listed, out of the number of all the classes.

The conjugacy classes of $\mathrm{Aut}(G)$ were found and sorted using the algebra package GAP [8].

The remaining small quasigroups (isotopic to $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_3 \times \mathbb{Z}_5$ respectively) are isomorphic to the direct product of quasigroups in view of the Structure theorem 1.5.6. Thus, we may observe, from what we already know about the quasigroups isotopic to $\mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_5$, that there is exactly one quasigroup isotopic to $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and three isotopic to $\mathbb{Z}_3 \times \mathbb{Z}_5$. We do not list them.

α	$id - \alpha$
$x \mapsto 2x$	$x \mapsto 2x$

2.1.1: $\mathbb{Z}_3$

α	$id - \alpha$
$x \mapsto 2x$	$x \mapsto 4x$
$x \mapsto 3x$	$x \mapsto 3x$
$x \mapsto 4x$	$x \mapsto 2x$

2.1.2: $\mathbb{Z}_5$

α	$id - \alpha$
$x \mapsto 2x$	$x \mapsto 6x$
$x \mapsto 3x$	$x \mapsto 5x$
$x \mapsto 4x$	$x \mapsto 4x$
$x \mapsto 5x$	$x \mapsto 3x$
$x \mapsto 6x$	$x \mapsto 2x$

2.1.3: $\mathbb{Z}_7$

α	$id - \alpha$
$x \mapsto 2x$	$x \mapsto 10x$
$x \mapsto 3x$	$x \mapsto 9x$
$x \mapsto 4x$	$x \mapsto 8x$
$x \mapsto 5x$	$x \mapsto 7x$
$x \mapsto 6x$	$x \mapsto 6x$
$x \mapsto 5x$	$x \mapsto 7x$
$x \mapsto 4x$	$x \mapsto 8x$
$x \mapsto 3x$	$x \mapsto 9x$
$x \mapsto 2x$	$x \mapsto 10x$

2.1.4: $\mathbb{Z}_{11}$

α	$id - \alpha$
$x \mapsto 2x$	$x \mapsto 12x$
$x \mapsto 3x$	$x \mapsto 11x$
$x \mapsto 4x$	$x \mapsto 10x$
$x \mapsto 5x$	$x \mapsto 9x$
$x \mapsto 6x$	$x \mapsto 8x$
$x \mapsto 7x$	$x \mapsto 7x$
$x \mapsto 8x$	$x \mapsto 6x$
$x \mapsto 9x$	$x \mapsto 5x$
$x \mapsto 10x$	$x \mapsto 4x$
$x \mapsto 11x$	$x \mapsto 3x$
$x \mapsto 12x$	$x \mapsto 2x$

2.1.5: $\mathbb{Z}_{13}$

Table 2.1: Quasigroups corresponding to groups of prime order

α	$id-\alpha$
$x \mapsto 2x$	$x \mapsto 8x$
$x \mapsto 5x$	$x \mapsto 5x$
$x \mapsto 8x$	$x \mapsto 2x$

2.2.1: $\mathbb{Z}_9$

Table 2.2: Quasigroups corresponding to cyclic p-groups

α	$id-\alpha$
$x \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} x$

2.3.1: $\mathbb{Z}_2 \times \mathbb{Z}_2$, 1 out of 3

α	$id-\alpha$
$x \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} x$
$x \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} x$

2.3.2: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, 2 out of 6

α	$id-\alpha$
$x \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} x$
$x \mapsto \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} x$
$x \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix} x$
$x \mapsto \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} x$
$x \mapsto \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} x$	$x \mapsto \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} x$

2.3.3: $\mathbb{Z}_3 \times \mathbb{Z}_3$, 5 out of 8

Table 2.3: Quasigroups corresponding to elementary abelian p-groups

2.3 Ruling out non-medial quasigroups

The statements in this part which concern groups of some particular order (for instance, 12 or 27) were checked using GAP [8] (unless they are justified by other means).

Let Q be a LD quasigroup with a distinguished element e, $\mathbf{L}$ its left multiplication group, $\mathbf{L}'$ the commutant of $\mathbf{L}$, $\mathbf{L}_e$ the stabilizer of $e \in Q$ in $\mathbf{L}$. For $a \in Q$ let λ_a be the left translation by a (note that for any $b \in Q$ are λ_a and λ_b conjugated in $\mathrm{LMlt}(Q)$ by 1.2.1).

When we talk about the Galkin's presentations $\mathbf{L} / \mathbf{L}_e$, $\mathbf{L}' / \mathbf{L}'_e$, we always assume the quasigroup structure induced by $\phi = (u \mapsto \lambda_e u \lambda_e^{-1}) \in \mathrm{Aut}(\mathbf{L})$ (and we identify it with its restriction on $\mathbf{L}'$).

By saying Q has cycle type k_1-k_2 - ... - k_m, we mean λ_e has such cycle type.

We first state a few useful observations:

Lemma 2.3.1 *Let $(Q, \cdot)$ be a LD quasigroup.*

(i) If Q is minimal (i.e. it has no proper subquasigroups), then it is medial.

(ii) If Q_0 is a subquasigroup of Q and $a \in Q_0$, then $\lambda_a^{Q_0}$ has the same cycle structure as λ_a restricted to Q_0, where $\lambda_a^{Q_0}$ is the left translation by a considered as a mapping in $\mathrm{LMlt}(Q_0)$

(iii) The set of fixed points of $u \in \mathbf{L}$ forms a subquasigroup (not necessarily proper).

(iv) The length l of the longest cycle in the cycle type of Q is always less than $|Q| - b$, where b is the size of the largest subquasigroup Q_0 in Q.

Proof.

(i) From 1.5.2, we know Q is an isogroup. The minimal isogroups are characterized by 1.4.7 - it is immediately verified, that the quasigroups mentioned in 1.4.7 are medial.

(ii) Obvious.

(iii) Because u is an automorphism of Q - fixed points of any automorphism form a substructure.

(iv) We may assume that Q_0 contains e (otherwise an isomorphic copy of Q_0 does - namely image of Q_0 under an appropriate left translation). λ_e fixes e, which lies in the subquasigroup, thus λ_e must fix the whole Q_0 setwise, as $e \cdot a \in Q_0,\ \forall a \in Q_0$. The number of elements in Q_0 itself is less than $|Q| - b$ from 1.1.5.

□

LD quasigroups of cardinality 3, 5, 7, 11, and 13 are minimal from 1.5.3, as any subquasigroup would have coprime order to the order of the whole quasigroup. Quasigroups of cardinality 4 and 8 are minimal from 1.1.5, as any nontrivial subquasigroup would have order 2 - but there is no such LD quasigroup. All of the LD quasigroups of these orders are therefore medial, from the preceding observations.

There are no LD quasigroups of order 6, 10 and 14 - from 1.5.1.

In classifying the small non-medial quasigroups, we may immediately consider just the non-right distributive (in view of 1.5.5 and the Galkin's comment, that the first distributive non-medial 3-quasigroup is on 81 elements).

Thus, we restrict our attention to orders 9, 12 and 15. Observe that such LD quasigroups (if not medial) will not be isogroups (groups on 9 and 15 elements are only abelian, the three non-abelian groups of order 12 have no regular automorphisms - which are necessary to induce the isogroup structure - see the beginning of Section 1.4).

Therefore, in what follows, we will try to derive some necessary conditions for a quasigroup to be a non-RD non-isogroup (i.e. we do not consider isogroups).

First a little proposition (of which we actually use just a small bit):

Proposition 2.3.2 *(About congruences in LD quasigroups)*
Let $(Q, *)$ be a finite LD quasigroup and $\mathbf{B}$ a nontrivial partition of Q.

1. *If the equivalence $\sim_{\mathbf{B}}$ corresponding to the partition is a congruence on Q, then $\mathbf{B}$ is a system of blocks (see A.1.1 for the definition) under the action of $\mathbf{L}$.*

2. *On the other hand, if $\mathbf{B}$ is a system of blocks under the action of $\mathbf{L}$, then the elements of $\mathbf{B}$ are isomorphic subquasigroups.*

Proof.

- Let $B \in \mathbf{B}$ - it is a normal subquasigroup in Q (see the discussion before 1.1.4).

  Write any mapping in $\mathrm{LMlt}(Q)$ as $u = \lambda_{x_0}^{\sigma_0} \dots \lambda_{x_n}^{\sigma_n}$ ($x_i \in Q,\ \sigma_i = \pm 1$). Now for any $b \in B$, the result of $u(b)$ is exactly the result of succesive left multiplying or left division by x_i (depending on whether $\sigma_i = 1$ or -1). Since B is a block of congruence, all $b \in B$ end up in the same block of congruence, say B_1. Then either $u(B) = B_1 \neq B$ and $u(B) \cap B = \emptyset$ or $u(B) = B_1 = B$. Since $u \in \mathrm{LMlt}(Q)$ was arbitrary, it follows that $\mathbf{B}$ is a system of blocks under the action of $\mathrm{LMlt}(Q)$.

- Let $B \in \mathbf{B}$ be a block in Q with respect to the action of $\mathbf{L}$.

  B is a subquasigroup - let $x,\ y \in B$. Then $\lambda_x(x) = x$, so $\lambda_x(B) = B$ and $x * y = \lambda_x(y) \in B$. All the B are isomorphic via appropriate left translations.

□

Remark.

- If $\mathbf{B}$ is a system of blocks under the action of $\mathbf{L}$, then for $y, z \in B \in \mathbf{B}$ we have also $x * z \sim_{\mathbf{B}} x * y$, because $\lambda_x \in \mathbf{L}$.

  However, $\mathbf{B}$ induces a congruence on Q (i.e. every $B \in \mathbf{B}$ is a normal subquasigroup) if and only if $\lambda_y^{-1}\lambda_z$ acts trivially on $\mathbf{B}$ whenever y and z lie in the same block of $\mathbf{B}$. Then for $x \in B,\ y, z \in B' \in \mathbf{B}$, we have $z * x \sim_{\mathbf{B}} y * x$ because $\lambda_z^{-1}\lambda_y$ stabilizes B.

- It is worth noting, that if we take a non-normal subquasigroup Q_0, then the set of all translates of Q_0 under $\mathbf{L}$ need not form a partition of Q. This is the case for 3-elements subquasigroups in the two non-RD quasigroups of order 15 constructed in 3.1.

In the classification, we proceed in two basic steps. First, we consider how to exhibit a normal subquasigroup in Q. Second, a normal subquasigroup gives rise to an epimorphism of quasigroups, which in turn gives rise to an epimorphism of their respective multiplication groups - we then examine the respective multiplication groups and their commutator subgroups.

2.3.1 Simple LD quasigroups

Consider the minimal presentation $Q = \mathbf{L}' / \mathbf{L}'_e$ and any normal proper ϕ-subgroup $N \lhd \mathbf{L}'$ (in particular this holds for any nontrivial proper characteristic subgroup). The theorem 1.3.4 gives us the quasigroup epimorphism $\mathbf{L}' / \mathbf{L}'_e \to (\mathbf{L}' / N)/(N \mathbf{L}'_e / N)$; because $(N \mathbf{L}'_e)/\mathbf{L}'_e$ is the preimage of $1N \mathbf{L}'_e / (N \mathbf{L}'_e / N)$, we may take $(N \mathbf{L}'_e)/ \mathbf{L}'_e$ as the desired normal subquasigroup.

The only remaining thing is to check that the epimorphism is nontrivial:

- If it was an isomorphism, the image would be a presentation of Q with a smaller group - a contradiction.
- If the image was trivial, we would have $N \mathbf{L}'_e = \mathbf{L}'$. But then, according to 1.3.3, $\mathbf{L}' / \mathbf{L}'_e = (N \mathbf{L}'_e)/ \mathbf{L}'_e \simeq N/(N \cap \mathbf{L}'_e)$ and we would again obtain a smaller presentation.

Put $\mathbf{S} := \mathrm{Soc}(\mathbf{L}')$ (we choose the socle, because it has quite some pleasant properties - see A.1.13). It is a characteristic group (thus normal and ϕ-invariant), write $\mathbf{S} = S_1 \times \ldots \times S_k$, with S_i being a minimal normal subgroup of $\mathbf{L}'$. From the above paragraph, the only case when $\mathbf{S} \mathbf{L}'_e$ is not a normal subquasigroup is for $\mathbf{S} = \mathbf{L}'$.

Consider the case $\mathbf{S} = \mathbf{L}'$. The abelian components of the socle form the center $Z(\mathbf{S}) = Z(\mathbf{L}')$ (this is a consequence of A.1.13). If $Z(\mathbf{L}') = \mathbf{L}'$, then Q is medial. If $Z(\mathbf{L}')$ is nontrivial, we can thus take $(Z(\mathbf{L}') \mathbf{L}'_e)/ \mathbf{L}'_e$ as the normal subquasigroup.

To summarize it:

Proposition 2.3.3 *If Q is simple, then $\mathbf{L}' = \mathrm{Soc}(\mathbf{L}')$ is a product of non-abelian simple groups.*

Remark. If $\mathrm{Soc}(\mathbf{L}')$ is abelian and Q is non-RD, then $N := \mathrm{Soc}(\mathbf{L}') < \mathbf{L}'$ (else Q would be medial) and we can take the normal subquasigroup in the form $(N \mathbf{L}'_e)/ \mathbf{L}'_e$.

2.3.2 Properties of $\mathbf{L}'$ in non-RD non-isogroup

Assume that in Q we have a normal subquasigroup Q_0 which contains e. Denote its size p. Then we have a system of them $\{Q_0, \ldots Q_{q-1}\}$ for some $q \in \mathbb{N}$, with all Q_i being isomorphic (cf. the discussion before 1.1.4).

There is no LD quasigroup on 2 elements, so $p \geq 3,\ q \geq 3$.

Now, we will use the normal subquasigroup Q_0 to obtain information about the structure of $\mathbf{L}$ and $\mathbf{L}'$. If there is a congruence $\sim$ on Q, we have the corresponding epimorphism $Q \to Q_\sim$ (sending x to $[x]$), thus we can produce the epimorphism Ψ

$$\begin{aligned} \Psi : \mathbf{L}(Q) &\to \mathbf{L}(Q_\sim) \\ \alpha &\mapsto ([\alpha] : [q] \mapsto [\alpha(q)]), \\ \text{in particular: } \lambda_x &\mapsto \lambda_{[x]}. \end{aligned}$$

This is correctly defined (see [12, Chapter 2.2]) even between the whole multiplication groups (groups generated by all left and right translations of Q, respectively $Q_\sim$) however we will only use it between $\mathbf{L}(Q)$ and $\mathbf{L}(Q_\sim)$ (as $\mathbf{L}(Q)$ maps on $\mathbf{L}(Q_\sim)$, since the generators of $\mathbf{L}(Q)$ maps on the generators of $\mathbf{L}(Q_\sim)$). We will denote the kernel of Ψ as K. $\Psi \restriction_{\mathbf{L}'}$ is an epimorphism of $\mathbf{L}(Q)'$ on $\mathbf{L}(Q_\sim)'$, its kernel being $K \cap \mathbf{L}'$. In particular, if $Q_\sim$ is an isogroup, then $\mathbf{L}'_e \leq K \cap \mathbf{L}'$ (if $\alpha \in \mathbf{L}'$ fixes e, then it fixes $[e]$, so $\Psi(\alpha) \in \mathbf{L}'(Q_\sim)_{[e]}$; but if $Q_\sim$ is an isogroup, then $\mathbf{L}'(Q_\sim)_{[e]}$ is trivial).

Observe also, that if $Q_\sim$ is an isogroup, then $K \cap \mathbf{L}'$ is always nontrivial (as we still assume that Q is not an isogroup, so $\{1_{\mathbf{L}'(Q)}\} < \mathbf{L}'(Q)_e \leq K \cap \mathbf{L}'$).

Also - if $Q_\sim$ is an isogroup and $Q_0 \simeq N\,\mathbf{L}'_e \,/\, \mathbf{L}'_e$ for N some normal ϕ-subgroup (this means $Q_\sim \simeq (\mathbf{L}'/N)/1$), then $K \cap \mathbf{L}' = N\,\mathbf{L}'_e$: First, if $\alpha \in K \cap \mathbf{L}'$, then $\Psi(\alpha) = [id]$ in $\mathbf{L}'(Q_\sim)$. From that, $\alpha \in N\,\mathbf{L}'_e$ (recall the argument of 1.3.4). Second, if $\alpha \in N\,\mathbf{L}'_e$, write $\alpha = \lambda_q \lambda_e^{-1} \beta$ for some $q \in Q_0, \beta \in \mathbf{L}'_e$ (observe that we can choose a complete set of coset representatives of $\mathbf{L}' \,/\, \mathbf{L}'_e$ in the form $\{\lambda_q \lambda_e^{-1}\,\mathbf{L}'_e;\ q \in Q\}$). Then

$$\Psi(\alpha) = \Psi(\lambda_q)\Psi(\lambda_e^{-1})\Psi(\beta) = \lambda_{[q]}\lambda_{[e]}^{-1}\ id = \lambda_{[e]}\lambda_{[e]}^{-1} = id,$$

which means that $\alpha \in K \cap \mathbf{L}'$.

As we are mainly interested in the small quasigroups, we make the following additional assumptions:

(Min) Every proper subquasigroup of Q is minimal.

(Min') $Q_\sim$ is an isogroup.

(Sol) $K \cap \mathbf{L}'$ is solvable. (When we use this condition, we always assume that $K \cap \mathbf{L}' = N\,\mathbf{L}'_e$, where N was taken to be $\mathrm{Soc}(\mathbf{L}')$ as in the remark after 2.3.3 - then, in particular, N is solvable as it is a subgroup of a solvable group $K \cap \mathbf{L}'$; thus N is a direct product of elementary abelian groups.)

This has following consequences:

- p is a prime power - this is from (Min), since we know from 1.4.7, that minimal LD quasigroups are isotopic to additive groups of finite fields.
- The intersection of any two distinct subquasigroups is either empty or has one element - from (Min), as any nonempty intersection of subquasigroups is again a subquasigroup.
- $\mathbf{L}'_e \leq K \cap \mathbf{L}'$ - from (Min'), this has been already justified above.
- Two normal subquasigroups $P,\ P'$ of different orders give rise to the direct product of quasigroups $Q \simeq P \times P'$ (in particular, Q is not a non-RD non-isogroup because the product of two minimal - thus medial - quasigroups is again medial) - from (Min): the congruences induced by P and P' are distinct, their intersection is just Δ and the congruence generated by them is ∇ (else the congruence containing both the smaller congruences would yield a non-minimal normal subquasigroup).

Consider any mapping u in $\mathbf{L}'_e$ (actually the following holds for any element in $K \cap \mathbf{L}_e$; also, the argument is the same for any other element of Q instead of e). $u \restriction_{Q_0}$ is a mapping from $\mathrm{Aut}(Q_0)$. Put $u_i := u \restriction_{Q_i}$. Since $\mathbf{L}'_e \leq K \cap \mathbf{L}'$, we have $u = u_0 \circ \ldots \circ u_{q-1}$ and u_i are disjoint permutations (so they commute with each other). From (Min), every u_i fixes either 0, 1 or p points (as $u_i \in \mathrm{Aut}(Q_i)$, so the set of its fixed points is a subquasigroup in Q_i), u_0 either 1 or p points (as we assumed that $e \in Q_0$ and $u_0(e) = e$). Observe that also from (Min) are all cycles in u of the same length (for mappings v in $(K \cap \mathbf{L}') \setminus \bigcup_i (\mathbf{L}'_{(Q_i)})$ we have at least that cycles in every v_i have the same length dividing p).

If u_0 fixes 1 point, then every u_i fixes 1 point (because of (Min) and because p and $p-1$ are always coprime - so if some u_i fixes no points, than u^p still fixes the 1 point in Q_0 , but also the whole Q_i, contradicting (Min)). Denote this type of mappins *cross mappings* (i.e. any automorphisms in $K \cap \mathbf{L}'$ fixing 1 point in every Q_i) . Similarly from (Min), if u_0 fixes p points, then all other u_i fix 0 points - denote these as *standard mappings* (i.e. let those be the mappings of $K \cap \mathbf{L}'$ fixing whole Q_i for some i).

Standard mappings. Every set of standard mappings (for some Q_i being fixed; united with identity) is a normal subgroup in $K \cap \mathbf{L}'$ - they

form the kernel of the group homomorphism (for $i \in \{0 \dots q-1\}$, as this applies to any Q_i)

$$\begin{aligned} \sigma_i : K \cap \mathbf{L}' &\to \mathrm{Aut}(Q_i) \\ u &\mapsto u_i. \end{aligned}$$

Observe also that the subgroup of $\mathbf{L}'_e$ consisting of standard mapping and the identity (i.e. $\ker(\sigma_0)$) is isomorphic to its image under σ_1 (because the maps in the kernel fix both Q_0 and Q_1 - this is just the identity, from (Min)). In particular, if p is prime, then $\ker(\sigma_0) \simeq \mathbb{Z}_p$. For $p = 4$, $\ker(\sigma_0)$ is isomorphic to either $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$ (and if (Sol) holds and there are only standard mappings, then $\mathbb{Z}_4$ is also impossible - $\mathrm{im}(\sigma_0) \simeq (K \cap \mathbf{L}')/\ker(\sigma_0) = N\,\mathbf{L}'_e\,/\,\mathbf{L}'_e \simeq N/(N \cap \mathbf{L}'_e) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ [as N is a product of elementary abelian groups and $|N\,\mathbf{L}'_e\,/\,\mathbf{L}'_e\,| = |Q_0| = p$], but if $\ker(\sigma_0) \simeq \mathbb{Z}_4$, then $\mathrm{im}(\sigma_0)$ also contains a 4-cycle - coming from a standard mapping lying in $\ker(\sigma_i)$, $i \neq 0$ [Since $\ker(\sigma_0) \simeq \ker(\sigma_i)$, but also $\ker(\sigma_i) \simeq \sigma_0(\ker(\sigma_i))$]. This contradicts $\mathrm{im}(\sigma_0) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$).

For $p = r^2$ (r prime), $\ker(\sigma_0)$ is isomorphic to either $\mathbb{Z}_r$, $\mathbb{Z}_r \times \mathbb{Z}_r$ or $\mathbb{Z}_{r^2}$ This is easily seen: given that $\ker(\sigma_0)$ is isomorphic to its image under σ_1, it contains only elements of order r or r^2 and it has no fixed points on Q_1 (from (Min)).

If $\mathbf{L}'_e$ contains only standard mappings and (Sol) holds, we have $(K \cap \mathbf{L}')/\,\mathbf{L}'_e \simeq N/(N \cap \mathbf{L}'_e)$ is a direct product of elementary abelian groups, $|(K \cap \mathbf{L}')/\,\mathbf{L}'_e\,| = |(K \cap \mathbf{L}')/\ker(\sigma_0)| = p$. Then we easily come to the conclusions (taking into consideration that both N and $\ker(\sigma_0) = \mathbf{L}'_e$ are normal in $K \cap \mathbf{L}'$ and we know them).

For instance, if there are only standard mappings and (Sol) holds and p is prime, then $\mathbf{L}'_e \simeq \mathbb{Z}_p$. Then either $N \cap \mathbf{L}'_e \simeq \{id\}$ or $N \geq \mathbf{L}'_e$ - in both cases $K \cap \mathbf{L}' = N\,\mathbf{L}'_e \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

If there are only standard mappings, (Sol) holds and $p = r^2$ for some prime r, then there is also the possibility (in addition to the two of the preceding paragraph), that $N \cap \mathbf{L}'_e \simeq \mathbb{Z}_r$. If $|\,\mathbf{L}'_e\,| = r$, then $(K \cap \mathbf{L}') = N \simeq (\mathbb{Z}_r)^3 \simeq (N/(N \cap \mathbf{L}'_e) \times \mathbf{L}'_e$. Now assume $|\,\mathbf{L}'_e\,| = r^2$. The mappings in $N \cap \mathbf{L}'_e$ lie in the center Z of $K \cap \mathbf{L}'$. We claim $K \cap \mathbf{L}'$ is commutative. For that, observe that Z is a normal ϕ-subgroup in $\mathbf{L}'$ (because it is characteristic in the normal ϕ-subgroup $K \cap \mathbf{L}'$). If $Z\,\mathbf{L}'_e < N\,\mathbf{L}'_e = K \cap \mathbf{L}'$, then either Z is contained in $\mathbf{L}'_e$ (contradicting the minimality of presentation) or $(Z\,\mathbf{L}'_e)/\,\mathbf{L}'_e$ is a nontrivial subquasigroup of Q contained in $(N\,\mathbf{L}'_e)/\,\mathbf{L}'_e$ (contradicting (Min)). Thus $Z\,\mathbf{L}'_e = K \cap \mathbf{L}'$ and since $\mathbf{L}'_e$ is commutative, $K \cap \mathbf{L}'$ is already commutative. In this case, we may again write $K \cap \mathbf{L}' \simeq$

$(N/(N \cap \mathbf{L}'_e)) \times \mathbf{L}'_e$.

Cross mappings. The subgroup of $\mathbf{L}'_e$ consisting of cross mappings and the identity is isomorphic to its image under σ_0 - the same argument holds as for the standard mappings.

Concerning the cross mappings, recall the discussion before 1.2.1 - elements in $\mathbf{L}_e$ commute with λ_e. If u is cross, then u_0 commutes with $\lambda_e \restriction Q_0$ and λ_e must contain cycles exchanging all other fixed points of u (so that $\lambda_e u \lambda_e^{-1} = u$).

If there are cross mappings in $K \cap \mathbf{L}'$ and p is prime consider $(K \cap \mathbf{L}')\,\mathbf{L}'_e \,/\, \ker(\sigma_0)$ - this will likely lead to a 2-transitive group and these are known (see the discussion in [4, cor. 3.5B]).

2.3.3 Application to orders 9, 12, 15

Now let us again turn our attention to the sizes 9, 12 and 15. Observe that - from 1.1.5 - for the order 9, only the subquasigroups of order 3 are admissible; for order 12 only those of order 3 or 4; for order 15 only those of order 3 and 5 (those of order 4 are not possible because of 1.5.3). Observe also that in a non-RD quasigroup, a nontrivial subquasigroup always exists (as minimal quasigroups are medial).

We have to do the following:

1. Produce a *normal* subquasigroup in Q.
2. Show (Min), (Min') and (using these two) also (Sol).
3. We eliminate the possibility of cross mappings occuring in $\mathbf{L}'_e$.
4. With this, we already have enough information on admissible $K \cap \mathbf{L}'$, for Q a non-RD non-isogroup (in particular, for $p = 3, 4, 5$, we know, by the preceding discussion, that $K \cap \mathbf{L}' = N\,\mathbf{L}'_e$ is abelian and only few groups are admissible). This description is satisfiable only for some values of $p,\ q$ (i.e. only for certain configurations of the normal quasigroups and the factor quasigroup), so we investigate those. The possible pairs (p, q) are (3,3), (3,4), (4,3), (3,5), (5,3). Except for (3,3) (for which there are only 2 non-abelian groups of order $27 = |K \cap \mathbf{L}'| \cdot |\,\mathbf{L}'_e(Q_\sim)|$), the order of $K \cap \mathbf{L}'$ and $\mathbf{L}'_e(Q_\sim)$ are coprime, so actually $\mathbf{L}'_e(Q) \simeq (K \cap \mathbf{L}') \rtimes \mathbf{L}'_e(Q_\sim)$ (from the Schur-Zassenhaus theorem - see A.1.8). We will show in Section 3.1 that (5,3) indeed works, while we show below that other pairs do not.

So we start:

1. For $|Q| = 9$, take any subquasigroup. It is normal because of 1.1.5.

   For any prime dividing the order of $\mathbf{L}$ we have an element of that order in $\mathbf{L}$ from Sylow theorems. For $|Q| = 12$, we may thus rule out any prime apart from 2, 3 and 11 (as concerns the other primes less than 12 - that is 5 and 7 - the fixed points of automorphisms of respective orders would form subquasigroups of wrong orders - i.e. others than 1, 3, 4 or 12). If there is a subquasigroup of order 4, then it is normal and we are done. If not, then $\mathbf{L}_e$ is divisible only by powers of 3 and 11 (an element of order two would have 4 fixed points), and so its Sylow 2-subgroup is trivial. But the order of $\lambda_e \in \mathbf{L}_e$ is divisible by 2, because there must be a 3 element subquasigroup containing e (if there is no subquasigroup having 4 elements) and thus λ_e must contain a 2-cycle (i.e. $\lambda_e \restriction_{Q_0}$). Thus order of $\mathbf{L}_e$ should be divisible by 2 as well, a contradiction.

   Observe we have actually shown that there is always a (necessarily normal) 4 element subquasigroup - i.e. the case (3,4) is already contained in the case (4,3).

   For $|Q| = 15$, if there is a subquasigroup of order 5, it is normal. So if Q is simple, it has only a non-normal subquasigroup of order 3. Then also the conclusion of Proposition 2.3.3 holds. We have $\mathbf{L}' = H_1 \times \ldots \times H_k$ (with H_i being nonabelian simple groups).

   As in the case of $|Q| = 12$, we find that $\mathbf{L}'$ has order divisible at most by 2, 3, 5 and 7.

   Consider the action of $\mathbf{L}$ on Q. We know, from 1.2.1, that it is transitive and faithful. Assume there is a non-trivial system of blocks. Every block would form a subquasigroup (by 2.3.2); as there are no subquasigroups of order 5, there must be 5 blocks of order 3. Now the action of $\mathbf{L}$ on the blocks provides a homomorphism h of $\mathbf{L}$ in S_5. $\ker(h) \cap \mathbf{L}' = \{1\}$, because no element of order 5 or 7 lies in the kernel - as every H_i contains either an element of order 5 or one of order 7 (else it would be divisible only by 2 and 3 and no such simple nonabelian groups exist by A.1.11) and $\ker(h) \cap H_i$ is normal in H_i; thus if one element of H_i does not lie in the kernel, none does. Therefore $h \restriction_{\mathbf{L}'}$ is an imbedding of $\mathbf{L}'$ in S_5 and, from size considerations, $\mathbf{L}' \simeq A_5$. Now this is impossible, by 1.3.1 (since $\mathrm{Aut}(A_5) \simeq S_5$ and $T \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \leq A_5 = G$).

   So the action of $\mathbf{L}$ would have to be primitive (on 15 elements). Groups with such action are known (and scarce - $\mathbf{L}' \simeq A_6$, S_6,

A_7, A_8, A_{15} or S_{15}) (see [4, the tables after p.305] or the GAP [8] library of primitive groups). We may argue for a contradiction with 1.2.1 - indeed, none of those groups have a conjugacy class with 15 elements.

2. (Min) holds for every quasigroup of order $< 27 = 3 * 9$ (from 1.1.5 and note that the first non-minimal quasigroup is on 9 elements).

   (Min') holds for every quasigroup of order $< 27 = 3 * 9$ (we know that for orders < 9 the quasigroups are minimal. Next, the respective normal subquasigroup - giving rise to the congruence - must have order at least 3. Note that this bound will be extendible to 45, once we are done with ruling out non-RD non-isogroups on 9 and 12 elements).

   (Soc): We use what we know, under the conditions (Min) and (Min'). We have the description of automorphisms in $K \cap \mathbf{L}'$ - those are the mappings of $(K \cap \mathbf{L}') \setminus \bigcup_i (\mathbf{L}'_{(Q_i)})$, the standard elements and the cross elements (the latter ones pertaining to some $\mathbf{L}'_{(Q_i)},\ i = 0 \dots q-1$). All of these have order dividing either p or $p-1$. So in particular, for $p = 3, 4, 5$, there are at most 2 primes dividing $|K \cap \mathbf{L}'|$, so $K \cap \mathbf{L}'$ is solvable by the Burnside's p, q theorem A.1.11.

3. For pairs (3,3), (3,5), the fixed points of any cross mapping would form a different normal (see 1.1.5) subquasigroup, thus Q would be a direct product of minimal quasigroups, so not non-RD.

   For (4,3), if there is a cross mapping u, then λ_e is of type 3-2-6 (indeed, $\lambda_e \restriction_{Q_0} = \lambda_e^{Q_0}$ - which we know from B.1; λ_e must contain a transposition exchanging the two fixed point of u, not lying in Q_0; now the 6-cycle is the only possibility for the rest, otherwise some power of λ_e would fix a non-admissible number of elements). But then, it is easy to compute the centralizer of λ_e (using GAP) in S_{12}. In particular, $C_{\mathbf{L}}(\lambda_e) = \mathbf{L}_e$ (the equality was discussed before 1.3.2) is commutative (this can be already seen from the fact,that λ_e consists of four cycles of different lengths). If there are also standard mappings in $\mathbf{L}'_e$, then they do not commute with the cross ones - indeed, $\sigma_1(\mathbf{L}'_e)$ would be all A_4 - a contradiction. So, there are no standard mappings. Then $K \cap \mathbf{L}' = N\,\mathbf{L}'_e \simeq \sigma_0(N\,\mathbf{L}'_e) \simeq A_4$ (there is at least one 3-cycle coming from a cross mapping and one 2-2 permutation coming from N - these generate all A_4).

   Now $|\,\mathbf{L}'_e\,| = |K \cap \mathbf{L}'\,| \cdot |\,\mathbf{L}'(Q_\sim)| = 12 \cdot 3 = 36$. There are just two

non-abelian groups on 36 elements having $\mathbb{Z}_2 \times \mathbb{Z}_2$ as a component of the socle (GAP computation). Both have $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_3$ as different characteristic subgroups - the normal subquasigroups corresponding to them (i.e. $N\,\mathbf{L}'_e\,/\,\mathbf{L}'_e \simeq N/(\mathbf{L}'_e \cap N)$) have different orders (and both are nontrivial, else it would contradict minimality of presentation), the corresponding congruences are different and Q is a direct product of medial quasigroups - a contradiction.

For (5,3), if there is a cross mapping, then the projection $\sigma_0(K \cap \mathbf{L}')$ is already A_5 (because, apart from the image of the cross mapping, there is also a 5-cycle, coming as an image of a mapping in N) - a contradiction, as a 3-cycle in A_5 would fix a 2-element subquasigroup lying under Q_0.

4. What remains to be done? To rule out $K \cap \mathbf{L}'$ with just standard mappings for $(p, q) =$ (3,3), (4,3), (3,5) (for (5,3) we know $K \cap \mathbf{L}' \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$, so $\mathbf{L}'$ is already uniquely identified, as there is only one non-abelian group on 75 elements).

   Now we have enough information about how would the group structure of $\mathbf{L}'$ look like, that we may rule them out by a direct calculation (to that end, we used GAP [8]).

   We may rule out (3,5), as there is no (noncommutative) semidirect product $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_5$, because such a semidirect product requires a nontrivial homomorphism of $\mathbb{Z}_5$ in $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$; $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$ has $(9-3)*(9-1) = 48$ elements, so such homomorphism does not exist.

   For (3,3), there are two non-abelian groups on 27 elements. We look for the respective left multiplication groups of Q, for which they would form a commutator subgroup - the left multiplication group must have 54 elements (because $\Psi^{-1}(1_{\mathbf{L}(Q_\sim)}) = K \cap \mathbf{L}' \leq \mathbf{L}'(Q)$, so $[\mathbf{L}(Q) : \mathbf{L}'(Q)] = [\mathbf{L}(Q_\sim) : \mathbf{L}'(Q_\sim)] = [S_3 : \mathbb{Z}_3]$, since we know $\mathbf{L}(Q_\sim)$ from B.1). Only one group on 54 elements has one of the above two non-abelian groups as the commutator subgroup - however, the group has a non-trivial center - this contradicts 1.2.1.

   For (4,3), the possibilities for $\mathbf{L}'_e$, are $\mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, so $K \cap \mathbf{L}' \simeq (\mathbb{Z}_2)^3$ or $(\mathbb{Z}_2)^4$. We obtain three candidates for $\mathbf{L}'_e$, two are easy to rule out (just by looking at the characteristic subgroups - these give rise to normal subquasigroups). The other is not so easy - however, no automorphism of it satisfies 1.3.1, so we may rule out this group as well.

Remark.

- Conjecture: The case with $\mathbf{L}'_e$ containing cross mappings doesn't occur.

  Observe that the cross mappings acts on Q_i as elements of $\mathbf{L}(Q_i)$, instead of as elements of $\mathbf{L}'(Q_i)$ (as the author would expect).

- Observe, that the epimorphism ψ from the proof of 1.3.5 for $Q_0 \simeq (K \cap \mathbf{L}')/\mathbf{L}'_e$ is exactly σ_0.

Chapter 3

Other results

3.1 Galkin's representation of two non-M LD quasigroups of order 15

In this section, we develop the Galkin's representation of two non-M LD quasigroups of order 15. As follows from our classification, no smaller LD non-medial quasigroups exist. This was first observed in [13, p.29], with evidence provided by the model builder SEM.

At 2.3 we found out, how big must $\mathbf{L}'$ be and that it is isomorphic to $(\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes \mathbb{Z}_3$. As it turns out, there are just three groups on 75 elements, only one of them being non-abelian, this being our G. We know that $\mathbf{L}'_e$ must be a cyclic subgroup of order 5.

We consider G with the presentation $\langle a, b, c | a^3 = b^5 = c^5 = 1,\ bc = cb,\ aba^{-1} = b^3c^3,\ aca^{-1} = b^4c \rangle$. We put $T := < c >$ (apparently, the choice of the five element subgroup is irrelevant - up to isomorphism).

Using the GAP computational system, we found out that $|\operatorname{Aut}(G)| = 1200$ and there are 20 conjugacy classes. Out of these there are 25 automorphisms having T as the subgroup of its fixed points, every of those lie in one of certain two conjugacy classes. We choose two arbitrary automorphisms $\phi_S,\ \phi_N$ of those 25, each in different conjugacy class and we construct $(G/T, \phi_S),\ (G/T, \phi_N)$. According to 2.2.4, these will be the only non-isomorphic quasigroups with this G (as already noted before, the choice of T was irrelevant).

We have chosen

$$\begin{aligned} \phi_N : G &\to G \\ a &\mapsto a^2c^3 \\ b &\mapsto b^4c^3 \\ c &\mapsto c \end{aligned} \qquad\qquad \begin{aligned} \phi_S : G &\to G \\ a &\mapsto a^2b^3c \\ b &\mapsto b^4c^3 \\ c &\mapsto c. \end{aligned}$$

Write any element of G/T as $a^ib^jT,\ i \in \{1,2,3\},\ j \in \{1 \dots 5\}$. Then we have (after a tedious computation using the definition of quasigroup operation from Section 1.3):

$$a^ib^jT \circ_N a^{i'}b^{j'}T = \begin{cases} a^ib^{2j+4j'}T & \text{if } (i-i') \equiv_3 0 \\ a^{i+1}b^2b^{4(j+j')}T & \text{if } (i-i') \equiv_3 -1 \\ a^{i-1}b^{4(j+j')}T & \text{if } (i-i') \equiv_3 1 \end{cases}$$

and

$$a^ib^jT \circ_S a^{i'}b^{j'}T = \begin{cases} a^ib^{2j+4j'}T & \text{if } (i-i') \equiv_3 0 \\ a^{i+1}bb^{4(j+j')}T & \text{if } (i-i') \equiv_3 -1 \\ a^{i-1}b^3b^{4(j+j')}T & \text{if } (i-i') \equiv_3 1 \end{cases}$$

Remark.

- Note that $(G/T, \circ_S)$ is left-symmetric, while $(G/T, \circ_N)$ is not (in particular, the two are not isomorphic).
- The left multiplication group of the constructed quasigroups is just the semidirect product of $\mathbf{L}' \rtimes \mathbb{Z}_2$. The right multiplication group is huge, having 24000 elements.

Conclusion

There undoubtedly exist many ways how to improve on the results achieved in this thesis.

Assume that we want to classify left distributive non-right distributive quasigroups somewhat further. The case of isogroups is a topic on its own - indeed, in view of 1.3.1, this boils down to the following group theoretical problem: *Given a finite group G, describe all conjugacy classes of automorphisms of G which fix just 1_G (if there are any).* The author would be very interested in knowing, whether a general description for some special classes of groups exists.

When we come to non-isogroups, it was possible to impose some other (perhaps less restrictive) conditions on the quasigroup Q than were the conditions (Min), (Min'), (Sol) from 2.3.2. One may also try to impose some condition on order - as is done in some cases when classifying groups. For instance, what about classifying p-quasigroups for some prime p?

The treatment of the simple LD quasigroups in 2.3.1 was very brief. It might be interesting to see them all classified (in such way, we would also avoid hassle with always trying to find a normal subquasigroup by some ad-hoc methods). The key to this probably lies in combining the facts, that, first - from 1.2.1 - all left translations form exactly one conjugacy class, second, we must be able to find automorphism satisfying the condition from 1.3.1.

In this work, there are just two examples (in 3.1) of left distributive groups which are not medial. A curious reader may find some more examples in [11, p.40] and [2, p.161-162]. Of course, the ultimate method how to generate examples is 1.3.1. One may try to find families of groups (and their automorphisms) satisfying it.

Yet another question: how about infinite left distributive quasigroups? We guess that there is a statement similar to 1.3.1, holding even for infinite groups. One must be probably more careful about the conditions

imposed on the distinguished automorphism ϕ. With this, we might ask if 1.3.2 holds (in the proof of which, finiteness was again used).

Appendix A

Preliminaries

For readers' convenience, we put here some results (mostly concerning the group theory), which have been used in this work. For the proofs the reader is referred to other sources.

A.1 Group theory

Definition A.1.1 *Let G be a group acting transitively on a set X. A nonempty subset $B \subset X$ is called* a block *for G, if for each $g \in G$, either $g(B) \cap B = B$ or $g(B) \cap B = \emptyset$.*

Definition A.1.2

A group G is a p-group *if $|G| = p^k$ for some prime p.*

Let G be a group with $|G| = p^k m$ for some prime p, such that $p \nmid m$. We say that $S \leq G$ is a Sylow p-subgroup *of G, if $|S| = p^k$.*

Theorem A.1.3 *If G is a nontrivial p-group, then it has a nontrivial center.*

Proof. [1, (5.16)] □

Theorem A.1.4 *Let G be a finite group, p a prime.*

1. *The set of Sylow p-subgroups of G is nonempty.*
2. *Any two Sylow p-subgroups of G are conjugated in G.*
3. *Every p-subgroup of G is contained in some Sylow p-subgroup of G.*
4. *Let P be a Sylow p-subgroup of G. Then $P \lhd G$ if and only if P is the unique Sylow p-subgroup of G.*

Proof. [1, Chapter 6] □

Theorem A.1.5 *A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.*

Proof. [1, (9.11)] □

Definition A.1.6

- *A* Frobenius group *is a transitive permutation group on a finite set, such that no element of $G\backslash\{id\}$ fixes more than one point and some element of $G\backslash\{id\}$ has a fixed point.*
- *A* Frobenius kernel *of a Frobenius group G is the subset of G consisting of elements fixing no point together with 1_G.*

Theorem A.1.7 (Frobenius' theorem) *Let G be a Frobenius group acting on a finite set X, K its Frobenius kernel, G_x the stabilizer of a point $x \in X$. Then K is a normal subgroup of G and $G \simeq K \rtimes G_x$.*

Proof. [1, (35.24) and (35.25)] □

Theorem A.1.8 (Schur-Zassenhaus theorem) *Let G be a finite group with a normal subgroup H. Assume that*

1. *$|H|$ and $|G/H|$ are coprime.*
2. *Either H or G/H is solvable.*

Then $G \simeq H \rtimes (G/H)$.

Proof. [1, (18.1)] □

Definition A.1.9 *Let G be a group, H its subgroup. A* complement *to H in G is a subgroup $K \leq G$, such that $KH = G$ and $K \cap H = \{1\}$.*

Theorem A.1.10 *Let G be a finite group. If p is the smallest prime divisor of the order of G and G has cyclic Sylow p-groups, then a Sylow p-group has a normal complement in G.*

Proof. [1, (39.2)] □

Theorem A.1.11 *Let G be a finite group, $|G| = p^a q^b$ for p, q prime. Then G is solvable.*

Proof. [1, (35.13)] □

Definition A.1.12 *Let G be a nontrivial group.*

- *A* minimal normal subgroup *of G is a nontrivial subgroup of G which does not properly contain any other nontrivial normal subgroup of G.*
- *The* socle *of G is the subgroup generated by the set of all minimal normal subgroups of G.*

Remark.

- For a finite group, the socle is nontrivial (observe that G itself may be its minimal normal subgroup).
- Apart from its useful properties, the socle plays an important role in the theory of finite permutation groups [4, particularly Chapter 4].

Proposition A.1.13 (Basic properties of the socle) *Let G be a nontrivial finite group.*

1. *If K is a minimal normal subgroup of G and L is any normal subgroup of G, then either $K \leq L$ or $KL \simeq K \times L$.*
2. *There exist minimal normal subgroups $K_1, \ldots, K_m$ (the* components *of the socle) of G, such that $\mathrm{Soc}(G) \simeq K_1 \times \ldots \times K_m$.*
3. *Every minimal normal subgroup K of G is a direct product $T_1 \times \ldots \times T_k$, where the T_i are simple normal subgroups of K which are conjugate under G.*
4. *If the subgroups K_i in (ii) are nonabelian, then $K_1, \ldots, K_m$ are the only minimal normal subgroups of G. If the T_i in (iii) are nonabelian, then these are the only minimal normal subgroups of K.*
5. *Every minimal normal subgroup of G is either an elementary abelian p-group for some prime p (i.e. a direct product of $\mathbb{Z}_p$), or its center is equal to $\{1\}$.*

Proof. [4, Theorem 4.3B] □

A.2 Some more quasigroup theory

Definition A.2.1 *Let $(Q, \odot), (P, *)$ be quasigroups.*

- *A* homotopy *from Q to P is a triple (α, β, γ) of maps from Q to P such that*
$$\alpha(x) * \beta(y) = \gamma(x \odot y), \qquad \forall x, y \in Q.$$
- *An* isotopy *is a homotopy, such that α, β and γ are all bijections.*

For basic properties, see [5, p.7].

Proposition A.2.2 *Let $(Q, \cdot)$ be a quasigroup such that $\cdot$ is associative. Then $(Q, \cdot)$ is already a group.*

Proof. [5, p.9, Lemma 2.20] □

Appendix B

Results of some computations

B.1 List of small left multiplication groups

Here we provide left multiplication groups of a few small quasigroups. (Recall that the derived subgroup is isomorphic to the respective isotopic group - i.e. the group G in the presentation (G, α) - as these are all isogroups).

These were computed by letting the model finder Mace [10] build the (non-isomorphic) quasigroups on 3, 4 and 5 elements, identifying them using the classification and extracting the left translations from respective Cayley tables (it would be of course possible to compute the translations directly). The left multiplication group is then just the one generated by them (the GAP package proves useful).

quasigroup	left multiplication group
$(\mathbb{Z}_3,\ (x \mapsto 2x))$	S_3
$(\mathbb{Z}_2 \times \mathbb{Z}_2,\ (x \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x))$	A_4
$(\mathbb{Z}_5,\ (x \mapsto 2x))$	D_{10}
$(\mathbb{Z}_5,\ (x \mapsto 3x))$	$(a,\ b\ \|a^4 = 1, b^5 = 1, aba = b^2)$
$(\mathbb{Z}_5,\ (x \mapsto 4x))$	$(a,\ b\ \|a^4 = 1, b^5 = 1, aba = b^2)$

Table B.1: List of left multiplication groups for small LD quasigroups

Bibliography

[1] M. Aschbacher. *Finite group theory.* Cambridge University Press, Cambridge, 1986.

[2] V. D. Belousov. *Osnovy teorii kvazigrupp i lup.* Nauka, Moscow, 1967.

[3] S. Burris and H. P. Sankappanavar. *A Course in Universal Algebra.* Springer-Verlag, New York, 1981.

[4] J. D. Dixon and B. Mortimer. *Permutation Groups.* Springer-Verlag, New York, 1996.

[5] A. Frisová. *Quasigroup based cryptography.* Master's thesis, Charles University, Prague, 2009.

[6] V. M. Galkin. O konecnyx distributivnyx kvazigruppax. *Matematicheskie issledovaniya*, 24(1):39–41, 1978.

[7] V. M. Galkin. Levodistributivnie kvazigruppy konecnogo poradka. *Matematicheskie Zametki*, 51:43–54, 1979.

[8] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.
`http://www.gap-system.org`.

[9] S. Lang. *Algebra.* Springer-Verlag, New York, 2002.

[10] W. McCune. *Mace4 Reference Manual and Guide.* Mathematics and Computer Science Division, Argonne National Laboratory, 2003.
`http://www.cs.unm.edu/~mccune/prover9/`.

[11] J. D. H. Smith. Finite distributive quasigroups. *Mathematical Proceedings of Cambridge Philosophical Society*, 80:37–41, 1976.

[12] J. D. H. Smith. *An Introduction to Quasigroups and Their Representations*. Chapman & Hall/CRC, Taylor & Francis Group, Boca Raton, 2007.

[13] D. Stanovský. *Left distributive left quasigroups*. PhD thesis, Charles University, Prague, 2004.

[14] K. Toyoda. On axioms of linear functions. *Proceedings of the Imperial Academy*, 17(7):221–227, 1941.
Available at `projecteuclid.org/euclid.pja/1195578751`.