On right conjugacy closed loops and right conjugacy closed loop folders

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades einer Doktorin der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Dipl.-Math. Katharina Artic, geb. Suchantke

aus Leipzig, Deutschland

Berichter: Universitätsprofessor Dr. Gerhard Hiß
Universitätsprofessor Dr. Alice Niemeyer

Tag der mündlichen Prüfung: 16.02.2017

Diese Dissertation ist auf den Internetseiten der Universitätsbibliothek online verfügbar.

Acknowledgement

At this point I would like to express my gratitude to the following people who have helped me while I prepared this thesis.

Foremost I am deeply indebted to my supervisor Prof. Dr. Gerhard Hiß for proposing the research questions and his continued guidance, advice and encouragement. He contributed substantially to the successful completion of this thesis with enthusiasm for the topic and constructive feedback. I always delighted in the numerous talks and inspiring mathematical discussions as well as our productive exchange. My sincere thanks also goes to him for his meticulous reading of my thesis and his valuable advice on the mathematical exposition. Additionally, I am grateful for his instructions and support during my teaching activities at RWTH Aachen.

Furthermore I thank Prof. Dr. Alice Niemeyer for giving me a second opinion and the always excellent collaboration during my employment.

Thanks are also due to Dr. Thomas Breuer for his exceedingly valuable council in connection with the computer algebra system GAP. By his comprehensive expertise and assistance I was able to design my computations more effectively and to push the limit of what was feasible.

My colleagues at Lehrstuhl D für Mathematik at RWTH Aachen have provided a wonderful working environment; I am particularly grateful to Dr. Frank Lübeck, Dr. Natalie Naehrig, Dr. Sebastian Thomas, Dr. Markus Kirschmer, Sabina Pannek, Moritz Schröer, Désirée Burkel and Helene Goblet for the constructive collaboration, the inspiring discussions on almost every topic and all their enriching advice. It has been a pleasure to work with you.

Moreover I thank the Cusanuswerk for the financial und idealistic support. In particular, I thank Dr. Manuel Ganser and Liane Neubert for their friendly and expert advice as well es their always dependably assistance.

However, I also, of course, owe very special thanks to my husband Christian for his patience and his everlasting lovingly assistance in all situations. Further I thank our daughter Amalia: You are my sunshine!

Katharina Artic
Aachen, January 2017

Contents

Introduction

Quasigroups and loops have been considered as research objects first in the course of geometric examinations. Loops have been studied intensely since the beginning of the last century. A quasigroup is a set $\mathcal{L}$ together with a multiplication $* : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ whose multiplication table is a latin square. This means that every element occurs exactly once in each row and column of the multiplication table. A loop is a quasigroup which contains an identity element.

Loops allow us to study structures with a possibly non-associative multiplication. Such structures occur frequently in algebraic applications. For example, projective planes cannot in general be coordinatized over a field or even a skew-field but over an algebraic structure called ternary ring. Such a ternary ring in turn gives rise to two different loops, see for example the notes of Peter Müller and Gábor P. Nagy in [MN].

Those loops in which the multiplication is associative are called groups and play a fundamental role in characterising symmetries in nature and science. They are important in physics and crystallography where they are used to determine symmetries of objects as well as to deduce further properties of these objects from the knowledge of their symmetries. Also in mathematics groups play an important role; thus group theory is an essential and highly active research area in modern algebra. In 1981 the classification of the finite simple groups was completed. Since all finite groups are built up from finite simple groups, many new results in finite group theory have been proven using this classification.

Loops also arise in the study of groups since the natural multiplication on transversals of subgroups of a group forms a loop. In [Bae39] and [Bae40] Reinhold Baer considered this relationship between loops and groups in his examinations on nets. This connection has been rephrased in terms of category theory by Michael Aschbacher in [Asc05]. In particular, he introduced the terms loop folders and envelopes of loops. Here the envelope of a loop is, among all loop folders associated to a fixed loop — in a certain sense — the smallest one. Hence it is possible to resort to group theory in order to answer

questions in loop theory. For exact definitions and background theory we refer at this point to Chapter 1.

In addition to the examination of general loops also loops with special properties have been research objects. For example, Edgar G. Goodaire and Daniel A. Robinson introduced in [GR82] the term of a conjugcy closed loop (CC loop). They proved that for almost every integer n there is a non-associative CC loop of order n. Further, CC loops play a crucial role in [Drá01] in the proof of Aleš Drápals theorem, that the groups $\mathrm{PSL}(2,q)$ and ${}^2B_2(q)$ are not multiplication groups of non-associative loops. In [Drá08] Aleš Drápal determines the isomorphism type (generators and relations) of the multiplication group of a CC loop of order p_1p_2 where p_1 and p_2 are distinct primes with $p_1 \mid (p_2 - 1)$. A generalization of CC loops are left conjugacy closed loops respectively right conjugacy closed loops (LCC loops respectively RCC loops). Again, Aleš Drápal shows in [Drá04] that the LCC loops of prime order are cyclic groups. This result is proven with loop theoretic methods. An analogous result holds for RCC loops.

This thesis considers RCC loops. As observed by Reinhold Baer groups can be used to describe loops via loop folders. A loop folder consists of a group, a subgroup and a transversal for the subgroup and the loop can be recovered from this data. For the examination of RCC loops in this thesis we will employ group theoretic methods, i.e. questions on RCC loops will be answered by examining RCC loop folders. Since — contrary to loop theory — group theory is a well established area in algebra, we have been able to answer open questions on RCC loops by this method.

The aim of this thesis is to establish basic results on RCC loop folders. For example, we show that although for an arbitrary non-associative loop of order n the right multiplication group of the loop might be the symmetic or alternating group on n letters this is not true for RCC loops. Their right multiplication groups are smaller. Further, we design an algorithm to compute envelopes of non-associative RCC loops and show how to construct non-isomorphic, non-associative RCC loops systematically from these envelopes of RCC loops. Moreover, we show that there is no RCC loop folder with the group $\mathrm{PSL}(2,q)$. In particular, the right multiplication group of an RCC loop is not a subgroup or a factor group of the group $\mathrm{PSL}(2,q)$. Analogously to Aleš Drápal examinations of LCC loops of prime order and of CC loops of order p_1p_2 where p_1 and p_2 are distinct primes we examine RCC loops of these orders. But we examine such RCC loops with group theoretic methods. By this strategy new results on the structure of the right multiplication group of such RCC loops have been obtained.

This thesis is divided into four chapters. In Chapter 1 we give the definitions

of loops and loop folders and show basic properties of these objects. Further, we explain the relationship between loops and loop folders. In Chapter 2 we define and examine RCC loops and RCC loop folders. Since the finite simple groups are so important in finite group theory we examine here i.a. the relationship between RCC loop folders and finite simple groups. Moreover, we give a group theoretic proof of Aleš Drápal theorem that an RCC loop of prime order is a cyclic group. In Chapter 3 we present an algorithm to compute RCC loops by computing their envelopes. With this algorithm all non-associative RCC loops of order up to 30 are computed. A database with these RCC loops has been complied and is now available in the open source computer algebra system GAP, via the package LOOPS by Gábor P. Nagy and Petr Vojtěchovsky. For more information about GAP see [Gap] and for more information about the package LOOPS see [NV15]. In Chapter 4 we examine the RCC loops of order p_1p_2 where p_1 and p_2 are distinct primes. We show that the right multiplication group of such an RCC loop is an imprimitive group. Moreover, in the case $p_1 = 2$ and p_2 an arbitrary prime we give an infinite series of right multiplication groups of non-associative RCC loops of order $2p_2$.

Chapter 1

Loops and loop folders

This chapter provides an introduction to the concepts of loops, envelopes of loops and loop folders. In the first section loops, loop homomorphisms, multiplication groups of loops and the envelope of a loop are defined and some properties of these objects are derived. The second section considers loop folders and their properties. In the third section we emphasize the relationship between loops and loop folders. Because loop folders are group theoretic objects, it is possible to prove loop theoretic propositions with known group theoretic statements.
The definitions and theorems are adopted from [Asc05] and [Pfl90]. Further, [KÖ7] considers multiplication groups of quasigroups in his diploma thesis, where he also gives a concise account of loops, their multiplication groups and loop folders.

1.1 Loops and their envelopes

(1.1) Definition (Quasigroup and loop)
A non-empty, finite[1] set $\mathcal{Q}$ with a binary operation $* : \mathcal{Q} \times \mathcal{Q} \to \mathcal{Q}$ is called a *quasigroup*, if for any fixed $\ell, \tilde{\ell} \in \mathcal{Q}$ the equations

$$x * \ell = \tilde{\ell} \quad \text{and} \quad \ell * y = \tilde{\ell}$$

have unique solutions $x, y \in \mathcal{Q}$. This amounts to saying that the multiplication table of $\mathcal{Q}$ is a Latin square.
A quasigroup $\mathcal{L}$ is called a *loop*, if there is an identity element of $\mathcal{L}$, i.e. there is an element $1_{\mathcal{L}} \in \mathcal{L}$ with

$$\ell * 1_{\mathcal{L}} = \ell = 1_{\mathcal{L}} * \ell \quad \text{for all } \ell \in \mathcal{L}.$$

In this case, the *left*, respectively the *right*, *inverse* of an element $\ell \in \mathcal{L}$ is the uniquely determined element x, respectively y, in $\mathcal{L}$ with

$$x * \ell = 1_{\mathcal{L}} \quad \text{respectively} \quad \ell * y = 1_{\mathcal{L}}.$$

[1] In this thesis all quasigroups, loops and groups are finite.

Notice that although every element in a loop has a left and a right inverse, generally they are not equal. If the loop is associative, equality holds and the loop is a group.

(1.2) Example
Let $\mathcal{L} := \{1, \ldots, 5\}$ and $* : \mathcal{L} \to \mathcal{L}$ with

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	5	1	2	4
4	4	1	5	3	2
5	5	4	2	1	3

Then $(\mathcal{L}, *)$ is a loop with identity element $1_{\mathcal{L}} = 1$. We have

$$4 * 2 = 1 = 2 * 5,$$

so the left and right inverse of 2 are not equal. Further we have

$$(2 * 2) * 3 = 1 \quad \text{and} \quad 2 * (2 * 3) = 5.$$

It is an easy computation to show that all loops of order less than five are associative. Hence $\mathcal{L}$ is one of the smallest examples of a non-associative loop.

(1.3) Definition (Isomorphims of loops)
A *loop homomorphism* φ between loops $(\mathcal{L}, *)$ and $(\mathcal{K}, \circ)$ is a map $\varphi : \mathcal{L} \to \mathcal{K}$ that satisfies

$$(x * y)\varphi = (x\varphi) \circ (y\varphi) \quad \text{for all } x, y \in \mathcal{L}.$$

A *loop isomorphism* is a bijective loop homomorphism.

(1.4) Lemma ([Pfl90, Sec. (I.7)])
Let $(\mathcal{L}, *)$ and $(\mathcal{K}, \circ)$ be two loops and $\varphi : \mathcal{L} \to \mathcal{K}$ a loop homomorphism. Then we have: $(1_{\mathcal{L}})\varphi = 1_{\mathcal{K}}$.

Proof. Note that $(1_{\mathcal{L}})\varphi \circ (1_{\mathcal{L}})\varphi = (1_{\mathcal{L}} * 1_{\mathcal{L}})\varphi = (1_{\mathcal{L}})\varphi$ and $(1_{\mathcal{L}})\varphi \circ 1_{\mathcal{K}} = (1_{\mathcal{L}})\varphi$. Since the equation $(1_{\mathcal{L}})\varphi \circ y = (1_{\mathcal{L}})\varphi$ has a unique solution in $\mathcal{K}$ we have $(1_{\mathcal{L}})\varphi = 1_{\mathcal{K}}$. □

(1.5) Example
Let $\mathcal{K} := \{1, \ldots, 5\}$ and $\circ : \mathcal{K} \to \mathcal{K}$ with

$\circ$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	2	1	4
4	4	3	5	2	1
5	5	4	1	3	2

$(\mathcal{K}, \circ)$ is a loop isomorphic to the loop $(\mathcal{L}, *)$ of Example (1.2). Identifying the sets $\mathcal{L}$ and $\mathcal{K}$, a loop isomorphism is given by the permutation $\varphi = (2\ 3)(4\ 5)$.

(1.6) Definition (Multiplication groups)
Let $\mathcal{L}$ be a loop and $x \in \mathcal{L}$. We define R_x to be the right multiplication by x and L_x to be the left multiplication by x as follows:

$$\mathrm{R}_x : \ \mathcal{L} \to \mathcal{L}, \ell \mapsto \ell * x, \qquad \mathrm{L}_x : \ \mathcal{L} \to \mathcal{L}, \ell \mapsto x * \ell.$$

Set $\mathrm{R}_\mathcal{L} := \{\mathrm{R}_x \mid x \in \mathcal{L}\}$ and $\mathrm{L}_\mathcal{L} := \{\mathrm{L}_x \mid x \in \mathcal{L}\}$. Then $\mathrm{R}_\mathcal{L}$ and $\mathrm{L}_\mathcal{L}$ are subsets of the symmetric group $\mathrm{Sym}(\mathcal{L})$. We define the *right multiplication group* $\mathrm{RM}(\mathcal{L})$, the *left multiplication group* $\mathrm{LM}(\mathcal{L})$ and the *multiplication group* $\mathrm{M}(\mathcal{L})$ of $\mathcal{L}$ as subgroups of $\mathrm{Sym}(\mathcal{L})$ by:

$$\mathrm{RM}(\mathcal{L}) := \langle \mathrm{R}_\mathcal{L} \rangle, \quad \mathrm{LM}(\mathcal{L}) := \langle \mathrm{L}_\mathcal{L} \rangle, \quad \mathrm{M}(\mathcal{L}) := \langle \mathrm{R}_\mathcal{L}, \mathrm{L}_\mathcal{L} \rangle.$$

Notice that for a group G (which is also a loop) we have $\mathrm{RM}(G) \cong G$.

Let $\mathcal{L}$ be a loop and $x, y \in \mathcal{L}$ be two arbitrary elements of $\mathcal{L}$. Let ℓ be the uniquely determined element with $x * \ell = y$. Then we have $x\mathrm{R}_\ell = y$. Hence the right multiplication group $\mathrm{RM}(\mathcal{L})$ acts transitively on $\mathcal{L}$.

(1.7) Example
In Example (1.2) we have: $\mathrm{RM}(\mathcal{L}) = \mathrm{LM}(\mathcal{L}) = \mathrm{M}(\mathcal{L}) \cong \mathrm{Sym}(5)$.

(1.8) Lemma ([Pfl90, Th. (III.2.7)])
The (left/right) multiplication groups of isomorphic loops are isomorphic.

Proof. Let $(\mathcal{L}, *)$ and $(\mathcal{K}, \circ)$ be two isomorphic loops and $\varphi : \mathcal{L} \to \mathcal{K}$ a loop isomorphism. Then we have for all $x, y \in \mathcal{K}$:

$$x \circ y = (x\varphi^{-1} * y\varphi^{-1})\varphi.$$

Therefore we have for arbitrary fixed $y \in \mathcal{K}$ and for all $x \in \mathcal{K}$:

$$\begin{aligned} x\mathrm{R}_y &= x \circ y \\ &= (x\varphi^{-1} * y\varphi^{-1})\varphi \\ &= ((x\varphi^{-1})\mathrm{R}_{y\varphi^{-1}})\varphi \\ &= x(\varphi^{-1}\mathrm{R}_{y\varphi^{-1}}\varphi). \end{aligned}$$

Hence $\mathrm{R}_y = \varphi^{-1}\mathrm{R}_{y\varphi^{-1}}\varphi \in \mathrm{Sym}(\mathcal{K})$ for all $y \in \mathcal{K}$. Since φ is bijective we have $\mathrm{R}_{\mathcal{K}} = \varphi^{-1}\mathrm{R}_{\mathcal{L}}\varphi$.
For $g \in \mathrm{RM}(\mathcal{L})$ set $g\Phi := \varphi^{-1}g\varphi$. Write

$$g = \mathrm{R}_{\ell_1}\mathrm{R}_{\ell_2}\ldots\mathrm{R}_{\ell_n}, \quad \ell_i \in \mathcal{L}, i \in \{1,\ldots,n\}.$$

Then

$$\varphi^{-1}g\varphi = \underbrace{\varphi^{-1}\mathrm{R}_{\ell_1}\varphi}_{\in \mathrm{R}_{\mathcal{K}}}\underbrace{\varphi^{-1}\mathrm{R}_{\ell_2}\varphi}_{\in \mathrm{R}_{\mathcal{K}}}\ldots\underbrace{\varphi^{-1}\mathrm{R}_{\ell_n}\varphi}_{\in \mathrm{R}_{\mathcal{K}}} \in \mathrm{RM}(\mathcal{K}).$$

So Φ is a map between $\mathrm{RM}(\mathcal{L})$ and $\mathrm{RM}(\mathcal{K})$. Clearly Φ is a group homomorphism and Φ is bijective. Hence the right multiplication groups of $\mathcal{L}$ and $\mathcal{K}$ are isomorphic.
Analogously, we have $\mathrm{L}_x = \varphi^{-1}\mathrm{L}_{x\varphi^{-1}}\varphi$ for all $x \in \mathcal{K}$ and so the left multiplication groups of $\mathcal{L}$ and $\mathcal{K}$ are isomorphic. Finally the multiplication groups are isomorphic. □

(1.9) Definition (Envelope of a loop)
Let $\mathcal{L}$ be a loop with identity element $1_{\mathcal{L}}$. We define the *envelope* $\mathcal{L}\varepsilon$ of $\mathcal{L}$ as the triple $(\mathrm{RM}(\mathcal{L}), \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}}), \mathrm{R}_{\mathcal{L}})$.

Note that in this definition the first entry, $\mathrm{RM}(\mathcal{L})$, is generated by the last entry, $\mathrm{R}_{\mathcal{L}}$, of this triple. However, later we will give a more general definition of a loop folder as a triple where this property no longer holds.

(1.10) Lemma ([Asc05, Example (1.2)])
Let $\mathcal{L}$ be a loop and consider the envelope $\mathcal{L}\varepsilon$ of $\mathcal{L}$. Set

$$G := \mathrm{RM}(\mathcal{L}), \quad H := \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}}) \quad \textit{and} \quad T := \mathrm{R}_{\mathcal{L}},$$

i.e. $\mathcal{L}\varepsilon = (G, H, T)$. Then T is a right transversal for every H^g, $g \in G$.

Proof. For an arbitrary element $g \in G$ let $\mathrm{R}_x, \mathrm{R}_y \in T$ for some $x, y \in \mathcal{L}$ be such that R_x, R_y lie in the same right coset of H^g in G, i.e.

$$\mathrm{R}_x\mathrm{R}_y^{-1} = g^{-1}hg \text{ for some } h \in H.$$

Set $\ell := (1_{\mathcal{L}})g$. Then $\ell g^{-1}hg = \ell$ and so $\ell\mathrm{R}_x\mathrm{R}_y^{-1} = \ell$. Hence we have $\ell * x = \ell * y$ in $\mathcal{L}$. Because of the uniqueness of a solution of an equation in $\mathcal{L}$

we have $x = y$ and so $R_x = R_y$. Thus T contains for every $g \in G$ at most one element of every right coset of H^g in G.
Since H is the stabilizer of $1_{\mathcal{L}}$ in $\mathrm{RM}(\mathcal{L})$ the length of the orbit $\mathrm{orb}(1_{\mathcal{L}})$ of $1_{\mathcal{L}}$ is equal to the index of H in G. Further, since G acts transitively on $\mathcal{L}$, we have $|\mathrm{orb}(1_{\mathcal{L}})| = |T|$. Hence $[G : H^g] = [G : H] = |T|$ and T contains for every $g \in G$ exactly one element of every right coset of H^g in G. □

1.2 Loop folders

In this section we define loop folders as a generalization of envelopes of loops. We also consider isomorphisms of loop folders and define faithful loop folders. The envelope of a loop is a faithful loop folder and this is one of two necessary properties to characterize a loop folder to be the envelope of a loop.

(1.11) Definition (Loop folder)
A triple (G, H, T) is called *loop folder*, if G is a finite group with identity element 1_G, H is a subgroup of G and T is a transversal for the right cosets of every H^g, $g \in G$, with $1_G \in T$.
We call the loop folder *trivial* if $|H| = 1$ or $|T| = 1$.

(1.12) Corollary
The envelope $\mathcal{L}\varepsilon$ of a loop $\mathcal{L}$ is a loop folder.

(1.13) Example
Let (G, H, T) be with $G = \mathrm{Sym}(5)$, $H = \mathrm{Stab}_G(1) \cong \mathrm{Sym}(4)$ and

$$T = \{(), (1\ 2\ 3\ 5\ 4), (1\ 3)(2\ 4\ 5), (1\ 4\ 3\ 2\ 5), (1\ 5\ 3\ 4\ 2)\}.$$

Then (G, H, T) is the envelope of the loop of Example (1.2).

(1.14) Definition (Homomorphisms of loop folders)
A *loop folder homomorphism* Φ between two loop folders (G_1, H_1, T_1) and (G_2, H_2, T_2) is a group homomorphism $\Phi : G_1 \to G_2$ that satisfies

$$H_1\Phi \leq H_2 \quad \text{and} \quad T_1\Phi \subseteq T_2.$$

The loop folder homomorphism Φ is called surjective, if $G_1\Phi = G_2$ and $T_1\Phi = T_2$. Further, if the group homomorphism Φ is bijective, the loop folder homomorphism Φ is called a *loop folder isomorphism*.

(1.15) Remark
Let Φ be a loop folder isomorphism between two loop folders (G_1, H_1, T_1) and (G_2, H_2, T_2). Then we have $|H_1| \leq |H_2|$ and $|T_1| \leq |T_2|$. Since $|G_1| = |G_2|$ and $|H_1| \cdot |T_1| = |G_1|$ as well as $|G_2| = |H_2| \cdot |T_2|$, we have $H_1\Phi = H_2$ and $T_1\Phi = T_2$.

(1.16) Lemma ([Asc05, (1.3)])
Let $\mathcal{L}$ and $\mathcal{K}$ be two isomorphic loops and $\varphi : \mathcal{L} \to \mathcal{K}$ a loop isomorphism. Let $(G, H, T) := \mathcal{L}\varepsilon$ be the envelope of $\mathcal{L}$. Then we have $\varphi^{-1}G\varphi \leq \mathrm{Sym}(\mathcal{K})$ and

$$(\varphi^{-1}G\varphi, \varphi^{-1}H\varphi, \varphi^{-1}T\varphi) = \mathcal{K}\varepsilon.$$

Proof. In the proof of (1.8) we have already shown that

$$\Phi : G \to \mathrm{RM}(\mathcal{K}), g \mapsto \varphi^{-1}g\varphi$$

is a group isomorphism with $T\Phi = \mathrm{R}_{\mathcal{K}}$. So it remains to show that

$$H\Phi = \mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}}).$$

Let $h \in H$, i.e $(1_{\mathcal{L}})h = 1_{\mathcal{L}}$. Because φ is a loop homomorphism, we have $(1_{\mathcal{L}})\varphi = 1_{\mathcal{K}}$ and

$$1_{\mathcal{K}}(h\Phi) = 1_{\mathcal{K}}(\varphi^{-1}h\varphi) = 1_{\mathcal{L}}(h\varphi) = (1_{\mathcal{L}})\varphi = 1_{\mathcal{K}}.$$

Hence we have $h\Phi \in \mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}})$ for all $h \in H$. Since Φ is a bijective map, we have

$$|H| = |H\Phi| \leq |\mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}})| = |\mathrm{RM}(\mathcal{K})|/|\mathrm{R}_{\mathcal{K}}| = |G|/|T| = |H|$$

and thus $H\Phi = \mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}})$. □

(1.17) Definition (Faithful loop folder)
Let (G, H, T) be a loop folder. The group G acts via right multiplication on the right cosets $\{Ht \mid t \in T\}$ of H. This action is transitive. The loop folder is called faithful if the induced homomorphism $\varphi : G \to \mathrm{Sym}(\{Ht \mid t \in T\})$ is injective.

Recall that the core of a subgroup H of a group G is defined as the intersection of all conjugates of H, i.e.

$$\mathrm{Core}_G(H) = \bigcap_{g \in G} H^g.$$

(1.18) Lemma ([Asc05, Remark (1.1)])
The loop folder (G, H, T) is faithful if and only if $\mathrm{Core}_G(H) = \{1_G\}$.

Proof. By definition (G, H, T) is faithful if and only if $Htx = Ht$ for all $t \in T$ implies $x = 1_G$. This is true if and only if

$$\bigcap_{t \in T} t^{-1}Ht = \{1_G\}.$$

Since for every $g \in G$ there exist $h \in H$ and $t \in T$ with $g = ht$ this is equivalent to $\{1_G\} = \bigcap_{g \in G} H^g = \mathrm{Core}_G(H)$. □

(1.19) Lemma ([Asc05, Ex. (1.2)])
The envelope of a loop is a faithful loop folder.

Proof. Let $\mathcal{L}$ be a loop and (G, H, T) be its envelope. The statement is trivial for $\mathcal{L} = \{1_\mathcal{L}\}$.
So suppose $|\mathcal{L}| > 1$. By Lemma (1.18) we have to show that $\bigcap_{g\in G} H^g = \{1_G\}$. Let $g \neq 1_G$ be an arbitrary element of G. Then there is $x \in \mathcal{L}$ with $xg \neq x$. Furthermore there is $\tilde{g} \in G$ with $(1_\mathcal{L})\tilde{g} = x$, as G acts transitively on $\mathcal{L}$. So

$$1_\mathcal{L}(\tilde{g}g\tilde{g}^{-1}) = x(g\tilde{g}^{-1}) \neq x\tilde{g}^{-1} = 1_\mathcal{L}$$

and hence $\tilde{g}g\tilde{g}^{-1} \notin H$. So $g \notin \tilde{g}^{-1}H\tilde{g}$ and since $\mathrm{Core}_G(H) \leq \tilde{g}^{-1}H\tilde{g}$ we have $g \notin \mathrm{Core}_G(H)$. □

1.3 The relationship between loops and loop folders

The class of all loop folders together with all loop folder homomorphisms forms a category **LF** as does the class of all loops together with all loop homomorphisms, named **Lp**. In this section we define a functor λ from **LF** to **Lp** and show that $(\mathcal{L}\varepsilon)\lambda \cong \mathcal{L}$ for all loops $\mathcal{L}$.
The map ε is not a functor from **Lp** to **LF** as we will see in an example. Consider the wide subcategory $\mathbf{Lp}_s$ of **Lp** with all loops as objects and all surjective loop homomorphisms as morphisms. We will show that ε is a functor from $\mathbf{Lp}_s$ to **LF**.
Generally $((G, H, T)\lambda)\varepsilon$ is not isomorphic to the loop folder (G, H, T) as we will see in an example. Further, we show how to construct the envelope of $(G, H, T)\lambda$ from (G, H, T) and characterize the loop folders which are envelopes of a loop to be exactly the faithful loop folders (G, H, T) with $G = \langle T\rangle$. The class of these loop folders together with the surjective loop folder homomorphisms form a category **EL**. The functors ε and λ provide an equivalence between the categories $\mathbf{LP}_s$ and **EL**. Hence for all faithful loop folders (G, H, T) with $G = \langle T\rangle$ we have $((G, H, T)\lambda)\varepsilon \cong (G, H, T)$.

(1.20) Lemma ([Asc05, Ex. (1.4)])
Let (G, H, T) be a loop folder. Define a multiplication $*$ on T by $t_1 * t_2 = t_3$ where t_3 is the uniquely determined element in $Ht_1t_2 \cap T$. Define a map λ by $(G, H, T)\lambda = (T, *)$. Then $(G, H, T)\lambda$ is a loop.

Proof. Since T is a transversal for the right cosets of H there is exactly one element t_3 with $Ht_3 = Ht_1t_2$ for given $t_1, t_2 \in T$. Thus the multiplication $*$ is a binary operation.
For any fixed $t_2, t_3 \in T$ consider the equation $x * t_2 = t_3$ and suppose this equation has two solutions in T, say t_1 and t_1'. Then $Ht_1t_2 = Ht_1't_2$ and hence $Ht_1 = Ht_1'$. Since T is a transversal for the right cosets of H we have $t_1 = t_1'$.
Now consider for any fixed $t_1, t_3 \in T$ the equation $t_1 * x = t_3$. Suppose this equation has two solutions in T, say t_2 and t_2'. Then $Ht_1t_2 = Ht_1t_2'$ and so

$(H^{t_1})t_2 = (H^{t_1})t_2'$. Because T is also a transversal for the right cosets of H^{t_1} and $t_2, t_2' \in T$ we have $t_2 = t_2'$.
Finally 1_G is the identity element of the loop because $1_G * t = t = t * 1_G$ for all $t \in T$. □

(1.21) Lemma ([Asc05, (1.5)])
Define the map λ from the category **LF** *to the category* **Lp** *for a loop folder (G, H, T) by $(G, H, T)\lambda = (T, *)$ as in Lemma (1.20) and by $\Phi\lambda = \Phi|_T$ for a loop folder homomorphism Φ. Then λ is a functor.*

Proof. Let (G_1, H_1, T_1) and (G_2, H_2, T_2) be two loop folders and

$$\Phi : (G_1, H_1, T_1) \to (G_2, H_2, T_2)$$

a loop folder homomorphism. Then we have $H_1\Phi \leq H_2$ and $T_1\Phi \subseteq T_2$. Consider the loops $(T_1, *) := (G_1, H_1, T_1)\lambda$ and $(T_2, \circ) := (G_2, H_2, T_2)\lambda$ and set $\varphi := \Phi\lambda = \Phi|_{T_1}$.
First we show that φ is a loop homomorphism between $(T_1, *)$ and $(T_2, \circ)$:
Let $x, y \in T_1$. Then $x * y$ is the uniquely determined element t_1 in $H_1xy \cap T_1$. Set $t_2 := t_1\varphi = t_1\Phi \in T_2$. We have $(H_1xy)\Phi \subseteq H_2(x\Phi)(y\Phi)$ and so

$$t_2 \in H_2(x\Phi)(y\Phi) \cap T_2.$$

We have $(x\varphi) \circ (y\varphi) = (x\Phi) \circ (y\Phi)$ and since $(x\Phi) \circ (y\Phi)$ is the uniquely determined element in $H_2(x\Phi)(y\Phi) \cap T_2 = \{t_2\}$ we have

$$(x * y)\varphi = t_1\varphi = t_2 = (x\varphi) \circ (y\varphi)$$

and φ is a loop homomorphism.
Further for loop folders (G_1, H_1, T_1), (G_2, H_2, T_2), (G_3, H_3, T_3) and loop folder homomorphisms

$$\Phi : (G_1, H_1, T_1) \to (G_2, H_2, T_2), \quad \Psi : (G_2, H_2, T_2) \to (G_3, H_3, T_3)$$

and the composition $\square$ of maps we have to show first that

$$(Id_{G_1})\lambda = (Id_{T_1})$$

and second that

$$(\Phi \square \Psi)\lambda = (\Phi \square \Psi)|_{T_1} = \Phi|_{T_1} \square \Psi|_{T_2} = \Phi\lambda \square \Psi\lambda.$$

But the first equation is trivial and the second holds since $(T_1)\Phi \subseteq T_2$. Thus λ is a functor. □

(1.22) Theorem ([Asc05, (1.7)])
Let $\mathcal{L}$ be a loop. Then $(\mathcal{L}\varepsilon)\lambda \cong \mathcal{L}$.

Proof. Consider $(\mathcal{L}, *)$ and $(\mathrm{R}_{\mathcal{L}}, \circ) = (\mathcal{L}\varepsilon)\lambda$ as loops. Then the map

$$\varphi : \mathcal{L} \to (\mathcal{L}\varepsilon)\lambda,\ x \mapsto \mathrm{R}_x$$

is a loop homomorphism:
Let $x, y \in \mathcal{L}$. Then

$$1_{\mathcal{L}}(\mathrm{R}_x\mathrm{R}_y) = (1_{\mathcal{L}}\mathrm{R}_x)\mathrm{R}_y = (1_{\mathcal{L}} * x) * y = x * y = 1_{\mathcal{L}} * (x * y) = 1_{\mathcal{L}}\mathrm{R}_{x*y}.$$

Hence we have $(\mathrm{R}_x\mathrm{R}_y)\mathrm{R}_{x*y}^{-1} \in \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}})$ and thus

$$\mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}})\mathrm{R}_x\mathrm{R}_y = \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}})\mathrm{R}_{x*y}.$$

Therefore we have $\mathrm{R}_x \circ \mathrm{R}_y = \mathrm{R}_{x*y}$ and it follows that $(x * y)\varphi = x\varphi \circ y\varphi$. The multiplication table of $\mathcal{L}$ is a Latin square, so φ is bijective and thus a loop isomorphism. □

(1.23) Lemma
[Asc05, (1.3)] Define the map ε from the category $\mathbf{Lp}_s$ to the category $\mathbf{LF}$ by

$$\mathcal{L}\varepsilon = (\mathrm{RM}(\mathcal{L}), \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}}), \mathrm{R}_{\mathcal{L}})$$

as in Definition(1.9) and for a surjective loop homomorphism $\varphi : \mathcal{L} \to \mathcal{K}$ by

$$\varphi\varepsilon := (\Phi : \mathcal{L}\varepsilon \to \mathcal{K}\varepsilon, \mathrm{R}_{x_1} \dots \mathrm{R}_{x_n} \mapsto \mathrm{R}_{x_1\varphi} \dots \mathrm{R}_{x_m\varphi}).$$

Then ε is a functor.

Proof. We first show that Φ is well defined:
Let $x_1, \dots, x_m, y_1, \dots, y_r \in \mathcal{L}$ such that $\mathrm{R}_{x_1} \dots \mathrm{R}_{x_m} = \mathrm{R}_{y_1} \dots \mathrm{R}_{y_r}$ in $\mathrm{RM}(\mathcal{L})$. Then we have for all $\ell \in \mathcal{L}$:

$$(\dots((\ell * x_1) * x_2)\dots) * x_m = (\dots((\ell * y_1) * y_2)\dots) * y_r.$$

It follows that

$$((\dots((\ell * x_1) * x_2)\dots) * x_m)\varphi = ((\dots((\ell * y_1) * y_2)\dots) * y_r)\varphi.$$

Since φ is a loop homomorphism we have

$$(\dots((\ell\varphi \circ x_1\varphi) \circ x_2\varphi)\dots) \circ x_m\varphi = (\dots((\ell\varphi \circ y_1\varphi) \circ y_2\varphi)\dots) \circ y_r\varphi.$$

Since φ is surjective this implies

$$(\dots((k \circ x_1\varphi) \circ x_2\varphi)\dots) \circ x_m\varphi = (\dots((k \circ y_1\varphi) \circ y_2\varphi)\dots) \circ y_r\varphi$$

for all $k \in \mathcal{K}$. Hence we get

$$\mathrm{R}_{x_1\varphi} \dots \mathrm{R}_{x_m\varphi} = \mathrm{R}_{y_1\varphi} \dots \mathrm{R}_{y_r\varphi}$$

and so Φ is well defined.
Clearly Φ is a group homomorphism and $\mathrm{R}_{\mathcal{L}}\Phi \subseteq \mathrm{R}_{\mathcal{K}}$.
We have to show that $(\mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}}))\Phi \subseteq \mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}})$. Since φ is a loop homomorphism, we have $1_{\mathcal{K}} = (1_{\mathcal{L}})\varphi$. Let $\mathrm{R}_{x_1} \dots \mathrm{R}_{x_m} \in \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}})$. Then we have

$$\begin{aligned}
1_{\mathcal{K}} &= (1_{\mathcal{L}})\varphi \\
&= ((1_{\mathcal{L}})\mathrm{R}_{x_1} \dots \mathrm{R}_{x_m})\varphi \\
&= ((\dots((1_{\mathcal{L}} * x_1) * x_2)\dots) * x_m)\varphi \\
&= (\dots(((1_{\mathcal{L}})\varphi \circ x_1\varphi) \circ x_2\varphi)\dots) \circ x_m\varphi \\
&= (\dots((1_{\mathcal{K}} \circ x_1\varphi) \circ x_2\varphi)\dots) \circ x_m\varphi \\
&= (1_{\mathcal{K}})\mathrm{R}_{x_1\varphi} \dots \mathrm{R}_{x_m\varphi}.
\end{aligned}$$

Thus we have $(\mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}}))\Phi \subseteq \mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}})$ and Φ is a loop folder homomorphism.
Clearly we have $(Id_{\mathcal{L}})\varepsilon = Id_{\mathcal{L}\varepsilon}$. Let $\varphi : \mathcal{L} \to \mathcal{K}$ and $\psi : \mathcal{K} \to \mathcal{M}$ be two surjective loop homomorphism and $\Phi = \varphi\varepsilon$ resp. $\Psi = \psi\varepsilon$. Then we have

$$\begin{aligned}
&(\mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}}))\Phi \subseteq \mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}}) \quad \text{respectively} \\
&(\mathrm{Stab}_{\mathrm{RM}(\mathcal{K})}(1_{\mathcal{K}}))\Psi \subseteq \mathrm{Stab}_{\mathrm{RM}(\mathcal{M})}(1_{\mathcal{M}})
\end{aligned}$$

and

$$(\mathrm{R}_{\mathcal{L}})\Phi \subseteq \mathrm{R}_{\mathcal{K}} \quad \text{respectively} \quad (\mathrm{R}_{\mathcal{K}})\Psi \subseteq \mathrm{R}_{\mathcal{M}}.$$

Hence we clearly have for the composition $\square$ of two maps

$$\varphi\varepsilon \,\square\, \psi\varepsilon = \Phi \,\square\, \Psi = (\varphi \,\square\, \psi)\varepsilon. \qquad \square$$

The previous lemma shows that ε is a functor from the category $\mathbf{Lp}_s$ to the category **LF**. As we mentioned in the introduction of this section ε is not a functor from the category **Lp** to the category **LF**. The next example demonstrates this.

(1.24) Example
Let $\mathcal{L}$ be the loop of Example (1.2) and $(\mathcal{L}', \circ)$ be the cyclic group with two elements (which is also a loop). We set $\mathcal{L}' = \{a, b\}$ where a denotes the identity element of $\mathcal{L}'$. Since the right multiplication group of a group is isomorphic to this group we have $\mathrm{RM}(\mathcal{L}') \cong \mathcal{L}'$. As a set we have $\mathrm{RM}(\mathcal{L}') = \{\mathrm{R}_a, \mathrm{R}_b\}$. By Example (1.7) we have $\mathrm{RM}(\mathcal{L}) \cong \mathrm{Sym}(5)$. We identify $\mathrm{RM}(\mathcal{L})$ and $\mathrm{Sym}(5)$.
The map

$$\varphi : \mathcal{L}' \to \mathcal{L},\ a \mapsto 1,\ b \mapsto 3$$

is a loop homomorphism. Clearly φ is not surjective and hence not a morphism in $\mathbf{Lp}_s$. Consider $\Phi := \varphi\varepsilon : \mathrm{RM}(\mathcal{L}') \to \mathrm{RM}(\mathcal{L})$. We have

$$\Phi : \quad \mathrm{R}_a \mapsto \mathrm{R}_1 = (), \quad \mathrm{R}_b \mapsto \mathrm{R}_3 = (1\ 3)(2\ 4\ 5).$$

Further the equation $R_bR_b = R_a$ holds in $RM(\mathcal{L}')$. But

$$(R_bR_b)\Phi = (1\ 3)(2\ 4\ 5)(1\ 3)(2\ 4\ 5) = (2\ 5\ 4) \neq () = (R_a)\Phi.$$

Hence Φ is not a group homomorphism and ε is not a functor from the category **Lp** to the category **LF**.

Let (G_1, H_1, T_1) and (G_2, H_2, T_2) be two loop folders. Note that in general $(G_1, H_1, T_1)\lambda \cong (G_2, H_2, T_2)\lambda$ does not imply $(G_1, H_1, T_1) \cong (G_2, H_2, T_2)$. In particular a loop folder (G, H, T) need not be isomorphic to the envelope of $(G, H, T)\lambda$. The next example will demonstrate this. Finally, we show how to construct the envelope of $(G, H, T)\lambda$ from (G, H, T).

(1.25) Example
Let (G, H, T) be a loop folder. In general we have $(G, H, T) \ncong ((G, H, T)\lambda)\varepsilon$: Set

$$G = \langle (2\ 3)(4\ 6\ 5\ 7), (1\ 2\ 3)(5\ 7)\rangle$$
$$H = \langle (1\ 2\ 3), (5\ 7), (1\ 2)(4\ 7)(5\ 6)\rangle$$
$$T = \{t_1, t_2, t_3, t_4, t_5, t_6\}$$

with

$$t_1 = ()$$
$$t_2 = (5\ 6\ 7)$$
$$t_3 = (4\ 7\ 5)$$
$$t_4 = (1\ 2)$$
$$t_5 = (1\ 2)(5\ 6\ 7)$$
$$t_6 = (1\ 2)(4\ 7\ 5).$$

A quick computation with GAP shows that (G, H, T) is a loop folder with $|G| = 144$. Let $(T, *) := (G, H, T)\lambda$. The multiplication table of $(T, *)$ is given by:

$*$	t_1	t_2	t_3	t_4	t_5	t_6
t_1	t_1	t_2	t_3	t_4	t_5	t_6
t_2	t_2	t_6	t_4	t_5	t_3	t_1
t_3	t_3	t_4	t_5	t_6	t_1	t_2
t_4	t_4	t_5	t_6	t_1	t_2	t_3
t_5	t_5	t_3	t_1	t_2	t_6	t_4
t_6	t_6	t_1	t_2	t_3	t_4	t_5

We have $\mathrm{RM}(T) = \langle \mathrm{R}_{t_1}, \dots \mathrm{R}_{t_6} \rangle$ and a quick computation with GAP shows that $|\mathrm{RM}(T)| = 24$. Note that $((G,H,T)\lambda)\varepsilon = (\mathrm{RM}(T), \mathrm{Stab}_{\mathrm{RM}(T)}(1_G), \mathrm{R}_T)$ hence there is no group isomorphism between G and $\mathrm{RM}(T)$ and so there is no loop folder isomorphism between (G,H,T) and $((G,H,T)\lambda)\varepsilon$.

Recall the notation for the right cosets of a subgroup U in a group G:

$$U\backslash G := \{Ug \mid g \in G\}.$$

For any subset M of G we define $U\backslash M := \{Um \mid m \in M\} \subseteq U\backslash G$. Let N be a normal subgroup of G. For the factor group we use the common notation G/N.

(1.26) Theorem ([Asc05, Ex. (1.6)])
Let (G,H,T) be a loop folder and $N = \mathrm{Core}_G(H)$. Set

$$\bar{G} = G/N, \quad \bar{H} = N\backslash H, \quad \bar{T} = N\backslash T.$$

Then $(\bar{G}, \bar{H}, \bar{T})$ is a faithful loop folder with $(G,H,T)\lambda \cong (\bar{G}, \bar{H}, \bar{T})\lambda$.

Proof. Since N is a normal subgroup of G we have that $\bar{G}$ is a group and since $N \leq H$ we have that $\bar{H}$ is a subgroup of $\bar{G}$. Further, since $1_G \in T$, we have $1_{\bar{G}} \in \bar{T}$. Thus $(\bar{G}, \bar{H}, \bar{T})$ is a loop folder if $\bar{T}$ is a transversal for the right cosets of $\bar{H}^{\bar{g}} \in \bar{G}$ for every $\bar{g} \in \bar{G}$.
Fix $\bar{g} \in \bar{G}$ and choose $g \in G$ with $Ng = \bar{g}$. Consider $\bar{t}_1, \bar{t}_2 \in \bar{T}$ with $\bar{t}_1\bar{t}_2^{-1} \in \bar{H}^{\bar{g}}$. Then $Nt_1t_2^{-1} = (Nh)^g$ for some $h \in H$, hence $t_1t_2^{-1} \in (Nh)^g \subseteq H^g$. But T is a transversal for the right cosets of H^g in G and hence $t_1 = t_2$. This implies $\bar{t}_1 = \bar{t}_2$ and $\bar{T}$ contains at most one representative for each right coset of $\bar{H}^{\bar{g}}$. Assume now that $\bar{t}_1 = \bar{t}_2$. Then there is an $n \in N \leq H$ with $nt_1 = t_2$ but this implies $t_1 = t_2$. So $|\bar{T}| = |T|$ and the map $^-|_T : T \to \bar{T}$ is a bijection. We have

$$|\bar{T}| = |T| = \frac{|G|}{|H|} = \frac{|G|}{|N|} \cdot \frac{|N|}{|H|} = \frac{|\bar{G}|}{|\bar{H}|}.$$

Hence $\bar{T}$ is a transversal for the right cosets of $\bar{H}^{\bar{g}}$ in $\bar{G}$.
By Lemma (1.18) $(\bar{G}, \bar{H}, \bar{T})$ is a faithful loop folder.
The map $^-|_T : T \to \bar{T}$ is a loop homomorphism between $(T, *) := (G,H,T)\lambda$ and $(\bar{T}, \circ) := (\bar{G}, \bar{H}, \bar{T})\lambda$:
Let $t_1, t_2 \in T$. We have

$$\{\overline{t_1 * t_2}\} = \overline{Ht_1t_2} \cap \bar{T} = \bar{H}\bar{t}_1\bar{t}_2 \cap \bar{T} = \{\bar{t}_1 \circ \bar{t}_2\}.$$

Since $^-|_T : T \to \bar{T}$ is bijective it is a loop isomorphism. □

(1.27) Example
For the loop folder (G, H, T) in Example (1.25) we have

$$N := \mathrm{Core}_G(H) = \langle (1\ 2\ 3) \rangle.$$

So (G, H, T) is not faithful. Set

$$\bar{G} = G/N, \quad \bar{H} = N\backslash H, \quad \bar{T} = N\backslash T.$$

By Theorem (1.26) the loop folder $(\bar{G}, \bar{H}, \bar{T})$ is a faithful and

$$(\bar{G}, \bar{H}, \bar{T})\lambda \cong (G, H, T)\lambda \cong (T, *)$$

as in Example (1.25). A quick computation with GAP shows that $|\bar{G}| = 48$. Since we have $|\mathrm{RM}(T)| = 24$ the loop folder $(\bar{G}, \bar{H}, \bar{T})$ is not isomorphic to the envelope of $(T, *)$.

(1.28) Theorem ([Asc05, (2.3)])
Let (G, H, T) be a loop folder. Set $\widetilde{G} := \langle T \rangle$ and $\widetilde{H} := H \cap \langle T \rangle$. Then $(\widetilde{G}, \widetilde{H}, T)$ is a loop folder with $(G, H, T)\lambda \cong (\widetilde{G}, \widetilde{H}, T)\lambda$. If (G, H, T) is faithful, then $(\widetilde{G}, \widetilde{H}, T)\lambda$ is faithful, too.

Proof. Fix $\tilde{g} \in \widetilde{G} \leq G$ and consider $t_1, t_2 \in T$ with $t_1 t_2^{-1} \in \widetilde{H}^{\tilde{g}}$. Then $t_1 t_2^{-1} \in H^{\tilde{g}}$ because $\widetilde{H} \leq H$. But T is a transversal for the right cosets of $H^{\tilde{g}}$ in G and so $t_1 = t_2$.
Further we have

$$[\widetilde{G} : \widetilde{H}] = \frac{|\langle T \rangle|}{|H \cap \langle T \rangle|} = \frac{|\langle T \rangle||H\langle T \rangle|}{|\langle T \rangle||H|} = \frac{|G|}{|H|} = |T|.$$

So $(\widetilde{G}, \widetilde{H}, T)$ is a loop folder.
Set $(T, *) := (G, H, T)\lambda$ and $(T, \circ) := (\widetilde{G}, \widetilde{H}, T)\lambda$. We have:

$$\begin{aligned} t_1 * t_2 = t_3 &\Leftrightarrow Ht_1t_2 = Ht_3 \\ &\Leftrightarrow t_1t_2t_3^{-1} \in H \\ &\Leftrightarrow t_1t_2t_3^{-1} \in H \cap \langle T \rangle \\ &\Leftrightarrow t_1t_2t_3^{-1} \in \widetilde{H} \\ &\Leftrightarrow \widetilde{H}t_1t_2 = \widetilde{H}t_3 \\ &\Leftrightarrow t_1 \circ t_2 = t_3. \end{aligned}$$

□

(1.29) Example
Let (G, H, T) be as in (1.25) and $(\bar{G}, \bar{H}, \bar{T})$ as in (1.27). Set

$$\widetilde{G} := \langle \bar{T} \rangle, \quad \widetilde{H} := \bar{H} \cap \langle T \rangle, \quad \widetilde{T} := \bar{T}.$$

We have $\widetilde{G} = \langle \widetilde{T} \rangle$ and by Theorems (1.26) and (1.28) we have

$$(\widetilde{G}, \widetilde{H}, \widetilde{T})\lambda \cong (\bar{G}, \bar{H}, \bar{T})\lambda \cong (G, H, T)\lambda \cong (T, *).$$

Since $(\bar{G}, \bar{H}, \bar{T})$ is faithful, the loop folder $(\widetilde{G}, \widetilde{H}, \widetilde{T})$ is faithful, too. A quick computation with GAP shows that $|\widetilde{G}| = 24$. So $\widetilde{G}$ might be isomorphic to the right multiplication group of $(G, H, T)\lambda$.
We want to show that $(\widetilde{G}, \widetilde{H}, \widetilde{T})$ is isomorphic to the envelope of $(G, H, T)\lambda$. Set $\mathcal{L} = (G, H, T)\lambda$. We compute with GAP if there is a group isomorphism $\Phi : \widetilde{G} \to \mathrm{RM}(\mathcal{L})$ with $\widetilde{H}\Phi = \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}})$ and $\widetilde{T}\Phi = \mathrm{R}_{\mathcal{L}}$. The computation in GAP, see [Gap], looks like follows:

```
gap> LoadPackage("loops");;
gap> G:=Group([(2,3)(4,6,5,7),(1,2,3)(5,7)]);;
gap> H:=Group([(1,2,3),(5,7),(1,2)(4,7)(5,6)]);;
gap> T:=[(),(5,6,7),(4,7,5),
>         (1,2),(1,2)(5,6,7),(1,2)(4,7,5)];;
gap> L:=LoopByRightFolder(G,H,T);;
gap> RM:=RightMultiplicationGroup(L);;
gap> RMH:=Stabilizer(RM,1);;
gap> RMT:=RightSection(L);;
gap> N:=Core(G,H);;
gap> h:=NaturalHomomorphismByNormalSubgroup(G,N);;
gap> bG:=Image(h,G);;
gap> bH:=Image(h,H);;
gap> bT:=Image(h,T);;
gap> tT:=bT;;
gap> tG:=Group(tT);;
gap> tH:=Intersection(bH,tG);;
gap> ForAny(AllHomomorphisms(tG,RM),
>       psi-> Image(psi,tG)=RM and
>             Image(psi,tH)=RMH and
>             Image(psi,tT)=RMT );
true
```

Hence the loop folder $(\widetilde{G}, \widetilde{H}, \widetilde{T})$ is isomorphic to the envelope of $(G, H, T)\lambda$.

Let (G, H, T) be a loop folder and $\mathcal{L} = (G, H, T)\lambda$. The previous two theorems showed that the image $\mathcal{L}$ under λ is invariant under passing from G to the factor group by $\mathrm{Core}_G(H)$ and under restricting G to $\langle T \rangle$. The following theorem combines these two processes and shows how to construct the envelope of $(G, H, T)\lambda$ for an arbitrary loop folder (G, H, T). But first we prove a technical lemma which we will use in the proof of this theorem.

(1.30) Lemma
Let (G, H, T) be a loop folder and $(T, *) = (G, H, T)\lambda$. Further let x as well as $t_1, \ldots t_n$ be elements of T. Then the element $(((x * t_1) * t_2) \ldots) * t_n$ is the uniquely determined element of $Hxt_1 \ldots t_n \cap T$.

Proof. We show by induction that $H((((x * t_1) * t_2) \ldots) * t_n) = Hxt_1 \ldots t_n$. By definition this is true if $n = 1$. So suppose that the equation is true for

$n-1 \geq 1$ and set $s := (((x * t_1) * t_2) \ldots) * t_{n-1}$. Then we have

$$H(s * t_n) \overset{\text{Def.}}{=} Hst_n = (Hs)t_n \overset{\text{Ind.}}{=} (Hxt_1 \ldots t_{n-1})t_n = Hxt_1 \ldots t_n. \qquad \square$$

(1.31) Theorem ([Asc05, (1.7)])
Let (G, H, T) be a loop folder, $N := \mathrm{Core}_G(H)$ and $\bar{G} = G/N$. Then:

$$((G, H, T)\lambda)\varepsilon \cong (\langle \bar{T} \rangle, \bar{H} \cap \langle \bar{T} \rangle, \bar{T}).$$

Proof. Let $(T, *) = (G, H, T)\lambda$ and set $(G', H', T') := ((G, H, T)\lambda)\varepsilon$. Then we have $T' = \{\mathrm{R}_t \mid t \in T\} \subseteq \mathrm{Sym}(T)$, $G' = \langle T' \rangle$ and $H' = \mathrm{Stab}_{G'}(\mathrm{R}_{1_G})$. Further set

$$\Phi : G' \to \langle \bar{T} \rangle,\ \mathrm{R}_{t_1} \ldots \mathrm{R}_{t_n} \mapsto Nt_1 \ldots t_n.$$

First we show that Φ is well defined:
Let $\mathrm{R}_{t_1} \ldots \mathrm{R}_{t_n} = \mathrm{R}_{s_1} \ldots \mathrm{R}_{s_m} \in G'$. Then we have for all $x \in T$:

$$(((x * t_1) * t_2) \ldots) * t_n = (((x * s_1) * s_2) \ldots) * s_m.$$

We want to show that $Nt_1 \ldots t_n = Ns_1 \ldots s_m$. Let $g \in G$ and choose $x \in T$ with $Hg = Hx$. By Lemma (1.30) the previous equation implies

$$Hxt_1 \ldots t_n = Hxs_1 \ldots s_m.$$

Thus

$$g^{-1}Hxt_1 \ldots t_n = g^{-1}Hxs_1 \ldots s_m$$

and hence

$$g^{-1}Hgt_1 \ldots t_n = g^{-1}Hgs_1 \ldots s_m.$$

Since g was an arbitrary element of G it follows that $Nt_1 \ldots t_n = Ns_1 \ldots s_m$ as $N = \bigcap_{g \in G} H^g$.
Clearly Φ is a group homomorphism. We have $(T')\Phi = \bar{T}$, hence Φ is surjective.
To show that Φ is injective assume there are $t_1, \ldots, t_n, s_1, \ldots, s_m \in T$ with

$$Nt_1 \ldots t_n = Ns_1 \ldots s_m.$$

Since N is a normal subgroup of G and $N \leq H$ we have for all $x \in T$:

$$\begin{aligned} Hxt_1 \ldots t_n &= HNxt_1 \ldots t_n = HxNt_1 \ldots t_n = HxNs_1 \ldots s_m \\ &= HNxs_1 \ldots s_m = Hxs_1 \ldots s_m. \end{aligned}$$

Thus, by Lemma (1.30), for all $x \in T$ the equation

$$(((x * t_1) * t_2) \ldots) * t_n = (((x * s_1) * s_2) \ldots) * s_m$$

holds. Hence $R_{t_1} \dots R_{t_n} = R_{s_1} \dots R_{s_m}$.
Finally we show $(H')\Phi = \bar{H} \cap \langle \bar{T} \rangle$: Consider $h' \in H'$. Choose $t_1, \dots t_n \in T$ with $h' = R_{t_1} \dots R_{t_n}$. Then we have

$$1_G = 1_G h' = (((1_G * t_1) * t_2) \dots) * t_n = (((t_1 * t_2) * t_3) \dots) * t_n.$$

So we have

$$H = H1_G = Ht_1 \dots t_n$$

and thus $t_1 \dots t_n \in H \cap \langle T \rangle$. Hence $h'\Phi = Nt_1 \dots t_n \in \bar{H} \cap \langle \bar{T} \rangle$. Since Φ is bijective and $\bar{H}\langle \bar{T} \rangle = \bar{G}$ we have

$$\begin{aligned} |\langle \bar{T} \rangle|/|\bar{T}| &= |G'|/|T'| = |H'| = |(H')\Phi| \leq |\bar{H} \cap \langle \bar{T} \rangle| \\ &= |\langle \bar{T} \rangle| \cdot |\bar{H}|/|\bar{H}\langle \bar{T} \rangle| = |\langle \bar{T} \rangle| \cdot |\bar{H}|/|\bar{G}| = |\langle \bar{T} \rangle|/|\bar{T}| \end{aligned}$$

and thus $(H')\Phi = \bar{H} \cap \langle \bar{T} \rangle$. □

(1.32) Remark
Let $\mathcal{L}$ be a loop. Among all loop folders (G, H, T) with $(G, H, T)\lambda \cong \mathcal{L}$ the envelope of $\mathcal{L}$ is the smallest one, i.e. the only one (up to isomorphism) that is faithful and satisfies $G = \langle T \rangle$. Thus, for such a loop folder, we have $((G, H, T)\lambda)\varepsilon \cong (G, H, T)$. Hence the functors ε and λ provide an equivalence between the categories $\mathbf{LP}_s$ and $\mathbf{EL}$.

Finally we show that for a loop folder (G, H, T) where T is a subgroup of G the loop $(G, H, T)\lambda$ is associative and hence a group. Further we show that the right multiplication group $\mathrm{RM}(\mathcal{L})$ of a non-associative loop $\mathcal{L}$ is non-abelian and that the envelope $\mathcal{L}\varepsilon$ of a loop $\mathcal{L}$ is a non-trivial loop folder.

(1.33) Lemma
Let (G, H, T) be a loop folder and $T \leq G$ be a subgroup of G. Then we have $(G, H, T)\lambda \cong (T, \cdot)$ as loops where $\cdot$ denotes the multiplication in G. In particular the loop $(G, H, T)\lambda$ is associative and hence a group.

Proof. By definition we have $(G, H, T)\lambda = (T, *)$ where $t_1 * t_2$ is the uniquely determined element in $Ht_1t_2 \cap T$. Since $T \leq G$ we have for all $t_1, t_2, t_3 \in T$:

$$t_1 * t_2 = t_3 \Leftrightarrow Ht_1t_2 = Ht_3 \Leftrightarrow t_1t_2t_3^{-1} \in H \cap T = \{1_G\} \Leftrightarrow t_1t_2 = t_3. \qquad \square$$

(1.34) Lemma
Let $\mathcal{L}$ be a loop and (G, H, T) be the envelope of $\mathcal{L}$. Suppose G is abelian. Then $G \cong \mathcal{L}$. Hence the right multiplication group of a non-associative loop is non-abelian.

Proof. Since (G, H, T) is the envelope of $\mathcal{L}$ we have $\mathrm{Core}_G(H) = \{1_G\}$ by Lemma (1.19). If G is abelian we have $H = \mathrm{Core}_G(H) = \{1_G\}$ and therefore $T = G$. By Lemma (1.33) we have $\mathcal{L} \cong T = G$ and $\mathcal{L}$ is associative. □

(1.35) Remark
Let $\mathcal{L}$ be a loop and (G, H, T) be the envelope of $\mathcal{L}$. Suppose (G, H, T) is a trivial loop folder. Then we have $T = \{1_G\}$ or $T = G$. Hence $T \leq G$ and by Theorem (1.22) and Lemma (1.33) the loop $\mathcal{L}$ is a group.
On the other hand the envelope of a group G is isomorphic to $(G, \{1_G\}, G)$ and hence a trivial loop folder. Thus the envelope of a loop is a trivial loop folder if and only if the loop is a group.

Chapter 2

RCC loops and RCC loop folders

This chapter is divided into four sections. The first section provides an introduction to right conjugacy closed loops and right conjugacy closed loop folders. The second section considers right conjugacy closed loop folders and simple groups. In the third section we give a new proof of a known result of Aleš Drápal (see [Drá04]): A right conjugacy closed loop of prime order is associative. In the fourth section we prove some necessary technical lemmas.

2.1 RCC loops and RCC loop folder

(2.1) Definition (RCC loop, LCC loop, CC loop)
A loop $\mathcal{L}$ is called right conjugacy closed (RCC), left conjugacy closed (LCC) or conjugacy closed (CC) if the set $\mathrm{R}_{\mathcal{L}}$, the set $\mathrm{L}_{\mathcal{L}}$ or both (see Chapter 1, Definition (1.6)) are closed under conjugation, respectively. I.e. for all $x, y \in \mathcal{L}$ we have

$$\mathrm{R}_x^{-1}\mathrm{R}_y\mathrm{R}_x \in \mathrm{R}_{\mathcal{L}} \quad \text{or/and} \quad \mathrm{L}_x^{-1}\mathrm{L}_y\mathrm{L}_x \in \mathrm{L}_{\mathcal{L}}.$$

(2.2) Example
Let $\mathcal{L} := \{1, \ldots, 6\}$ and $* : \mathcal{L} \to \mathcal{L}$ with

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	5	6	3
3	3	4	5	6	1	2
4	4	3	6	1	2	5
5	5	6	1	2	3	4
6	6	5	2	3	4	1

We have $\mathrm{R}_{\mathcal{L}} = \{\mathrm{R}_1, \ldots, \mathrm{R}_6\}$ and $\mathrm{R}_1, \mathrm{R}_3, \mathrm{R}_5 \in Z(\mathrm{RM}(\mathcal{L}))$. Further, the conjugacy class of R_2 in $\mathrm{RM}(\mathcal{L})$ is given by

$$\mathrm{R}_2{}^{RM(\mathcal{L})} = \{\mathrm{R}_2, \mathrm{R}_4, \mathrm{R}_6\}.$$

As a union of $\mathrm{RM}(\mathcal{L})$-conjugacy classes the set $\mathrm{R}_{\mathcal{L}}$ is $\mathrm{RM}(\mathcal{L})$-invariant and hence also $\mathrm{R}_{\mathcal{L}}$-invariant. So $\mathcal{L}$ is an RCC loop.

In fact $\mathcal{L}$ is one of the smallest examples of a non-associative RCC loop. Later we show that all RCC loops of prime order are associative so there is just one RCC loop of order five: the cyclic group Cyc(5).

(2.3) Definition (RCC loop folder)
A loop folder (G, H, T) is called *right conjugacy closed* (RCC) if the transversal T is G-invariant under conjugation, i.e. $g^{-1}tg \in T$ for all $g \in G, t \in T$.

(2.4) Lemma
Let (G, H, T) be an RCC *loop folder. Then $(G, H, T)\lambda$ is an* RCC *loop. Further, if $\mathcal{L}$ is an* RCC *loop then $\mathcal{L}\varepsilon$ is an* RCC *loop folder.*

Proof. By Lemma (1.20), $(G, H, T)\lambda$ is a loop. So we have to show that for any fixed $t_1, t_2 \in T$ there is $t_3 \in T$ with $\mathrm{R}_{t_1}^{-1}\mathrm{R}_{t_2}\mathrm{R}_{t_1} = \mathrm{R}_{t_3} \in \mathrm{R}_T$: Let $t_1, t_2 \in T$. Since $T^G = T$ there is $t_3 \in T$ with $t_1^{-1}t_2t_1 = t_3$. Let $x \in T$. Then $(x * t_2) * t_1$ is the uniquely determined element in $Hxt_2t_1 \cap T$ and $(x * t_1) * t_3$ is the uniquely determined element in $Hxt_1t_3 \cap T$. Since $t_2t_1 = t_1t_3$ we have for all $x \in T$:

$$(x * t_2) * t_1 = (x * t_1) * t_3.$$

So $\mathrm{R}_{t_2}\mathrm{R}_{t_1} = \mathrm{R}_{t_1}\mathrm{R}_{t_3}$, i.e. $\mathrm{R}_{t_1}^{-1}\mathrm{R}_{t_2}\mathrm{R}_{t_1} = \mathrm{R}_{t_3}$.
Clearly the envelope of an RCC loop is an RCC loop folder. □

The next lemmas and remarks give some basic properties of RCC loop folders, which we will require in our study of RCC loops and their envelopes.

(2.5) Lemma
Let (G, H, T) be an RCC *loop folder. Then T is a transversal for the left cosets of H in G. Hence (G, H, T^{-1}) is also an* RCC *loop folder.*

Proof. Let $g \in G$. Then there are $h \in H$ and $s \in T$ with $g = hs$. Set $t := hsh^{-1}$. We have $t \in T$ and

$$g = hs = (hsh^{-1})h = th \in tH.$$

Hence T is a transversal for the left cosets of H in G. Thus T^{-1} is a transversal for the right cosets of H in G and (G, H, T^{-1}) is an RCC loop folder. □

Notice that the proof of the last lemma only requires that the set T is H-invariant. However, since we are interested in RCC loop folders, we formulated the lemma for this case. The next remark shows a general construction method for RCC loop folders.

(2.6) Remark
Let G be a group and denote the derived subgroup of G by G'. Let $H \leq G$ be a subgroup of G with $H \cap G' = \{1_G\}$ and let $S \subseteq G$ with $1_G \in S$ be a right transversal of HG' in G. Set $T := G'S$. Then we have

$$|T| = |G'| \cdot |S| = |G'| \cdot [G : HG'] = |G'| \cdot |G|/(|H|\,|G'|) = [G : H].$$

Additionally, for arbitrary $g \in G$ there are $s \in S$, $x \in G'$ and $h \in H$ with

$$g = (hx)s = h(xs) \in H(xs)$$

and $xs \in T$. Hence T is a transversal for the right cosets of H in G.
Further, we show that T is G-invariant: Let $t = xs \in T$ with $x \in G'$ and $s \in S$. Then we have for arbitrary $g \in G$ and $y := [g, t^{-1}]$:

$$g^{-1}tg = g^{-1}tgt^{-1}t = yt = (yx)s \in G's \subseteq T.$$

Thus, (G, H, T) is an RCC loop folder.
A G-invariant right transversal $T = G'S$ can be a subgroup of G. In this case T is a normal subgroup of G and by Lemma (1.33) the loop $(G, H, T)\lambda \cong T$ is associative. However, there might be G-invariant right transversals of H which are not of the form $G'S$, where S is a right transversal of HG' in G.

The following statement is an unpublished lemma of Gerhard Hiß.

(2.7) Lemma
Let (G, H, T) be an RCC *loop folder. Then $N_G(H) = H \cdot C_G(H)$.*

Proof. Let $g \in N_G(H) \leq G$. There are $h \in H$ and $t \in T$ with $g = ht$. Since $h \in N_G(H)$ we have $t \in N_G(H)$. For all $\tilde{h} \in H$ we have

$$\underbrace{(\tilde{h}t\tilde{h}^{-1})}_{\in T}t^{-1} = \tilde{h}\,\underbrace{(t\tilde{h}^{-1}t^{-1})}_{\in H} \in H.$$

Since $\tilde{h}t\tilde{h}^{-1}$ and t are two elements of T which lie in the same right coset of H they are equal, i.e. $\tilde{h}t\tilde{h}^{-1} = t$. Thus $t^{-1}\tilde{h}t = \tilde{h}$ for all $\tilde{h} \in H$. Hence $t \in C_G(H)$ and $g = ht \in H \cdot C_G(H)$. □

(2.8) Remark
Let (G, H, T) be an RCC loop folder. As T is G-invariant, T is a union of conjugacy classes of G. Let $\{1_G\} = C_1, C_2, \ldots, C_m$ be the conjugacy classes

of G. For a suitable numbering there is a $k \in \{1, \ldots, m\}$ with $T = \bigcup_{i=1}^{k} C_i$. In particular we have

$$[G : H] = |T| = \sum_{i=1}^{k} |C_i| = 1 + \sum_{i=2}^{k} |C_i|.$$

This is often useful to show that there is no RCC loop folder (G, H, T) for a fixed group G. See for example Section 2.2.

Recall that all loops of order less than five are associative. The right multiplication group of an associative loop is isomorphic to the loop. So in general[1] the right multiplication group of an associative loop $\mathcal{L}$ is much smaller than the symmetric group $\mathrm{Sym}(\mathcal{L})$ or the alternating group $\mathrm{Alt}(\mathcal{L})$.
However the right multiplication group of a non-associative loop $\mathcal{L}$ may be the whole symmetric group $\mathrm{Sym}(\mathcal{L})$ as we have seen in Example (1.7). Moreover, see [DK89], there are also non-associative loops whose right multiplication group is the alternating group $\mathrm{Alt}(\mathcal{L})$. For a non-associative RCC loop this is not possible as we see in the next lemma.

(2.9) Lemma
Let $\mathcal{L}$ be a non-associative RCC *loop. Then* $\mathrm{RM}(\mathcal{L})$ *is a proper subgroup of* $\mathrm{Sym}(\mathcal{L})$ *not equal to* $\mathrm{Alt}(\mathcal{L})$.

Proof. Since $\mathcal{L}$ is non-associative we have $|\mathcal{L}| \geq 5$. Suppose that $\mathrm{RM}(\mathcal{L})$ is equal to $\mathrm{Sym}(\mathcal{L})$ or $\mathrm{Alt}(\mathcal{L})$. Set

$$G := \mathrm{RM}(\mathcal{L}), \quad H := \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_{\mathcal{L}}), \quad T := \mathrm{R}_{\mathcal{L}}.$$

Then the envelope of $\mathcal{L}$ is given by (G, H, T). We know that T is a union of conjugacy classes of G with $1_G \in T$ and $|T| = |\mathcal{L}|$. By [Con, Lemma 5.1] we also know that the non-trivial conjugacy classes of $\mathrm{Sym}(\mathcal{L})$ and $\mathrm{Alt}(\mathcal{L})$ have size at least $|\mathcal{L}|$. In view of (2.8), this is a contradiction. □

2.2 RCC loop folder and simple groups

Recall that a loop folder (G, H, T) is trivial if $|T| = 1$ or $|H| = 1$. In this section we examine the following conjecture:

(2.10) Conjecture
Let (G, H, T) be a non-trivial RCC loop folder. Then G is not simple.

Although the above conjecture concerns arbitrary RCC loop folders we can reduce it to envelopes of RCC loops:

[1] If the order of the loop is at least four.

Let $\mathcal{L}$ be an RCC loop and (G, H, T) a non-trivial loop folder with $(G, H, T)\lambda \cong \mathcal{L}$. Suppose G is simple. Since $N := \mathrm{Core}_G(H) \trianglelefteq G$ we have $N = \{1_G\}$ and since $\langle T \rangle \trianglelefteq G$ we have $\langle T \rangle = G$. By Remark (1.32) we have $(G, H, T) \cong \mathcal{L}\varepsilon$. So conjecture (2.10) is equivalent to:

(2.11) Conjecture
Let $\mathcal{L}$ be an RCC loop. Then $\mathrm{RM}(\mathcal{L})$ is simple if and only if $\mathcal{L}$ is a group and hence $\mathcal{L} \cong \mathrm{RM}(\mathcal{L})$.

In this section the conjecture is proved for the alternating groups $\mathrm{Alt}(n)$ with $5 \leq n \leq 18$, all sporadic simple groups and the group $\mathrm{PSL}(2, q)$, q a prime power. For this we apply a lemma about the class multiplication coefficients of conjugacy classes of G which contains elements of H.

Recall the definition of the class multiplication coefficients, see [Isa06, Theorem (2.4) and Problem (3.9)]
Let G be a group and let C_1, C_2, C_3 be conjugacy classes of G. Then the corresponding class multiplication coefficient is defined for a fixed $c_3 \in C_3$ as

$$\mathrm{cmc}(C_1, C_2, C_3) = |\{(c_1, c_2) \mid c_1 \in C_1, c_2 \in C_2, c_1 c_2 = c_3\}|.$$

This definition is independent of the choice of $c_3 \in C_3$. It is possible to calculate the class multiplication coefficients from the ordinary $\mathbb{C}$-character table of G by

$$\mathrm{cmc}(C_1, C_2, C_3) = \frac{|C_1||C_2|}{|G|} \sum_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \frac{\chi(c_1)\chi(c_2)\chi(c_3^{-1})}{\chi(1_G)}$$

for fixed $c_i \in C_i$, $i = 1, 2, 3$.

For the alternating groups $\mathrm{Alt}(n)$ with $5 \leq n \leq 18$, the sporadic simple groups and for the groups $\mathrm{PSL}(2, q)$ the $\mathbb{C}$-character tables are known and in most of these cases we can calculate the class multiplication coefficients with GAP or CHEVIE. For more information about GAP see [Gap] and for more information about CHEVIE see [Gec+96]. But first we prove the following lemma about the class multiplication coefficients. For an element x of a group G we denote the conjugacy class of x in G by x^G.

(2.12) Lemma
Let G be a group and $H \leq G$ be a subgroup of G. Let U be a union of conjugacy classes of G with $1_G \in U$. Then U contains at most one element of each right coset of H in G if and only if

$$\mathrm{cmc}(C_1, C_2^{-1}, h^G) = 0$$

for all conjugacy classes $C_1, C_2 \subseteq U$ *and* $h \in H \setminus \{1_G\}$.
In particular, if (G, H, T) *is an* RCC *loop folder then we have for all conjugacy classes* C *of* G *with* $C \subseteq T$*:*

$$\mathrm{cmc}(C, C^{-1}, h^G) = 0$$

for all $h \in H \setminus \{1_G\}$.

Proof. Fix two conjugacy classes $C_1, C_2 \subseteq U$. By definition we have for some $h \in H \setminus \{1_G\}$ that $\mathrm{cmc}(C_1, C_2^{-1}, h^G) \neq 0$ if and only if there are elements $c_1 \in C_1$ and $c_2 \in C_2$ with $c_1 c_2^{-1} = h$. Hence we have for some $h \in H \setminus \{1_G\}$ that $\mathrm{cmc}(C_1, C_2^{-1}, h^G) \neq 0$ if and only if there are $c_1 \in C_1 \subseteq U$ and $c_2 \in C_2 \subseteq U$ with $Hc_1 = Hc_2$. So U contains at most one element of each right coset of H in G if and only if $\mathrm{cmc}(C_1, C_2^{-1}, h^G) = 0$ for all conjugacy classes $C_1, C_2 \subseteq U$ and $h \in H \setminus \{1_G\}$. □

Consider an RCC loop folder (G, H, T). The following criterion allows us to reduce the number of conjugacy classes we need to consider for constructing T, by eliminating some conjugacy classes which cannot possibly lie in T.

(2.13) Remark
Let G be a group and C a conjugacy class of G with

$$\mathrm{cmc}(C, C^{-1}, D) \neq 0$$

for all conjugacy classes $D \neq \{1_G\}$ of G. Then there is no RCC loop folder (G, H, T) with $C \subseteq T$.

Now we show that there is no non-trivial RCC loop folder (G, H, T) with G isomorphic to a sporadic simple group or an alternating group $\mathrm{Alt}(n)$ for $5 \leq n \leq 18$. Before proving the theorems we first show explicitly for the case of the Mathieu Group M_{12} how we use Remark (2.13) to prove that there is no non-trivial RCC loop folder (G, H, T) with G isomorphic to M_{12}. This illustrates the idea of the proof.

(2.14) Example
The Mathieu Group on twelve points M_{12} is provided in GAP as

AltlasGroup(″M12″).

The group M_{12} has 15 conjugacy classes with GAP names

$$1a, 2a, 5a, 10a, 3a, 6a, 2b, 4a, 8a, 4b, 3b, 8b, 11a, 11b, 6b.$$

Let C be a non-trivial conjugacy class of M_{12}. We calculate the class multiplication coefficient $\mathrm{cmc}(C, C^{-1}, D)$ for all non-trivial conjugacy classes D of M_{12}

with GAP. The next table lists all non-trivial conjugacy classes C of M_{12} for which a non-trivial conjugacy class D of M_{12} exists with $\mathrm{cmc}(C, C^{-1}, D) = 0$ in column one and all of these conjugacy classes D in column two.

C	D
$2a$	$10a, 8a, 3b, 8b, 11a, 11b, 6b$
$2b$	$2a, 10a, 6a, 8a, 8b, 11a, 11b$
$4a$	$2a$
$4b$	$2a$
$3b$	$10a$

Suppose there is a non-trivial RCC loop folder (G, H, T) with $G \cong M_{12}$. By Remark (2.13) only the conjugacy classes $2a, 2b, 4a, 4b$ and $3b$ are potential subsets of T. The next table lists the sizes of these conjugacy classes.

class	$2a$	$2b$	$4a$	$4b$	$3b$
size	396	495	2970	2970	1760

Hence there are 23 possibilities for the length of T. Since $1_{M_{12}}$ is an element of T we have

$$\begin{aligned} |T| \in \{ \quad & 397, \quad 496, \quad 892, \quad 1761, \quad 2157, \quad 2256, \quad 2652, \\ & 2971, \quad 3367, \quad 3466, \quad 3862, \quad 4731, \quad 5127, \quad 5226, \\ & 5622, \quad 5941, \quad 6337, \quad 6436, \quad 6832, \quad 7701, \quad 8097, \\ & 8196, \quad 8592 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \}. \end{aligned}$$

But all these possibilities do not divide the order of M_{12}. So there is no non-trivial RCC loop folder (G, H, T) with $G \cong M_{12}$.

(2.15) Theorem
Let (G, H, T) be a non-trivial RCC *loop folder. Then G is not a sporadic simple group.*

Proof. Suppose G is a sporadic simple group. We know that T is a union of conjugacy classes of G. By Remark (2.13) we can eliminate most of the conjugacy classes of G from being a subset of T by calculating the class multiplication coefficients with GAP. For the remaining conjugacy classes there are only a few possibilities for the length of T. But for all sporadic simple groups these possibilities do not divide the order of G.
Table 2.1 gives an overview of the sporadic simple groups, the number $nr_{C,T}$ of their non-trivial conjugacy classes C which cannot be eliminated by Remark (2.13) in column two, and the number $nr_{|T|}$ of possibilities for the length of T in column three. □

Table 2.1: The conjugacy classes of the sporadic simple groups

G	$nr_{C,T}$	$nr_{\|T\|}$	G	$nr_{C,T}$	$nr_{\|T\|}$
M_{11}	1	1	He	6	47
M_{12}	5	23	McL	4	15
M_{22}	1	1	Suz	5	31
M_{23}	1	1	Fi_{22}	28	201 326 591
M'_{24}	2	3	Fi_{23}	27	100 663 295
J_1	0	0	Fi'_{24}	5	31
J_2	7	71	Ly	3	7
J_3	3	7	Ru	3	7
J_4	2	3	B	12	4 095
HS	6	63	ON	2	3
Co_1	10	1 023	Th	2	3
Co_2	8	255	HN	5	31
Co_3	7	127	M	3	7

(2.16) Theorem
Let (G, H, T) *be a non-trivial* RCC *loop folder. Then* G *is not* $\mathrm{Alt}(n)$ *with* $5 \leq n \leq 18$.

Proof. Suppose $G = \mathrm{Alt}(n)$, $5 \leq n \leq 18$. The $\mathbb{C}$-character table of G is provided in GAP. So we can calculate the class multiplication coefficients of G and eliminate most of the conjugacy classes of G from being a subset of T by Remark (2.13). For the remaining conjugacy classes there are only a few possibilities for the length of T. But these possibilities do not divide the order of G.
For $5 \leq n \leq 18$, Table 2.2 gives the number $nr_{C,T}$ of non-trivial conjugacy classes C of $\mathrm{Alt}(n)$ which cannot be eliminated by Remark (2.13) in column two, and the number $nr_{|T|}$ of possibilities for the length of T in column three. The number $nr_{|T|}$ increases very quickly with n. This shows the complexity of the decision problem whether a conjugacy class is possibly a subset of a G-invariant transversal. □

Table 2.2: The conjugacy classes of $\mathrm{Alt}(n)$

n	$nr_{C,T}$	$nr_{\|T\|}$
5	2	2
6	2	2
7	2	3
8	6	31
9	7	95
10	6	63
11	9	511

G	$nr_{C,T}$	$nr_{\|T\|}$
12	12	4 095
13	12	3 071
14	16	65 535
15	25	25 165 823
16	27	75 497 471
17	27	100 663 295
18	39	412 316 860 415

Now we show that there is no non-trivial RCC loop folder (G, H, T) with $G = \mathrm{PSL}(2, q)$, $q \geq 4$. The conjugacy classes of G depend on the parity of q so we distinguish between $q \equiv 0 \pmod 2$, $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. The generic $\mathbb{C}$-character table of G is provided in CHEVIE. Again we calculate the class multiplication coefficients of G. Most of them can be calculated with CHEVIE. Those which cannot, are calculated in some technical lemmas in Section 2.4. By Remark (2.13) we can eliminate most of the conjugacy classes of G from being a subset of T. If we combine the remaining conjugacy classes of G to a potential transversal T, the length of T does not divide the order of G. Hence there is no non-trivial RCC loop folder (G, H, T) with $G = \mathrm{PSL}(2, q)$, $q \geq 4$.

(2.17) Lemma
Let (G, H, T) be a non-trivial RCC *loop folder. Suppose $G = \mathrm{PSL}(2, q)$ with $q \equiv 0 \pmod 2$. Then $q = 2$, $G \cong \mathrm{Sym}(3)$ and*

$$(G, H, T) \cong (\mathrm{Sym}(3), \mathrm{Sym}(2), \{(), (1\ 2\ 3), (1\ 3\ 2)\}).$$

In particular G is not simple.

Proof. Let $G = \mathrm{PSL}(2, q)$ with $q \equiv 0 \pmod 2$ and suppose there is an RCC loop folder (G, H, T). The group G has the trivial conjugacy class C_1 and three types of non-trivial conjugacy classes, denoted by C_2, C_3 and C_4. There are one class of type C_2, $q/2 - 1$ classes of type C_3, called $C_3(j)$, and $q/2$ classes of type C_4, called $C_4(j)$.
In [Sch07, Sec. 6] the generic $\mathbb{C}$-character table of G is computed. It is provided in CHEVIE and given by:

	C_1	C_2	$C_3(j)$	$C_4(j)$
Size	1	$(q-1)(q+1)$	$q(q+1)$	$q(q-1)$
Number	1	1	$\frac{q}{2}-1$	$\frac{q}{2}$
χ_1	1	1	1	1
χ_2	q	0	1	-1
$\chi_3(k)$	$q+1$	1	α_{jk}	0
$\chi_4(k)$	$q-1$	-1	0	β_{jk}

with

$$\begin{aligned} \alpha_{jk} &= 2\cos(\tfrac{2jk\pi}{q-1}), \\ \beta_{jk} &= -2\cos(\tfrac{2jk\pi}{q+1}) \end{aligned}$$

and

$$\begin{aligned} &j \in \{1,\ldots,q-2\} && \text{for type } C_3, \\ &j \in \{1,\ldots,q\} && \text{for type } C_4, \\ &k \in \{1,\ldots,q-2\} && \text{for type } \chi_3, \\ &k \in \{1,\ldots,q\} && \text{for type } \chi_4. \end{aligned}$$

Here the classes of type C_3 and C_4 as well as the characters of type χ_3 and χ_4 occur twice in the character table. We have $C_3(j) = C_3(q-1-j)$ and $C_4(j) = C_4(q+1-j)$.
Since all entries in the character table of G are real numbers we have $C^{-1} = C$ for each conjugacy class C in G.
We want to identify the non-trivial conjugacy classes C of G which satisfy

$$\mathrm{cmc}(C, C^{-1}, D) \neq 0$$

for all non-trivial conjugacy classes D of G. The classes of type C_3 and, for $q \geq 4$, the class C_2 satisfy this condition. Hence we can eliminate these classes from being a subset of T by Remark (2.13) whereas for the classes of type C_4 a different strategy is required.

Consider the class C_2. The following table gives for all non-trivial conjugacy classes D of G the class multiplication coefficients $\mathrm{cmc}(C_2, C_2^{-1}, D)$.

D	C_2	$C_3(j)$	$C_4(j)$
$\mathrm{cmc}(C_2, C_2^{-1}, D)$	$q-2$	$q-1$	$q+1$

All these class multiplication coefficients are calculated with CHEVIE.
For $q \geq 4$ none of these class multiplication coefficients is zero. Hence, by Remark (2.13), the class C_2 is not a subset of T, if $q \geq 4$.

Now we want to consider the classes of type C_3. These classes do only occur if $q \geq 4$. Since $C_3(j) = C_3(q-1-j)$ it suffices to consider the classes $C_3(j)$ with $j \in \{1, \ldots, q/2-1\}$.
Let j and l be two integers with $j, l \in \{1, \ldots, q/2-1\}$. Then we have $\mathrm{cmc}(C_3(j), C_3(j)^{-1}, C_3(l)) = q-1$ unless $C_3(l) = C_3(2j)$. We now determine the integer l with $l \in \{1, \ldots, q/2-1\}$ and $C_3(l) = C_3(2j)$:
If $1 \leq j < q/4$ then $l = 2j \in \{1, \ldots, q/2-1\}$ and $C_3(l) = C_3(2j)$.
If $q/4 \leq j \leq q/2-1$ then $l = q-1-2j \in \{1, \ldots, q/2-1\}$ and $C_3(l) = C_3(2j)$.
For notation we set

$$d_{3j} = \begin{cases} 2j & 1 \leq j < q/4 \\ q-1-2j & q/4 \leq j \leq q/2-1. \end{cases}$$

The following table gives for all non-trivial conjugacy classes D of G the class multiplication coefficients $\mathrm{cmc}(C_3(j), C_3(j)^{-1}, D)$.

D	C_2	$C_3(l)$		$C_4(l)$
$\mathrm{cmc}(C_3(j), C_3(j)^{-1}, D)$	$2q$	$2q-1$,	$l = d_{3j}$	$q+1$
		$q-1$,	else	

For the conjugacy classes D with $D \in \{C_2, C_3(d_{3j})\}$ these class multiplication coefficients are calculated in Lemma (2.30). The other two class multiplication coefficients are calculated with CHEVIE.
Since none of these class multiplication coefficients is zero, by Remark (2.13), none of the classes of type C_3 is a subset of T.

Let $q \geq 4$. Then only C_1 and the classes of type C_4 are possibly subsets of T. Let m be the number of those classes of type C_4, which are subsets of T. Then $|T| = mq(q-1)+1$. By Lemma (2.33) we have $|T| \nmid |G|$. But this is a contradiction.
For $q = 2$ we have $G = \mathrm{PSL}(2,2) \cong \mathrm{Sym}(3)$ and the class C_2 of length 3 and the (only) class C_4 of length 2 are possibly subsets of T. Thus there are three possibilities for T:

$$\begin{aligned} T &= C_1 \cup C_2 && \text{and hence} \quad |T| = 4, \\ T &= C_1 \cup C_4 && \text{and hence} \quad |T| = 3, \\ T &= C_1 \cup C_2 \cup C_4 && \text{and hence} \quad |T| = 6. \end{aligned}$$

In the first case we have $|T| \nmid |G|$, in the third case the RCC loop folder is trivial. The second case is in fact the statement of the lemma. □

In the proof of the previous lemma we did not eliminate the classes of type C_4 by Remark (2.13) from being a subset of T. Notice that this is in fact not possible since we have

$$\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_2) = 0$$

for all $j \in \{1, \ldots, q\}$.

(2.18) Lemma
Let (G, H, T) be a non-trivial RCC *loop folder. Then $G \neq \mathrm{PSL}(2, q)$ with $q \equiv 1 \pmod 4$.*

Proof. Let $G = \mathrm{PSL}(2, q)$ with $q \equiv 1 \pmod 4$ and suppose there is an RCC loop folder (G, H, T). The group G has the trivial conjugacy class C_1 and five types of non-trivial conjugacy classes, denoted by C_2, C_3, C_4, C_5 and C_6. There are $(q-5)/4$ classes of type C_4, called $C_4(j)$ and $(q-1)/4$ classes of type C_5, called $C_5(j)$. For every other type there is exactly one conjugacy class of this type.
As G is a factor group of $\mathrm{SL}(2, q)$ the generic $\mathbb{C}$-character table of G is computable from the generic $\mathbb{C}$-character table of $\mathrm{SL}(2, q)$ which is given in [Sch07, Sec. 6]. It is also provided in CHEVIE and given by:

	C_1	C_2	C_3	$C_4(j)$	$C_5(j)$	C_6
Size	1	$\frac{q^2-1}{2}$	$\frac{q^2-1}{2}$	$q(q+1)$	$q(q-1)$	$\frac{q(q+1)}{2}$
Number	1	1	1	$\frac{q-5}{4}$	$\frac{q-1}{4}$	1
χ_1	1	1	1	1	1	1
χ_2	q	0	0	1	-1	1
χ_3	$\frac{1}{2}(q+1)$	γ	δ	$(-1)^j$	0	$(-1)^{\frac{q-1}{4}}$
χ_4	$\frac{1}{2}(q+1)$	δ	γ	$(-1)^j$	0	$(-1)^{\frac{q-1}{4}}$
$\chi_5(k)$	$q+1$	1	1	α_{jk}	0	$2(-1)^k$
$\chi_6(k)$	$q-1$	-1	-1	0	β_{jk}	0

with

$$\begin{aligned}
\alpha_{jk} &= 2\cos(\tfrac{4jk\pi}{q-1}),\\
\beta_{jk} &= -2\cos(\tfrac{4jk\pi}{q+1}),\\
\gamma &= \tfrac{1}{2} - \tfrac{1}{2}\sqrt{q},\\
\delta &= \tfrac{1}{2} + \tfrac{1}{2}\sqrt{q}
\end{aligned}$$

and

$$\begin{aligned} j &\in \{1,\dots,\tfrac{q-3}{2}\} \setminus \{\tfrac{q-1}{4}\} && \text{for type } C_4,\\ j &\in \{1,\dots,\tfrac{q-1}{2}\} && \text{for type } C_5,\\ k &\in \{1,\dots,\tfrac{q-3}{2}\} \setminus \{\tfrac{q-1}{4}\} && \text{for type } \chi_5,\\ k &\in \{1,\dots,\tfrac{q-1}{2}\} && \text{for type } \chi_6. \end{aligned}$$

Here the classes of type C_4 and C_5 as well as the characters of type χ_5 and χ_6 occur twice in the character table. We have $C_4(j) = C_4((q-1)/2-j)$ and $C_5(j) = C_5((q+1)/2-j)$.
Since all entries in the character table of G are real numbers we have $C^{-1} = C$ for each conjugacy class C in G.
We want to determine the non-trivial conjugacy classes C of G which satisfy

$$\mathrm{cmc}(C, C^{-1}, D) \neq 0$$

for all non-trivial conjugacy classes D of G. The classes of the types C_4, C_5 and C_6 satisfy this condition. Hence we can eliminate these classes from being a subset of T by Remark (2.13) whereas for the classes C_2 and C_3 a different strategy is required.

Consider the class C_6. The following table gives for all non-trivial conjugacy classes D of G the class multiplication coefficients $\mathrm{cmc}(C_6, C_6^{-1}, D)$.

D	C_2	C_3	$C_4(j)$	$C_5(j)$	C_6
$\mathrm{cmc}(C_6, C_6^{-1}, D)$	q	q	$(q-1)/2$	$(q+1)/2$	$(q-1)/2$

All these class multiplication coefficients are calculated with CHEVIE.
Since none of these class multiplication coefficients is zero, by Remark (2.13), the class C_6 is not a subset of T.

Consider the classes of type C_4. These classes only occur if $q \geq 9$. Since we have $C_4(j) = C_4((q-1)/2-j)$ it suffices to consider the classes $C_4(j)$ with $j \in \{1,\dots,(q-5)/4\}$.
Let j and l be two integers with $j, l \in \{1,\dots,(q-5)/4\}$. Then we have $\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(l)) = 2q-2$ unless $C_4(l) = C_4(2j)$. Notice that if $q \equiv 1 \pmod 8$ and $j = (q-1)/8$ then there is no class $C_5(2j)$. So suppose $j \neq (q-1)/8$. We now determine the integer l with $l \in \{1,\dots,(q-5)/4\}$ and $C_4(l) = C_4(2j)$:
If $1 \leq j \leq (q-5)/8$ then $l = 2j \in \{1,\dots,(q-5)/4\}$ and $C_4(l) = C_4(2j)$.
If $(q+3)/8 \leq j \leq (q-5)/4$ then $l = (q-1)/2 - 2j \in \{1,\dots,(q-5)/4\}$ and $C_4(l) = C_4(2j)$.
For notation we set

$$d_{4j} = \begin{cases} 2j & 1 \leq j \leq (q-5)/8 \\ (q-1)/2 - 2j & (q+3)/8 \leq j \leq (q-5)/4. \end{cases}$$

The following table gives for all non-trivial conjugacy classes D of G the class multiplication coefficients $\mathrm{cmc}(C_4(j), C_4(j)^{-1}, D)$.

D	C_2	C_3	$C_4(l)$		$C_5(l)$	C_6	
$\mathrm{cmc}(C_4(j), C_4(j)^{-1}, D)$	$3q$	$3q$	$3q-2$	$l=d_{4j}$	$2q+2$	$4q-2$	$j=\frac{q-1}{8}$
			$2q-2$	else		$2q-2$	else

For the conjugacy classes D with $D \in \{C_2, C_3, C_4(d_{3j})\}$ and for $D = C_6$ where $q \equiv 1 \pmod 8$ and $j = (q-1)/8$ these class multiplication coefficients are calculated in Lemma (2.31). The other three class multiplication coefficients are calculated with CHEVIE.
Since none of these class multiplication coefficients is zero, by Remark (2.13), none of the classes of type C_4 is a subset of T.

Consider now the classes of type C_5. Since $C_5(j) = C_5((q+1)/2-j)$ it suffice to consider the classes $C_5(j)$ with $j \in \{1, \ldots, (q-1)/4\}$.
Let j and l be two integers with $j, l \in \{1, \ldots, (q-1)/4\}$. Then we have $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(l)) = 2q+2$ unless $C_5(l) = C_5(2j)$. We now determine the integer l with $l \in \{1, \ldots, (q-1)/4\}$ and $C_5(l) = C_5(2j)$:
If $1 \leq j \leq (q-1)/8$ then $l = 2j \in \{1, \ldots, (q-1)/4\}$ and $C_5(l) = C_5(2j)$.
If $(q+3)/8 \leq j \leq (q-1)/4$ then $l = (q+1)/2 - 2j \in \{1, \ldots, (q-1)/4\}$ and $C_5(l) = C_5(2j)$.
For notation we set

$$d_{5j} = \begin{cases} 2j & 1 \leq j \leq (q-1)/8 \\ (q+1)/2 - 2j & (q+3)/8 \leq j \leq (q-1)/4. \end{cases}$$

The following table gives for all non-trivial conjugacy classes D of G the class multiplication coefficients $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, D)$.

D	C_2	C_3	$C_4(l)$	$C_5(l)$		C_6
$\mathrm{cmc}(C_5(j), C_5(j)^{-1}, D)$	q	q	$2q-2$	$q+2$	$l=d_{5j}$	$2q-2$
				$2q+2$	else	

For the conjugacy classes D with $D \in \{C_2, C_3, C_5(d_{5j})\}$ these class multiplication coefficients are calculated in Lemma (2.31). The other three class multiplication coefficients are calculated with CHEVIE.
Since none of these class multiplication coefficients is zero, by Remark (2.13), none of the classes of type C_5 is a subset of T.

Thus, only the non-trivial classes C_2 and C_3 are possibly subsets of T. Hence we have :

$T = C_1 \cup C_2$ or

$$\begin{aligned} T &= C_1 \cup C_3 \text{ or} \\ T &= C_1 \cup C_2 \cup C_3. \end{aligned}$$

Since $|C_2| = (q^2-1)/2 = |C_3|$ we have $|T| = (q^2+1)/2$ or $|T| = q^2$. By Lemma (2.34) we have $|T| \nmid |G|$. But this is a contradiction. □

In the proof of the previous lemma we did not eliminate the classes C_2 and C_3 by Remark (2.13) from being a subset of T. Notice that this is in fact not possible since we have

$$\mathrm{cmc}(C_2, C_2^{-1}, C_4(j)) = \mathrm{cmc}(C_3, C_3^{-1}, C_4(j)) = 0$$

if $j \in \{1, \ldots, (q-5)/4\}$ is odd.

(2.19) Lemma
Let (G, H, T) be a non-trivial RCC *loop folder. Suppose $G = \mathrm{PSL}(2, q)$ with $q \equiv 3 \pmod 4$. Then $q = 3$, $G \cong \mathrm{Alt}(4)$ and*

$$(G, H, T) \cong (\mathrm{Alt}(4), \langle (1\ 2\ 3) \rangle, \{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}).$$

In particular G is not simple.

Proof. Let $G = \mathrm{PSL}(2, q)$ with $q \equiv 3 \pmod 4$ and suppose there is an RCC loop folder (G, H, T). The group G has the trivial conjugacy class C_1 and five types of non-trivial conjugacy classes, denoted by C_2, C_3, C_4, C_5 and C_6. There are $(q-3)/4$ classes of type C_4, called $C_4(j)$, and $(q-3)/4$ classes of type C_5, called $C_5(j)$. For every other type there is exactly one conjugacy class of this type.
As G is a factor group of $\mathrm{SL}(2, q)$ the generic $\mathbb{C}$-character table of G is computable from the generic $\mathbb{C}$-character table of $\mathrm{SL}(2, q)$ which is given in [Sch07, Sec. 6]. It is also provided in CHEVIE and given by:

	C_1	C_2	C_3	$C_4(j)$	$C_5(j)$	C_6
Size	1	$\frac{q^2-1}{2}$	$\frac{q^2-1}{2}$	$q(q+1)$	$q(q-1)$	$\frac{q(q-1)}{2}$
Number	1	1	1	$\frac{q-3}{4}$	$\frac{q-3}{4}$	1
χ_1	1	1	1	1	1	1
χ_2	q	0	0	1	-1	-1
χ_3	$\frac{1}{2}(q-1)$	δ	γ	0	$-(-1)^j$	$-(-1)^{\frac{q+1}{4}}$
χ_4	$\frac{1}{2}(q-1)$	γ	δ	0	$-(-1)^j$	$-(-1)^{\frac{q+1}{4}}$
$\chi_5(k)$	$q+1$	1	1	α_{jk}	0	0
$\chi_6(k)$	$q-1$	-1	-1	0	β_{jk}	$-2(-1)^k$

with

$$\begin{aligned}\alpha_{jk} &= 2\cos(\tfrac{4jk\pi}{q-1}),\\ \beta_{jk} &= -2\cos(\tfrac{4jk\pi}{q+1}),\\ \gamma &= -\tfrac{1}{2}-\tfrac{1}{2}\sqrt{q}i,\\ \delta &= -\tfrac{1}{2}+\tfrac{1}{2}\sqrt{q}i,\end{aligned}$$

where i denotes the imaginary unit, and

$$\begin{aligned}&j \in \{1,\dots,\tfrac{q-3}{2}\} && \text{for type } C_4,\\ &j \in \{1,\dots,\tfrac{q-1}{2}\}\setminus\{\tfrac{q+1}{4}\} && \text{for type } C_5,\\ &k \in \{1,\dots,\tfrac{q-3}{2}\} && \text{for type } \chi_5,\\ &k \in \{1,\dots,\tfrac{q-1}{2}\}\setminus\{\tfrac{q+1}{4}\} && \text{for type } \chi_6.\end{aligned}$$

Here the classes of type C_4 and C_5 as well as the characters of type χ_5 and χ_6 occur twice in the character table. We have $C_4(j) = C_4((q-1)/2-j)$ and $C_5(j) = C_5((q+1)/2-j)$.
The entries γ and δ in the columns of the conjugacy classes C_2 and C_3 in the character table of G are not real numbers. Hence these two classes are not self-inverse. But since all other entries of the character table are real numbers we have $C_l^{-1} = C_l$ for all conjugacy classes C_l of G with $l \neq 2,3$. We have $C_2^{-1} = C_3$ since there are excatly two conjugacy classes of G which are not self-inverse.
We want to determine the non-trivial conjugacy classes C of G which satisfy

$$\mathrm{cmc}(C, C^{-1}, D) \neq 0$$

for all non-trivial conjugacy classes D of G. The classes of the types C_4 and C_5 satisfy this condition. Hence we can eliminate these classes from being a subset of T by Remark (2.13) whereas for the classes C_2, C_3 and C_6 a different strategy is required.

Consider the classes of type C_4. These classes only occur if $q \geq 7$. Since we have $C_4(j) = C_4((q-1)/2-j)$ it suffices to consider the classes $C_4(j)$ with $j \in \{1,\dots,(q-3)/4\}$.
Let j and l be two integers with $j,l \in \{1,\dots,(q-3)/4\}$. Then we have $\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(l)) = 2q-2$ unless $C_4(l) = C_4(2j)$. We now determine the integer l with $l \in \{1,\dots,(q-3)/4\}$ and $C_4(l) = C_4(2j)$:
If $1 \leq j \leq (q-3)/8$ then $l = 2j \in \{1,\dots,(q-3)/4\}$ and $C_4(l) = C_4(2j)$.
If $(q+1)/8 \leq j \leq (q-3)/4$ then $l = (q-1)/2-2j \in \{1,\dots,(q-3)/4\}$ and $C_4(l) = C_4(2j)$.
For notation we set

$$d_{4j} = \begin{cases} 2j & 1 \leq j \leq (q-3)/8\\ (q-1)/2-2j & (q+1)/8 \leq j \leq (q-3)/4.\end{cases}$$

The following table gives for all non-trivial conjugacy classes D of G the class multiplication coefficients $\mathrm{cmc}(C_4(j), C_4(j)^{-1}, D)$.

D	C_2	C_3	$C_4(l)$		$C_5(l)$	C_6
$\mathrm{cmc}(C_4(j), C_4(j)^{-1}, D)$	$3q$	$3q$	$3q-2$	$l=d_{4j}$	$2q+2$	$2q+2$
			$2q-2$	else		

For the conjugacy classes D with $D \in \{C_2, C_3, C_4(d_{4j})\}$ these class multiplication coefficients are calculated in Lemma (2.32). The other three class multiplication coefficients are calculated with CHEVIE.
Since none of these class multiplication coefficients is zero, by Remark (2.13), none of the classes of type C_4 is a subset of T.

Consider now the classes of type C_5. These classes do only occur if $q \geq 7$. Since $C_5(j) = C_5((q+1)/2 - j)$ it suffice to consider the classes $C_5(j)$ with $j \in \{1, \ldots, (q-3)/4\}$.
Let j and l be two integers with $j, l \in \{1, \ldots, (q-3)/4\}$. Then we have $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(l)) = 2q+2$ unless $C_5(l) = C_5(2j)$. Notice that if $q \equiv -1 \pmod 8$ and $j = (q+1)/8$ then there is no class $C_5(2j)$. So suppose $j \neq (q+1)/8$. We now determine the integer l with $l \in \{1, \ldots, (q-3)/4\}$ and $C_5(l) = C_5(2j)$:
If $1 \leq j \leq (q-3)/8$ then $l = 2j \in \{1, \ldots, (q-3)/4\}$ and $C_5(l) = C_5(2j)$.
If $(q+5)/8 \leq j \leq (q-3)/4$ then $l = (q+1)/2 - 2j \in \{1, \ldots, (q-3)/4\}$ and $C_5(l) = C_5(2j)$.
For notation we set

$$d_{5j} = \begin{cases} 2j & 1 \leq j \leq (q-3)/8 \\ (q+1)/2 - 2j & (q+5)/8 \leq j \leq (q-3)/4. \end{cases}$$

The following table gives for all non-trivial conjugacy classes D of G the class multiplication coefficients $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, D)$.

D	C_2	C_3	$C_4(l)$	$C_5(l)$		C_6	
$\mathrm{cmc}(C_5(j), C_5(j)^{-1}, D)$	q	q	$2q-2$	$q+2$	$l=d_{5j}$	2	$j=\frac{q+1}{8}$
				$2q+2$	else	$2q+2$	else

For the conjugacy classes D with $D \in \{C_2, C_3, C_5(d_{5j})\}$ and for $D = C_6$ where $q \equiv -1 \pmod 8$ and $j = (q+1)/8$ these class multiplication coefficients are calculated in Lemma (2.32). The other three class multiplication coefficients are calculated with CHEVIE.
Since none of these class multiplication coefficients is zero, by Remark (2.13), none of the classes of type C_5 is a subset of T.

Thus only the non-trivial classes C_2, C_3 and C_6 are possibly subsets of T. Hence there are seven possibilities for T:

$$\begin{aligned} T &= C_1 \cup C_2, \\ T &= C_1 \cup C_3, \\ T &= C_1 \cup C_6, \\ T &= C_1 \cup C_2 \cup C_3, \\ T &= C_1 \cup C_2 \cup C_6, \\ T &= C_1 \cup C_3 \cup C_6, \\ T &= C_1 \cup C_2 \cup C_3 \cup C_6. \end{aligned}$$

But then we have $|T| = n$ with

$$n \in \{\frac{q^2+1}{2},\ \frac{q^2-q+2}{2},\ q^2,\ \frac{2q^2-q+1}{2},\ \frac{1}{2}q(3q-1)\}.$$

By Lemma (2.34) we have $q = 3$ and $n = \frac{q^2-q+2}{2} = 4$. Thus, we have $G \cong \mathrm{Alt}(4)$ and $T = C_1 \cup C_6$ with $|T| = 4$. In fact, for $H = \langle (1\ 2\ 3) \rangle$ and

$$T = C_1 \cup C_6 = \{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

the triple (G, H, T) is an RCC loop folder. This is the statement of the lemma. □

In the proof of the previous lemma we could not eliminate the classes C_2, C_3 and C_6 by Remark (2.13) from being a subset of T since we have

$$\mathrm{cmc}(C_6, C_6^{-1}, C_2) = 0$$

and

$$\mathrm{cmc}(C_2, C_2^{-1}, C_5(j)) = \mathrm{cmc}(C_3, C_3^{-1}, C_5(j)) = 0$$

if $j \in \{1, \ldots, (q-3)/4\}$ is even.

(2.20) Theorem
Let (G, H, T) be a non-trivial RCC *loop folder with G simple. Then G is not equal to* $\mathrm{PSL}(2, q)$*, q a prime power.*

2.3 The RCC loops of prime order

In [Drá04] Aleš Drápal proved that an LCC loop of prime order p is associative and hence isomorphic to the cyclic group $\mathrm{Cyc}(p)$. Clearly this is also true for RCC loops. The result was proved with loop theoretic methods. In this section we give a new group theoretical proof. For an RCC loop $\mathcal{L}$ of prime order we determine the envelope (G, H, T) of $\mathcal{L}$. We show that $G \cong \mathcal{L}$ if G is abelian and that the assumption G is not abelian leads to a contradiction. Since the

loops of order n with $n \in \{2, 3\}$ are associative and since there is only one group of this order they are isomorphic to $\mathrm{Cyc}(n)$. Thus, to prove that an RCC loop of prime order is associative, we restrict our argumentation to primes p with $p \geq 5$.

In this section G' denotes the derived subgroup of G.

(2.21) Lemma
Let p be a prime with $p \geq 5$ and let $\mathcal{L}$ be an RCC *loop of order p. Further, let (G, H, T) be the envelope of $\mathcal{L}$. Suppose that G is abelian. Then $\mathcal{L}$ is isomorphic to the cyclic group* $\mathrm{Cyc}(p)$.

Proof. By Lemma (1.34) we have $G \cong \mathcal{L}$. Hence $\mathcal{L}$ is a group and there is just one group of order p up to isomorphism. □

(2.22) Lemma
Let p be a prime with $p \geq 5$ and let $\mathcal{L}$ be an RCC *loop of order p. Further, let (G, H, T) be the envelope of $\mathcal{L}$. Suppose that G is non-abelian. Then G' is a non-abelian simple group which acts transitively on $\mathcal{L}$.*

Proof. Recall that H is a point stabilizer. First we show that G' acts transitively on $\mathcal{L}$. Suppose it does not. Then $G \neq G'H$. Since H is a subgroup of index p and hence a maximal subgroup this implies $G' \leq H$. By Lemma (1.19) we have $\mathrm{Core}_G(H) = \{1_G\}$. Since $G' \trianglelefteq G$ we have $G' \leq \mathrm{Core}_G(H) = \{1_G\}$ and so G is abelian. But this is a contradiction.
By [Hup67, p. V.21.1], G' is a simple (possibly abelian) group and the factor group G/G' is isomorphic to $\mathrm{Cyc}(n)$ where n divides $p - 1$. Suppose G' is abelian. Then $G' \cong \mathrm{Cyc}(p)$. Since G' acts transitively we have

$$p = |G'| = p \cdot |G' \cap H|$$

and hence $G' \cap H = \{1_G\}$, $H \cong \mathrm{Cyc}(n)$ and $G = G' \rtimes H$.
We show that $Z(G) = \{1_G\}$: Suppose there is $z \in Z(G)$ with $z \neq 1_G$. Since (G, H, T) is the envelope of a loop we have $\mathrm{Core}_G(H) = \{1_G\}$ and hence $z \notin H$. Let $g, h \in G$ with $G' = \langle g \rangle$ and $H = \langle h \rangle$. Then $\langle g, h \rangle = G$. Let $e_1, e_2 \in \mathbb{N}$ with $z = h^{e_1} g^{e_2}$ and $g^{e_2} \neq 1_G$. We have $zh = hz$ and so $h^{e_1+1} g^{e_2} = h^{e_1} g^{e_2} h$. Thus, we have $g^{e_2} h = h g^{e_2}$, i.e. $g^{e_2} \in Z(G)$. Since $g^{e_2} \neq 1_G$ the element g^{e_2} generates G' and we have $G = \langle g^{e_2}, h \rangle$. But then G is abelian and this is a contradiction.
If $T = G'$ then $\langle T \rangle \neq G$. Hence this is a contradiction. Thus, we have $T \neq G'$. We show for all $x \in G \setminus G'$ that $|x^G| \geq p$. But this is a contradiction since T is a union of conjugacy classes and $|T| = p$.
Let $x \in G \setminus G'$. There are $h_x \in H \setminus \{1_G\}$ and $g_x \in G'$ with $x = h_x g_x$. Let $g_1, g_2 \in G'$ with $g_1^{-1} x g_1 = g_2^{-1} x g_2$. Then we have $(g_1 g_2^{-1})^{-1} x g_1 g_2^{-1} = x$ and since G' is abelian we have

$$h_x g_x = x = (g_1 g_2^{-1})^{-1} x g_1 g_2^{-1} = (g_1 g_2^{-1})^{-1} h_x g_1 g_2^{-1} g_x.$$

So $g_1 g_2^{-1} \in C_G(h_x) \cap G'$. If $C_G(h_x) \cap G' = G'$ we have $G' \leq C_G(h_x)$. Since H is abelian we have $h_x \in Z(G) = \{1_G\}$. But this is a contradiction. So we have $C_G(h_x) \cap G' = \{1_G\}$ and $g_1 = g_2$. Hence all elements of G' yield different conjugates of x and $|x^G| \geq |G'| = p$. □

(2.23) Lemma
Let p be a prime with $p \geq 5$ and let $\mathcal{L}$ be an RCC *loop of order p. Further, let (G, H, T) be the envelope of $\mathcal{L}$ and suppose that G is non-abelian. Then G is almost simple and G acts doubly transitively on $\mathcal{L}$.*

Proof. By Lemma (2.22), G' is a non-abelian simple group. Hence G is not solvable. By [Hup67, p. V.21.3], G is doubly transitive. Hence G acts primitively.
By [DM96, Th. 4.1A] the socle of a primitive group G is either the product of isomorphic simple groups or G is almost simple. Suppose there is a normal subgroup N of G, not equal to G'. Then $N \cong G'$ and $N \cap G' \trianglelefteq G$. Since G' is a minimal normal subgroup of G we have $N \cap G' = \{1_G\}$. But we have $[N, G'] \leq N \cap G' = \{1_G\}$ and so

$$N \cong N/(N \cap G') \cong NG'/G' \trianglelefteq G/G'.$$

Again, by [Hup67, p. V.21.1], the factor group G/G' is cyclic. Hence N (and so G') is abelian. But this is a contradiction. So G is almost simple. □

(2.24) Remark
Let p be a prime with $p \geq 5$ and let $\mathcal{L}$ be an RCC loop of order p. Further, let (G, H, T) be the envelope of $\mathcal{L}$ and suppose that G is non-abelian. By Lemma (2.23) G is almost simple and doubly transitive. In [Cam99, Table 7.4] the isomorphism types of the socles of almost simple and doubly transitive groups are listed. Notice that $\mathrm{soc}(G) = G'$. The following table lists the isomorphism types of $\mathrm{soc}(G)$ for which the degree of the action is potentially a prime p. (The action of $\mathrm{Alt}(k)$ in Line (9) is not specified in [Cam99, Table 7.4].)

case	soc(G)		p
(1)	$\mathrm{Sp}(2d, 2)$	$d \geq 3$	$2^{2d-1} + 2^{d-1}$
(2)	$\mathrm{Sp}(2d, 2)$	$d \geq 3$	$2^{2d-1} - 2^{d-1}$
(3)	$\mathrm{PSU}(3, q)$	$q \geq 3$	$q^3 + 1$
(4)	$R_1(q)$	$q = 3^{2d+1} > 3$	$q^3 + 1$
(5)	$Sz(q)$	$q = 2^{2d+1} > 2$	$q^2 + 1$
(6)	$\mathrm{PSL}(2, 11)$		11

case	soc(G)		p
(7)	M_{11}		11
(8)	M_{23}		23
(9)	Alt(k)		
(10)	PSL(m, q)	$m \geq 2$	$\frac{q^m-1}{q-1}$

(2.25) Lemma
Let p be a prime with $p \geq 5$ and let $\mathcal{L}$ be an RCC *loop of order p. Further, let (G, H, T) be the envelope of $\mathcal{L}$ and suppose that G is non-abelian. Then G' is not of the isomorphism types (1)-(9) of Remark (2.24).*

Proof. Suppose that Case (1) or Case (2) of Remark (2.24) holds. Since $d \geq 3$ the integer $p = 2^{2d-1} \pm 2^{d-1} = 2^{d-1}(2^d \pm 1)$ is not a prime.
Suppose that Case (3) or Case (4) of Remark (2.24) holds. Then the integer $p = q^3 + 1 = (q+1)(q^2 - q + 1)$ is not a prime.
Suppose that Case (5) of Remark (2.24) holds. Then $p = q^2 + 1 = 2^{2(2d+1)} + 1$ is not a prime since $2(2d+1)$ is not a power of 2.
Suppose that Case (6) of Remark (2.24) holds. Then soc(G) = PSL$(2, 11)$ and hence we have $G =$ PSL$(2, 11)$ or $G =$ PGL$(2, 11)$. By Theorem (2.20) we have $G =$ PGL$(2, 11)$. The transversal T is a union of conjugacy classes with $\{1_G\} \subseteq T$ and $|T| = 11$. But a non-trivial conjugacy class of PGL$(2, 11)$ has size at least 55. Hence this is a contradiction.
Suppose that Case (7) or Case (8) of Remark (2.24) holds. Since the outer automorphism groups of M_{11} and M_{23} are trivial we have $G = M_{11}$ respectively $G = M_{23}$. But this is a contradiction to Theorem (2.15).
Suppose that Case (9) of Remark (2.24) holds. By Lemma (2.22) G' acts transitively on p points. Since Alt(k) does not contain a subgroup of index p for $k < p$ we have $k \geq p$. By Lemma (1.19) G acts faithfully on $\mathcal{L}$, thus it is isomorphic to a subgroup of Sym(p). Hence soc(G) $\cong$ Alt(p) and $G \cong$ Alt(p) or $G \cong$ Sym(p). By [Con, Lemma 5.1] we have that the size of a non-trivial conjugacy class of G is a least p. But this is a contradiction. □

So far, we know that the right multiplication group G of an RCC loop $\mathcal{L}$ of prime order p with $p \geq 5$ is either abelian or almost simple with socle PSL(d, q) and $p = (q^d - 1)/(q - 1)$. Now we want to show that this almost simple case leads to a contradiction.
Let G be an almost simple group with socle S. Then we have $S \leq G \leq$ Aut(S). To show that G is not the right multiplication group of an RCC loop we need some information about the sizes of the conjugacy classes of G. Since the socle S is a normal subgroup of G the conjugacy classes of G contain only elements of S or contain no element of S. The following lemma gives an estimate of the sizes of the conjugacy classes of elements of $G \setminus S$. Although we usually identify the simple group S with its inner automorphism group Inn(S) we

will distinguish between these two groups in the following lemma for better readability.

(2.26) Lemma
Let G be an almost simple group with socle S, i.e. $S \cong \mathrm{Inn}(S) \leq G \leq \mathrm{Aut}(S)$. Let $\alpha \in G \setminus \mathrm{Inn}(S)$ and denote the conjugacy class of α in G by α^G. We have $C_{\mathrm{Inn}(S)}(\alpha) < \mathrm{Inn}(S)$ and

$$|\alpha^G| = [G : \mathrm{Inn}(S)\, C_G(\alpha)] \cdot [\mathrm{Inn}(S) : C_{\mathrm{Inn}(S)}(\alpha)].$$

In particular if c denotes the smallest index of any proper subgroup of S, then the size of the non-trivial conjugacy classes of G is at least c.

Proof. For elements $s \in S$ denote the conjugation with s by γ_s, i.e. the map $\gamma_s : S \to S, t \mapsto s^{-1}ts$ is an element of $\mathrm{Inn}(S)$. We have

$$\begin{aligned}
|\alpha^G| &= \frac{|G|}{|C_G(\alpha)|} \\
&= [G : \mathrm{Inn}(S)\, C_G(\alpha)] \cdot \frac{|\mathrm{Inn}(S)\, C_G(\alpha)|}{|C_G(\alpha)|} \\
&= [G : \mathrm{Inn}(S)\, C_G(\alpha)] \cdot \frac{|\mathrm{Inn}(S)|}{|C_G(\alpha) \cap \mathrm{Inn}(S)|} \\
&= [G : \mathrm{Inn}(S)\, C_G(\alpha)] \cdot \frac{|\mathrm{Inn}(S)|}{|C_{\mathrm{Inn}(S)}(\alpha)|}.
\end{aligned}$$

Suppose that $C_{\mathrm{Inn}(S)}(\alpha) = \mathrm{Inn}(S)$. Then we have $\alpha^{-1}\gamma_s\alpha = \gamma_s$ for all $s \in S$. Hence we have for all $t \in S$:

$$s^{-1}ts = (s^{-1} \cdot (t)\alpha^{-1} \cdot s)\alpha = (s^{-1})\alpha \cdot t \cdot (s)\alpha.$$

Thus $\gamma_s = \gamma_{(s)\alpha}$ for all $s \in S$. Since $\mathrm{Inn}(S) \cong S$ has a trivial center it follows that $s = (s)\alpha$ for all $s \in S$. Hence α is the trivial automorphism, $\alpha = 1_G$ which contradicts our assumption $\alpha \in G \setminus S$. Hence $C_{\mathrm{Inn}(S)}(\alpha) < \mathrm{Inn}(S)$.
Since $\mathrm{Inn}(S)$ is a normal subgroup of G the conjugacy classes of G contain only elements of $\mathrm{Inn}(S)$ or contain no element of $\mathrm{Inn}(S)$. Denote by c the smallest index of any proper subgroup of $\mathrm{Inn}(S)$. Since $\mathrm{Inn}(S)$ is simple c is an lower bound on the size of the non-trivial conjugacy classes of $\mathrm{Inn}(S)$. The non-trivial conjugacy classes of G which consists of elements of $\mathrm{Inn}(S)$ have size at least the minimal size of a non-trivial conjugacy class of $\mathrm{Inn}(S)$ hence size at least c. Since we have

$$|\alpha^G| \geq [\mathrm{Inn}(S) : C_{\mathrm{Inn}(S)}(\alpha)] \geq c$$

for all $\alpha \in G \setminus \mathrm{Inn}(S)$ the integer c is a lower bound on the size of the non-trivial conjugacy classes of G. □

(2.27) Lemma
Let p be a prime with $p \geq 5$ and let $\mathcal{L}$ be an RCC *loop of order p. Further, let (G, H, T) be the envelope of $\mathcal{L}$. Then G is abelian.*

Proof. Suppose that G is non-abelian. By Remark (2.24) and Lemma (2.25), G is an almost simple group with socle $\mathrm{soc}(G) = \mathrm{PSL}(m, q)$, $(m, q) \neq (2, 2), (2, 3)$, and $p = (q^m - 1)/(q - 1)$.
Denote by c the smallest index of any proper subgroup of $\mathrm{PSL}(m, q)$. By Lemma (2.26), c is a lower bound for the size of the non-trivial conjugacy classes of G. By [KL90, Th. 5.2.2] we have $c = (q^m - 1)/(q - 1)$ unless

$$(m, q) \in \{(2, 5), (2, 7), (2, 9), (2, 11), (4, 2)\}.$$

But in these exceptions the integer $(q^m - 1)/(q - 1)$ is not a prime. Hence the non-trivial conjugacy classes of G have size at least $p = (q^m - 1)/(q - 1)$. Since the tranversal T is a union of conjugacy classes with $\{1_G\} \subseteq T$ and $|T| = p$ this is a contradiction. □

(2.28) Corollary
Let $\mathcal{L}$ be an RCC *loop of prime order p. Then $\mathcal{L}$ is associative and $\mathcal{L} \cong \mathrm{Cyc}(p)$.*

2.4 Technical lemmas

In the next lemmas we calculate the class multiplication coefficients of $\mathrm{PSL}(2, q)$ that cannot be calculated with CHEVIE and show that special expressions in q do not divide the order of $\mathrm{PSL}(2, q)$ for the considered prime powers q. But first we prove a lemma which is very useful for calculating the class multiplication coefficients.

Recall the trigonometric equation (see [BBT07, Th.15.2])

$$\sum_{k=1}^{n} \cos(kx) = -\frac{1}{2} + \frac{1}{2} \cdot \sin((n + \frac{1}{2})x)/\sin(\frac{x}{2})$$

and the equation (see [Wal07, 7.16.k])

$$\cos^2(x) = \frac{1}{2} + \frac{1}{2}\cos(2x).$$

Thus, we also have

$$\cos^2(x) \cdot \cos(2x) = \frac{1}{4} + \frac{1}{2}\cos(2x) + \frac{1}{4}\cos(4x).$$

(2.29) Lemma
For $n \in \mathbb{N}$ and $y \in \mathbb{Z} \setminus \{0\}$ we have

$$\begin{aligned}
&\textstyle\sum_{k=1}^{n} \cos(k \cdot \frac{1}{n} \cdot 2\pi y) && = 0,\\
&\textstyle\sum_{k=1}^{n} \cos^2(k \cdot \frac{1}{n} \cdot 2\pi y) && = n/2,\\
&\textstyle\sum_{k=1}^{n} \cos^2(k \cdot \frac{1}{n} \cdot \pi y)\cos(k \cdot \frac{1}{n} \cdot 2\pi y) && = n/4.
\end{aligned}$$

Proof. We have

$$\begin{aligned}
\sum_{k=1}^{n} \cos(k \cdot \tfrac{1}{n} \cdot 2\pi y) &= -\tfrac{1}{2} + \tfrac{1}{2} \cdot \sin((n+\tfrac{1}{2})\tfrac{1}{n} \cdot 2\pi y)/\sin(\tfrac{\pi y}{n})\\
&= -\tfrac{1}{2} + \tfrac{1}{2} \cdot \sin(2\pi y + \tfrac{\pi y}{n})/\sin(\tfrac{\pi y}{n})\\
&= 0
\end{aligned}$$

and

$$\sum_{k=1}^{n} \cos^2(k \cdot \tfrac{1}{n} \cdot 2\pi y) = \sum_{k=1}^{n} \left[\tfrac{1}{2} + \tfrac{1}{2}\cos(k \cdot \tfrac{1}{n} \cdot 4\pi y)\right] = \tfrac{n}{2} + 0$$

and

$$\begin{aligned}
&\sum_{k=1}^{n} \cos^2(k \cdot \tfrac{1}{n} \cdot \pi y)\cos(k \cdot \tfrac{1}{n} \cdot 2\pi y)\\
&= \sum_{k=1}^{n} \left[\tfrac{1}{4} + \tfrac{1}{2}\cos(k \cdot \tfrac{1}{n} \cdot 2\pi y) + \tfrac{1}{4}\cos(k \cdot \tfrac{1}{n} \cdot 4\pi y)\right]\\
&= \frac{n}{4} + 0 + 0.
\end{aligned}$$

□

(2.30) Lemma
Let $G = \mathrm{PSL}(2,q)$ with $q \equiv 0 \pmod 2$ and $j \in \{1, \ldots, q/2-1\}$. Assume the notation of the conjugacy classes of G and of d_{3j} as in the proof of Lemma (2.17). Then we have

$$\begin{aligned}
\mathrm{cmc}(C_3(j), C_3(j)^{-1}, C_2) &= 2q,\\
\mathrm{cmc}(C_3(j), C_3(j)^{-1}, C_3(d_{3j})) &= 2q-1.
\end{aligned}$$

Proof. Recall that we have $C^{-1} = C$ for all conjugacy classes C of G. By Lemma (2.29), choosing $n = q-1$ and $y = j$, we have:

$$\begin{aligned}
&\mathrm{cmc}(C_3(j), C_3(j)^{-1}, C_2)\\
&= \frac{|C_3(j)|^2}{|G|}\left[\frac{1^3}{1} + \frac{1}{2}\cdot\frac{1}{q+1}\cdot 4 \cdot \sum_{k=1}^{q-2}\cos^2(\frac{2jk\pi}{q-1})\right]\\
&= \frac{q(q+1)}{q-1}\left[1 + \frac{2}{q+1}\cdot\left(\frac{q-1}{2} - \cos^2(2j\pi)\right)\right]
\end{aligned}$$

$$= \frac{q(q+1)}{q-1}\left[1+\frac{q-3}{q+1}\right]$$
$$= \frac{q(q+1)}{q-1}\cdot\frac{1}{(q+1)}\cdot[2q-2]$$
$$= 2q.$$

By Lemma (2.29), choosing $n = q-1$ and $y = 2j$, we have:

$$\begin{aligned}
&\mathrm{cmc}(C_3(j), C_3(j)^{-1}, C_3(2j))\\
&= \frac{|C_3(j)|^2}{|G|}\left[\frac{1^3}{1}+\frac{1^3}{q}+\frac{1}{2}\cdot\frac{1}{q+1}\cdot 8\cdot\sum_{k=1}^{q-2}\cos^2(\frac{2jk\pi}{q-1})\cos(\frac{4jk\pi}{q-1})\right]\\
&= \frac{q(q+1)}{q-1}\left[1+\frac{1}{q}+\frac{4}{q+1}\cdot\left(\frac{q-1}{4}-\cos^2(2j\pi)\cos(4j\pi)\right)\right]\\
&= \frac{q(q+1)}{q-1}\left[1+\frac{1}{q}+\frac{q-5}{q+1}\right]\\
&= \frac{q(q+1)}{q-1}\cdot\frac{1}{q(q+1)}\cdot\left[2q^2-3q+1\right]\\
&= 2q-1.
\end{aligned}$$

Notice that we have $C_3(d_{3j}) = C_3(2j)$. Hence we have also

$$\mathrm{cmc}(C_3(j), C_3(j)^{-1}, C_3(d_{3j})) = 2q-1. \qquad \square$$

(2.31) Lemma
Let $G = \mathrm{PSL}(2,q)$ with $q \equiv 1 \pmod 4$. Assume the notation of the conjugacy classes of G and of d_{4j} respectively d_{5j} as in the proof of Lemma (2.18). Then we have

$$\begin{aligned}
\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_2) &= 3q && \text{for } j \in \{1,\dots,(q-5)/4\},\\
\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_3) &= 3q && \text{for } j \in \{1,\dots,(q-5)/4\},\\
\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(d_{4j})) &= 3q-2, && \text{for } j \in \{1,\dots,(q-5)/4\},\\
\mathrm{cmc}(C_4(\tfrac{q-1}{8}), C_4(\tfrac{q-1}{8})^{-1}, C_6) &= 4q-2 && \text{for } q \equiv 1 \pmod 8,\\
\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_2) &= q && \text{for } j \in \{1,\dots,(q-1)/4\},\\
\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_3) &= q && \text{for } j \in \{1,\dots,(q-1)/4\},\\
\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(d_{5j})) &= q+2 && \text{for } j \in \{1,\dots,(q-1)/4\}.
\end{aligned}$$

Proof. Recall that we have $C^{-1} = C$ for all conjugacy classes C of G. Clearly we have $\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_2) = \mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_3)$. By Lemma (2.29), choosing $n = (q-1)/2$ and $y = j$, we have

$$\begin{aligned}
&\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_2))\\
&= \frac{|C_4(j)|^2}{|G|}\left[\frac{1^3}{1}+\frac{2}{q+1}(\frac{1}{2}-\frac{1}{2}\sqrt{q}+\frac{1}{2}+\frac{1}{2}\sqrt{q})\right.
\end{aligned}$$

$$
\begin{aligned}
&\quad + \frac{1}{2}\cdot\frac{1}{q+1}\cdot 4\cdot \sum_{\substack{1\le k\le \frac{q-3}{2}\\ k\neq \frac{q-1}{4}}} \cos^2(\frac{4jk\pi}{q-1}) \Bigg] \\
&= \frac{2q(q+1)}{q-1}\left[1+\frac{2}{q+1}+\frac{2}{q+1}\left(\frac{q-1}{4}-\cos^2(j\pi)-\cos^2(2j\pi)\right)\right] \\
&= \frac{2q(q+1)}{q-1}\left[1+\frac{2}{q+1}+\frac{2}{q+1}\cdot(\frac{q-1}{4}-2)\right] \\
&= \frac{2q(q+1)}{q-1}\cdot\frac{1}{2(q+1)}\left[3q-3\right] \\
&= 3q.
\end{aligned}
$$

By Lemma (2.29), choosing $n=(q-1)/2$ and $y=2j$ we have

$$
\begin{aligned}
&\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(2j)) \\
&= \frac{|C_4(j)|^2}{|G|}\left[\frac{1^3}{1}+\frac{1^3}{q}+2\cdot\frac{2(-1)^{4j}}{q+1}\right. \\
&\quad \left. + \frac{1}{2}\cdot\frac{1}{q+1}\cdot 8\cdot \sum_{\substack{1\le k\le \frac{q-3}{2}\\ k\neq \frac{q-1}{4}}} \cos^2(\frac{4jk\pi}{q-1})\cos(\frac{8jk\pi}{q-1}) \right] \\
&= \frac{2q(q+1)}{q-1}\left[1+\frac{1}{q}+\frac{4}{q+1}\right. \\
&\quad \left. +\frac{4}{q+1}\left(\frac{q-1}{8}-\cos^2(j\pi)\cos(2j\pi)-\cos^2(2j\pi)\cos(4j\pi)\right)\right] \\
&= \frac{2q(q+1)}{q-1}\left[1+\frac{1}{q}+\frac{4}{q+1}+\frac{q-1}{2(q+1)}-\frac{8}{q+1}\right] \\
&= \frac{2q(q+1)}{q-1}\cdot\frac{1}{2q(q+1)}\left[3q^2-5q+2\right] \\
&= 3q-2.
\end{aligned}
$$

Notice that we have $C_4(d_{4j}) = C_4(2j)$. Hence we have also

$$\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(d_{4j})) = 3q-2.$$

If $q \equiv 1 \pmod 8$ we have

$$
\begin{aligned}
&\mathrm{cmc}(C_4(\frac{q-1}{8}), C_4(\frac{q-1}{8})^{-1}, C_6) \\
&= \frac{|C_4(\frac{q-1}{8})|^2}{|G|}\left[\frac{1^3}{1}+\frac{1^3}{q}+2\cdot\frac{(-1)^{\frac{q-1}{4}}\cdot(-1)^{2\cdot\frac{q-1}{8}}\cdot 2}{q+1}\right. \\
&\quad \left. + \frac{1}{2}\cdot\frac{1}{q+1}\cdot 8\cdot \sum_{\substack{1\le k\le \frac{q-3}{2}\\ k\neq \frac{q-1}{4}}} \underbrace{(-1)^k\cos(\frac{1}{2}k\pi)}_{\begin{cases}=1 & k \text{ even}\\ =0 & k \text{ odd}\end{cases}} \right]
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{2q(q+1)}{q-1}\left[1+\frac{1}{q}+\frac{4}{q+1}+\frac{4}{q+1}\left(\frac{q-3}{4}-1\right)\right] \\
&= \frac{2q(q+1)}{q-1}\cdot\frac{1}{q(q+1)}\left[2q^2-3q+1\right] \\
&= 4q-2.
\end{aligned}
$$

Now we calculate $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_2)$ and $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_3)$. They are clearly equal. By Lemma (2.29), choosing $n = (q+1)/2$ and $y = j$, we have

$$
\begin{aligned}
&\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_2)) \\
&= \frac{|C_5(j)|^2}{|G|}\left[\frac{1^3}{1}-\frac{1}{2}\cdot\frac{1}{q-1}\cdot 4\cdot\sum_{k=1}^{\frac{q-1}{2}}\cos^2(\frac{4jk\pi}{q+1})\right] \\
&= \frac{2q(q-1)}{q+1}\left[1-\frac{2}{q-1}\left(\frac{q+1}{4}-\cos^2(2j\pi)\right)\right] \\
&= \frac{2q(q-1)}{q+1}\left[1-\frac{2}{q-1}\cdot\frac{q-3}{4}\right] \\
&= \frac{2q(q-1)}{q+1}\cdot\frac{1}{2(q-1)}\left[q+1\right] \\
&= q.
\end{aligned}
$$

By Lemma (2.29), choosing $n = (q+1)/2$ and $y = 2j$ we have

$$
\begin{aligned}
&\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(2j)) \\
&= \frac{|C_5(j)|^2}{|G|}\left[\frac{1^3}{1}+\frac{(-1)^3}{q}+\frac{1}{2}\cdot\frac{1}{q-1}\cdot(-8)\cdot\sum_{k=1}^{\frac{q-1}{2}}\cos^2(\frac{4jk\pi}{q+1})\cos(\frac{8jk\pi}{q+1})\right] \\
&= \frac{2q(q-1)}{q+1}\left[1-\frac{1}{q}-\frac{4}{q-1}\left(\frac{q+1}{8}-\cos^2(2j\pi)\cos(4j\pi)\right)\right] \\
&= \frac{2q(q-1)}{q+1}\left[1-\frac{1}{q}-\frac{q-7}{2(q-1)}\right] \\
&= \frac{2q(q-1)}{q+1}\cdot\frac{1}{2q(q-1)}\left[q^2+3q+2\right] \\
&= q+2
\end{aligned}
$$

Notice that we have $C_5(d_{5j}) = C_5(2j)$. Hence we have also

$$\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(d_{5j})) = q+2. \qquad \square$$

(2.32) Lemma
Let $G = \mathrm{PSL}(2,q)$ with $q \equiv 3 \pmod 4$.Assume the notation of the conjugacy classes of G and of d_{4j} respectively d_{5j} as in the proof of Lemma (2.19). Then we have

$$\begin{aligned}
\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_2) &= 3q && \text{for } j \in \{1,\dots,(q-3)/4\},\\
\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_3) &= 3q && \text{for } j \in \{1,\dots,(q-3)/4\},\\
\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(d_{4j})) &= 3q-2 && \text{for } j \in \{1,\dots,(q-3)/4\},
\end{aligned}$$

$$\begin{aligned}
\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_2) &= q && \text{for } j \in \{1,\dots,(q-3)/4\},\\
\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_3) &= q && \text{for } j \in \{1,\dots,(q-3)/4\},\\
\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(d_{5j})) &= q+2 && \text{for } j \in \{1,\dots,(q-3)/4\},\\
\mathrm{cmc}(C_5(\tfrac{q+1}{8}), C_5(\tfrac{q+1}{8})^{-1}, C_6) &= 2 && \text{for } q \equiv -1 \pmod 8.
\end{aligned}$$

Proof. Recall that we have $C_2^{-1} = C_3$ and $C_l^{-1} = C_l$ for $i \neq 2,3$ and that i denote the imaginary unit. First we calculate $\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_2)$ and $\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_3)$. Clearly they are equal. By Lemma (2.29), choosing $n = (q-1)/2$ and $y = j$, we have

$$\begin{aligned}
&\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_2))\\
&= \frac{|C_4(j)|^2}{|G|}\left[\frac{1^3}{1} + \frac{1}{2}\cdot\frac{1}{q+1}\cdot 4\cdot\sum_{k=1}^{\frac{q-3}{2}}\cos^2(\frac{4jk\pi}{q-1})\right]\\
&= \frac{2q(q+1)}{q-1}\left[1 + \frac{2}{q+1}\left(\frac{q-1}{4} - \cos^2(2j\pi)\right)\right]\\
&= \frac{2q(q+1)}{q-1}\left[1 + \frac{2}{q+1}\cdot\frac{q-5}{4}\right]\\
&= \frac{2q(q+1)}{q-1}\cdot\frac{1}{2(q+1)}\left[3q-3\right]\\
&= 3q.
\end{aligned}$$

By Lemma (2.29), choosing $n = (q-1)/2$ and $y = 2j$ we have

$$\begin{aligned}
&\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(2j))\\
&= \frac{|C_4(j)|^2}{|G|}\left[\frac{1^3}{1} + \frac{1^3}{q} + \frac{1}{2}\cdot\frac{1}{q+1}\cdot 8\cdot\sum_{k=1}^{\frac{q-3}{2}}\cos^2(\frac{4jk\pi}{q-1})\cos(\frac{8jk\pi}{q-1})\right]\\
&= \frac{2q(q+1)}{q-1}\left[1 + \frac{1}{q} + \frac{4}{q+1}\left(\frac{q-1}{8} - \cos^2(2j\pi)\cos(4j\pi)\right)\right]\\
&= \frac{2q(q+1)}{q-1}\left[1 + \frac{1}{q} + \frac{q-9}{2(q+1)}\right]\\
&= \frac{2q(q+1)}{q-1}\cdot\frac{1}{2q(q+1)}\left[3q^2 - 5q + 2\right] = 3q-2.
\end{aligned}$$

Notice that we have $C_4(d_{4j}) = C_4(2j)$. Hence we have also

$$\mathrm{cmc}(C_4(j), C_4(j)^{-1}, C_4(d_{4j})) = 3q - 2.$$

Now we calculate $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_2)$ and $\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_3)$. Again they are clearly equal. By Lemma (2.29), choosing $n = (q+1)/2$ and $y = j$, we have

$$\begin{aligned}
&\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_2)) \\
&= \frac{|C_5(j)|^2}{|G|}\left[\frac{1^3}{1} + \frac{2}{q-1}(-\frac{1}{2} + \frac{1}{2}\sqrt{q}i - \frac{1}{2} - \frac{1}{2}\sqrt{q}i)\right. \\
&\qquad \left. + \frac{1}{2}\cdot\frac{1}{q-1}\cdot(-4)\cdot\sum_{\substack{1\le k\le\frac{q-1}{2}\\ k\neq\frac{q+1}{4}}}\cos^2(\frac{4jk\pi}{q+1})\right] \\
&= \frac{2q(q-1)}{q+1}\left[1 - \frac{2}{q-1} - \frac{2}{q-1}\left(\frac{q+1}{4} - \cos^2(j\pi) - \cos^2(2j\pi)\right)\right] \\
&= \frac{2q(q-1)}{q+1}\left[1 - \frac{2}{q-1} - \frac{2}{q-1}\cdot\frac{q-7}{4}\right] \\
&= \frac{2q(q-1)}{q+1}\cdot\frac{1}{2(q-1)}\left[q+1\right] \\
&= q.
\end{aligned}$$

By Lemma (2.29), choosing $n = (q+1)/2$ and $y = 2j$ we have

$$\begin{aligned}
&\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(2j)) \\
&= \frac{|C_5(j)|^2}{|G|}\left[\frac{1^3}{1} + \frac{(-1)^3}{q} + 2\cdot\frac{2}{q-1}\cdot(-(-1)^j)^2\cdot(-(-1)^{2j})\right. \\
&\qquad \left. + \frac{1}{2}\cdot\frac{1}{q-1}\cdot(-8)\cdot\sum_{\substack{1\le k\le\frac{q-1}{2}\\ k\neq\frac{q+1}{4}}}\cos^2(\frac{4jk\pi}{q-1})\cos(\frac{8jk\pi}{q-1})\right] \\
&= \frac{2q(q-1)}{q+1}\left[1 - \frac{1}{q} - \frac{4}{q-1}\right. \\
&\qquad \left. - \frac{4}{q+1}\left(\frac{q-1}{8} - \cos^2(j\pi)\cos(2j\pi) - \cos^2(2j\pi)\cos(4j\pi)\right)\right] \\
&= \frac{2q(q-1)}{q+1}\left[1 - \frac{1}{q} - \frac{4}{q-1} - \frac{q+1}{2(q-1)} + \frac{8}{q-1}\right] \\
&= \frac{2q(q-1)}{q+1}\cdot\frac{1}{2q(q-1)}\left[q^2+3q+2\right] \\
&= q+2.
\end{aligned}$$

Notice that we have $C_5(d_{5j}) = C_5(2j)$. Hence we have also

$$\mathrm{cmc}(C_5(j), C_5(j)^{-1}, C_5(d_{5j})) = q+2.$$

Last we have for $q \equiv -1 \pmod 8$

$$\begin{aligned}
&\operatorname{cmc}(C_5(\tfrac{q+1}{8}), C_5(\tfrac{q+1}{8})^{-1}, C_6) \\
&= \frac{|C_5(\frac{q+1}{8})|^2}{|G|} \left[\frac{1^3}{1} + \frac{(-1)^3}{q} + 2 \cdot \frac{(-(-1)^{\frac{q+1}{4}}) \cdot (-(-1)^{\frac{q+1}{8}})^2 \cdot 2}{q-1} \right. \\
&\quad \left. + \frac{1}{2} \cdot \frac{1}{q-1} \cdot (-8) \cdot \sum_{\substack{1 \le k \le \frac{q-1}{2} \\ k \neq \frac{q+1}{4}}} \underbrace{(-1)^k \cos(\frac{1}{2} k\pi)}_{\begin{cases} = 1 & k \text{ even} \\ = 0 & k \text{ odd} \end{cases}} \right] \\
&= \frac{2q(q-1)}{q+1} \left[1 - \frac{1}{q} - \frac{4}{q-1} - \frac{4}{q-1} \left(\frac{q-1}{4} - 1 \right) \right] \\
&= \frac{2q(q-1)}{q+1} \cdot \frac{1}{q(q-1)} \left[q+1 \right] \\
&= 2.
\end{aligned}$$

□

(2.33) Lemma
Let $q > 2$ be a power of 2 and m an integer in $\{1, \ldots, q/2\}$. Then $mq(q-1)+1$ does not divide $(q-1)q(q+1)$.

Proof. Suppose $mq(q-1)+1$ divides $(q-1)q(q+1)$. Since $mq(q-1)+1$ is odd we have $mq(q-1)+1$ divides $(q-1)(q+1) = q^2-1$. But for $m \geq 2$ we have $mq(q-1)+1 > q^2-1$, a contradiction. For $m = 1$ and $q > 2$ we have

$$\frac{1}{2}(q^2-1) < \frac{1}{2}q^2 + \underbrace{\frac{1}{2}q^2 - q + \frac{3}{2}}_{>0} - \frac{1}{2} = q(q-1) + 1 < q^2 - 1.$$

Hence $m = 1$ leads to a contradiction, too. □

(2.34) Lemma
Let q be an odd prime power and n with

$$n \in \left\{ \frac{q^2+1}{2}, \frac{q^2-q+2}{2}, q^2, \frac{2q^2-q+1}{2}, \frac{1}{2}q(3q-1) \right\}.$$

Then n divides $(q-1)q(q+1)/2$ if and only if $q = 3$ and $n = (q^2-q+2)/2 = 4$.

Proof. Suppose that $(q^2+1)/2$ divides $(q-1)q(q+1)/2$. Since q^2+1 and q are coprime we have q^2+1 divides q^2-1 which is a contradiction.
Suppose that $(q^2-q+2)/2$ divides $(q-1)q(q+1)/2$. Since q^2-q+2 and q are coprime we have q^2-q+2 divides q^2-1 which is a contradiction, since

$$\frac{1}{2}(q^2-1) < \frac{1}{2}q^2 + \underbrace{\frac{1}{2}q^2 - q + \frac{5}{2}}_{>0} - \frac{1}{2} = q(q-1) + 1 < q^2 - 1.$$

Clearly q^2 does not divide $(q-1)q(q+1)/2$.
Suppose that $(2q^2-q+1)/2$ divides $(q-1)q(q+1)/2$. Since $2q^2-q+1$ and q are coprime we have $2q^2-q+1$ divides q^2-1. But since $2q^2-q+1 > q^2-1$ this is a contradiction.
Suppose that $q(3q-1)/2$ divides $(q-1)q(q+1)/2$. Hence $3q-1$ divides q^2-1. We have

$$10 = (3q+1)(3q-1) - 9(q^2-1)$$

and so

$$\frac{10}{3q-1} = 3q+1-9\cdot \underbrace{\frac{q^2-1}{3q-1}}_{\in\mathbb{Z}} \in \mathbb{Z}.$$

For $q=2$ we have $3q-1=5 \mid 10$ but $3q-1=5 \nmid 3=q^2-1$. For $q=3$ we have $3q-1=8 \nmid 10$. For $q \geq 4$ we have $3q-1>10$ but this is a contradiction. $\square$

Chapter 3

A GAP-database of small RCC-Loops

A primary aim of this work is to provide a GAP database of small RCC loops up to isomorphism and to integrate the database into the GAP package LOOPS by Gábor P. Nagy and Petr Vojtěchovsky. We restrict the RCC loops database to non-associative RCC loops because all associative RCC loops are groups and the small groups are provided in the GAP database SMALL GROUPS. In this chapter we describe the computation of RCC loops by computing their envelopes. For more information about GAP see [Gap] and for more information about the package LOOPS see [NV15].

The RCC loops database lists exactly one representative of each isomorphism class of non-associative RCC loops of order at most 30. Let $\mathcal{L}$ be a non-associative RCC loop of order n. Without loss of generality we assume that $\mathcal{L}$ is equal to $\{1, \ldots, n\}$ as a set and that $1_{\mathcal{L}} = 1$. The right multiplication group $\mathrm{RM}(\mathcal{L})$ of $\mathcal{L}$ is transitive on n points, we have $\mathrm{RM}(\mathcal{L}) \leq \mathrm{Sym}(n)$. Moreover we showed in Lemma (1.16), that if $\mathcal{L}$ and $\mathcal{K}$ are isomorphic RCC loops on the set $\{1, \ldots n\}$, their right multiplication groups $\mathrm{RM}(\mathcal{L})$ and $\mathrm{RM}(\mathcal{K})$ are conjugate in $\mathrm{Sym}(n)$.

To classify the RCC loops on $\{1, \ldots, n\}$ up to isomorphism we need to consider each transitive group of degree n up to conjugacy in $\mathrm{Sym}(n)$. For $n \leq 30$ the GAP database TRANSITIVE GROUPS contains one representative of each conjugacy class of transitive subgroups of $\mathrm{Sym}(n)$ of degree n.

Recall that there is an equivalence between the categories $\mathbf{LP}_s$ of all loops together with all surjective loop homomorphisms and the category $\mathbf{EL}$ of all loop folders that are envelopes of a loop together with the surjective loop folder homomorphisms. Hence instead of computing all RCC loops of order n with $n \leq 30$ we compute all RCC loop folders $(G, H, T) \in \mathbf{EL}$ with $|(G, H, T)\lambda| = n$. For this we consider each group G of degree n in the GAP

database TRANSITIVE GROUPS in turn and since $1_{\mathcal{L}} = 1$ we set $H = \mathrm{Stab}_G(1)$. For the pair (G, H) we compute all right transversals T such that (G, H, T) is the envelope of an RCC loop. If no such T exists, G is not the right multiplication group of an RCC loop. Otherwise we obtain a list of RCC loop folders (G, H, T) which are envelopes of RCC loops. This list may still contain RCC loop folders describing isomorphic RCC loops. In a final step we reduce the list to contain exactly one RCC loop folder for each isomorphism class of RCC loops.

Recall that all loops and groups occurring in this thesis are finite.

3.1 An algorithm to compute envelopes of RCC loops

In this section we describe the algorithm COMPUTETT to compute all G-invariant right transversals T of H in G with $\langle T \rangle = G$ for a given group G and a subgroup $H \leq G$. Here we do not need to assume that $G \leq \mathrm{Sym}(n)$ and that $\mathrm{Core}_G(H) = \{1_G\}$.

(3.1) Definition
Let G be a group and $H \leq G$ be a subgroup of G. We define the set $TT(G, H)$ as the set of all subsets $T \subseteq G$ of G such that (G, H, T) is an RCC loop folder with $\langle T \rangle = G$.

(3.2) Remark
First we want to design an algorithm COMPUTETT which takes as input an arbitrary group G and a subgroup $H \leq G$ and computes the set $TT(G, H)$, i.e. all subsets T of G such that

(i) $1_G \in T$,

(ii) T is a union of conjugacy classes of G,

(iii) $|T| = [G : H]$,

(iv) for all $t_1, t_2 \in T$ we have $t_1 t_2^{-1} \in H$ if and only if $t_1 = t_2$ and

(v) $\langle T \rangle = G$.

In general, for a given subset $T \subseteq G$, it is an expensive computation to test condition (3.2)(iv). So we ensure that the algorithm COMPUTETT never violates this condition during the construction of T. As T is a union of conjugacy classes we make some remarks on conjugacy classes and their unions. Since $\{1_G\} \subseteq T$ we restrict ourselves to the non-trivial conjugacy classes. The following lemma shows which unions of conjugacy classes satisfy condition (3.2)(iv).

Let G be a group and $H \leq G$ be a subgroup of G. We set

- $C_1 = \{1_G\}$,
- $\mathcal{C}(G)$ to be the set of non-trivial conjugacy classes of G and
- $\mathcal{C}^H(G)$ to be the set of non-trivial conjugacy classes of G which contain an element of H.

Recall, see Chapter 2, page 22, the definition of the class multiplication coefficient $\mathrm{cmc}(K_1, K_2, K_3)$ of three conjugacy classes K_1, K_2, K_3 of G:

$$\mathrm{cmc}(K_1, K_2, K_3) = |\{(k_1, k_2) \mid k_1 \in K_1, k_2 \in K_2, k_1k_2 = k_3\}|$$

for a fixed $k_3 \in K_3$.

Let $U = \cup_{i=1}^{k} C_i$ be a union of conjugacy classes of G. If U contains a conjugacy class D of $\mathcal{C}^H(G)$ the set U contains at least two elements of H and we have $\mathrm{cmc}(D, C_1^{-1}, D) \neq 0$. Hence we can formulate Lemma (2.12) with the terms $\mathcal{C}(G)$ and $\mathcal{C}^H(G)$ as:

Lemma
Let G be a group and $H \leq G$ be a subgroup of G. Let $U = \cup_{i=1}^{k} C_i$ with $C_2, C_3, \ldots, C_k \in \mathcal{C}(G) \setminus \mathcal{C}^H(G)$. Then U contains at most one element of each right coset of H in G if and only if

$$\mathrm{cmc}(C_i, C_j^{-1}, D) = 0$$

for all $i, j \in \{1, \ldots, k\}$ and $D \in \mathcal{C}^H(G)$.

The algorithm ComputeTT performs a recursive search and constructs the set $TT(G, H)$ by attempting to extend an initial union of conjugacy classes to a transversal in $TT(G, H)$. In every step ComputeTT assumes it has already chosen a union of conjugacy classes satisfying conditions (3.2)(i), (ii) and (iv). The next aim is to extend this union by one further conjugacy class such that these conditions still hold. The previous lemma allows us to restrict the set of conjugacy classes which have to be considered for this extension.

In the very first step of the algorithm we only assume that the trivial conjugacy classes C_1 has been choosen as a subset of T. The following lemma determines the set of conjugacy classes to be considered in this first initial step.

(3.3) Lemma
Let G be a group and $H \leq G$ be a subgroup of G. Suppose there is an RCC *loop folder (G, H, T). Define the set $\mathcal{N}(G, H)$ of non-viable classes to be*

$$\mathcal{N}(G, H) = \{C \in \mathcal{C}(G) \mid \exists D \in \mathcal{C}^H(G) : \mathrm{cmc}(C, C^{-1}, D) \neq 0\}$$

and the set $\mathcal{P}(G,H)$ of possibly viable classes to be

$$\mathcal{P}(G,H) = \mathcal{C}(G) \setminus \left(\mathcal{C}^H(G) \cup \mathcal{N}(G,H)\right).$$

Then we have

$$T \subseteq \{1_G\} \cup \bigcup_{C \in \mathcal{P}(G,H)} C.$$

Proof. The set T is a right transversal of H in G. Hence it contains exactly one element of every right coset of H. Further T is a union of conjugacy classes. Since $\{1_G\} \subseteq T$, no conjugacy class of $\mathcal{C}^H(G)$ is a subset of T. Further, setting $C_i = C_j = C$ in Lemma (2.12), no conjugacy class C of G with

$$\mathrm{cmc}(C, C^{-1}, D) \neq 0$$

for some $D \in \mathcal{C}^H(G)$ is a subset of T. □

(3.4) Remark
Let G be a group and $H \leq G$ be a subgroup of G. Suppose there is an RCC loop folder (G,H,T). Since $C_1 \subseteq T$, no conjugacy class C of G with $|C| \geq [G:H]$ is a subset of T. Clearly we want to ensure that the algorithm ComputeTT never considers such conjugacy classes during the construction of $TT(G,H)$. Such conjugacy classes C lie in $\mathcal{N}(G,H) \cup \mathcal{C}^H(G)$, since such a C contains an element of H or two elements of the same coset of H in G. So if ComputeTT considers only the conjugacy classes of $\mathcal{P}(G,H)$ it will not consider such conjugacy classes C.
Notice that $\mathcal{N}(G,H)$ may also contain conjugacy classes C with $|C| < [G:H]$.

Lemma (3.3) identifies for a given group G and a subgroup $H \leq G$ the set $\mathcal{P}(G,H)$ of all conjugacy classes of G which have to be considered in the first step of the algorithm ComputeTT. It starts with the set $C_1 = \{1_G\}$ and extends it step by step with other conjugacy classes. Let $C_2, C_3 \in \mathcal{P}(G,H)$. Then $C_1 \cup C_2 \cup C_3$ and $C_1 \cup C_3 \cup C_2$ are equal as sets but are considered to be two different extensions. For performance purposes we do not want to consider this set twice. To avoid unnecessary repetitions during the execution of ComputeTT we do not consider a transversal $T \in TT(G,H)$ as set but as an ordered sequence of conjugacy classes with first element C_1 in the following sense.

(3.5) Remark
Let G be a group and $H \leq G$ be a subgroup of G. Let $r - 1 = |\mathcal{P}(G,H)|$. We label the conjugacy classes in $\mathcal{P}(G,H)$ by $2, \ldots, r$ and define the strict order $<$ by

$$C_1 < C_2 < \ldots < C_{r-1} < C_r.$$

An ordered sequence S with first element C_1 is a sequence

$$S = [C_1, C_{k_2}, C_{k_3}, \ldots, C_{k_s}]$$

for $s \leq r$ and $1 < k_2 < k_3 < \ldots < k_s \leq r$. Define $OS(G,H)$ as the set of all these ordered sequences with first element C_1. Then for all unions U of conjugacy classes with

$$U \subseteq \{1_G\} \cup \bigcup_{C \in \mathcal{P}(G,H)} C$$

there is exactly one $S \in OS(G,H)$ with $U = \cup_{C \in S} C$.
Let $S = [C_1, C_{k_2}, C_{k_3}, \ldots, C_{k_s}] \in OS(G,H)$ and let $C_{k_{s+1}}$ be an element of $\mathcal{P}(G,H)$ with $C_{k_s} < C_{k_{s+1}}$. We define the extension of S by $C_{k_{s+1}}$ as the ordered sequence $\tilde{S} \in OS(G,H)$ with

$$\tilde{S} = [C_1, C_{k_2}, C_{k_3}, \ldots, C_{k_s}, C_{k_{s+1}}].$$

Further we define an eligible ordered sequence S to be an element of $OS(G,H)$ such that $U = \cup_{C \in S} C$ satisfies the conditions (3.2)(i), (ii) and (iv). Hence for all $T \in TT(G,H)$ there is exactly one eligible ordered sequence $S \in OS(G,H)$ with $T = \cup_{C \in S} C$.

The algorithm ComputeTT uses $OS(G,H)$ to compute the set $TT(G,H)$. Since we consider the transversals in $TT(G,H)$ as sets the result $TT(G,H)$ of ComputeTT is independent of the chosen labeling of the conjugacy classes of $\mathcal{P}(G,H)$.

ComputeTT is a recursive algorithm which repeats a basic step. In this basic step the algorithm attempts to extend a given eligible ordered sequence S of $OS(G,H)$ by one further conjugacy class to an eligible ordered sequence $\tilde{S} \in OS(G,H)$.

The following lemma restricts the set $\mathcal{P}(G,H)$ to the set $\mathcal{P}(G,H,S)$ of conjugacy classes which have to be considered in such a subsequent step when an eligible ordered sequence $S \in OS(G,H)$ already has been chosen.

(3.6) Definition
Let G be a group and $H \leq G$ be a subgroup of G. For a conjugacy class $C \in \mathcal{P}(G,H)$ we define $\mathcal{N}(G,H,C)$ to be the set

$$\mathcal{N}(G,H,C) = \{\, K \in \mathcal{P}(G,H) | K \leq C \text{ or } \exists D \in \mathcal{C}^H(G) \text{ with } \mathrm{cmc}(C, K^{-1}, D) \neq 0 \,\}.$$

Let $S \in OS(G,H)$ be an eligible ordered sequence. We define $\mathcal{P}(G,H,S)$ to be the set

$$\mathcal{P}(G,H,S) = \mathcal{P}(G,H) \setminus \bigcup_{C \in S} \mathcal{N}(G,H,C).$$

(3.7) Lemma
Let G be a group and $H \leq G$ be a subgroup of G. Let

$$S = [C_1, C_{k_2}, C_{k_3}, \ldots, C_{k_s}] \in OS(G, H)$$

be an eligible ordered sequence and let $\tilde{S} \in OS(G, H)$ be the extension of S by one conjugacy class $C_{k_{s+1}}$, i.e.

$$\tilde{S} = [C_1, C_{k_2}, C_{k_3}, \ldots, C_{k_s}, C_{k_{s+1}}].$$

Then $\tilde{S}$ is an eligible ordered sequence if and only if $C_{k_{s+1}} \in \mathcal{P}(G, H, S)$. Note in particular if $U = \cup_{C \in S} C$ is a right transversal of H in G we have $\mathcal{P}(G, H, S) = \emptyset$.

Proof. Set $\tilde{U} = \cup_{C \in \tilde{S}} C$. By Lemma (2.12) $\tilde{U}$ contains at most one element of each right coset of H in G if and only if

$$\mathrm{cmc}(C, K^{-1}, D) = 0$$

for all $C, K \in \tilde{S}$ and $D \in \mathcal{C}^H(G)$. The conjugacy classes in S satisfy this condition by assumption. So $\tilde{U}$ satisfies condition (3.2)(iv) if and only if

$$\mathrm{cmc}(C, C_{k_{s+1}}^{-1}, D) = 0$$

for all $C \in S$ and $D \in \mathcal{C}^H(G)$. Since $\tilde{S} \in OS(G, H)$ we have that $C_{k_{s+1}} > C$ for all $C \in S$. Hence $\tilde{S}$ is an eligible ordered sequence if and only if

$$C_{k_{s+1}} \notin \bigcup_{C \in S} \mathcal{N}(G, H, C),$$

i.e. if and only if $C_{k_{s+1}} \in \mathcal{P}(G, H, S)$. □

During an initial computation the algorithm ComputeTT first computes the set $\mathcal{C}^H(G)$ of all conjugacy classes which contain an element of H, the set $\mathcal{P}(G, H)$ of all possibly viable conjugacy classes and for each conjugacy class $C \in \mathcal{P}(G, H)$ the set $\mathcal{N}(G, H, C)$ of all conjugacy classes non-viable for C. Then the algorithm calls a basic step which in turn calls itself recursively.
The basic step takes an eligible ordered sequence $S \in OS(G, H)$ and a set $P \subseteq \mathcal{P}(G, H, S)$ as input and returns the (possibly empty) set of all right transversals T with $\langle T \rangle = G$ and

$$\bigcup_{C \in S} C \subseteq T \subseteq \bigcup_{C \in S} C \cup \bigcup_{C \in P} C.$$

In particular, the returned right transversals have initial segment S and are extensions of S by conjugacy classes of P. The algorithm ComputeTT calls the basic step exactly once with $S = [C_1]$ and $P = \mathcal{P}(G, H)$, the set of all possibly viable conjugacy classes. This call ensures that all right transversals in $TT(G, H)$ are found as we will prove in Lemma (3.10).

At this point we describe how the basic step computes the set of all right transversals T with $\langle T\rangle = G$ and

$$\bigcup_{C\in S} C \subseteq T \subseteq \bigcup_{C\in S} C \cup \bigcup_{C\in P} C$$

for a fixed input S and P where $S \in OS(G,H)$ and $P \subseteq \mathcal{P}(G,H,S)$. Set $U = \cup_{C\in S} C$ and $V = \cup_{C\in P} C$.

The basic step starts with Test 1, which tests if there are enough elements in $U \cup V$ for a right transversal T of H in G with $U \subseteq T \subseteq U \cup V$. If not, the basic step returns $\emptyset$. This means, the algorithm ComputeTT returns to the previous level of the recursion as S cannot be extended by conjugacy classes in P to a right transversal of $TT(G,H)$.

If Test 1 does not abort the basic step, i.e. if we have $|U \cup V| \geq [G:H]$, we execute Test 2, which tests if $U \cup V$ generates the group G. If not, there is no right transversal T of H in G with $\langle T\rangle = G$ and $U \subseteq T \subseteq U \cup V$ and the basic step returns $\emptyset$. This means, the algorithm ComputeTT returns to the previous level of the recursion as S cannot be extended by conjugacy classes in P to a right transversal of $TT(G,H)$.

If these two tests do not abort the basic step, then, in particular, we have $\langle U \cup V\rangle = G$ and $|U \cup V| \geq [G:H]$. Now we disinguish between two cases of the given input P, namely $P = \emptyset$ and $P \neq \emptyset$.

In the first case S is no longer extendable. Since $P = \emptyset$ implies $V = \emptyset$ we have $\langle U\rangle = G$ and $|U| = [G:H]$. Hence U is a valid transversal in $TT(G,H)$. Clearly U is the only right transversal T with $\langle T\rangle = G$ and $U \subseteq T \subseteq U \cup V$. The basic step returns $\{U\}$.

In the second case, i.e. if $P \neq \emptyset$, the eligible ordered sequence S is extendable. We choose the smallest conjugacy class $C \in P$ in the order $<$. To find all right transversals with initial segment S satisfying the given properties we have to consider two subcases, namely to extend S by C or to skip C.

In the first subcase, the extend case, we define the extension $\tilde{S}$ of S by C. A recursive call to the basic step with $\tilde{S}$ and $\tilde{P} = P \setminus \mathcal{N}(G,H,C)$ returns the set TT_1 of all right transversals T with $\langle T\rangle = G$ and

$$\bigcup_{K\in\tilde{S}} K \subseteq T \subseteq \bigcup_{K\in\tilde{S}} K \cup \bigcup_{K\in\tilde{P}} K.$$

In particular such right transversals contain the conjugacy class C. Notice that, if $P = \mathcal{P}(G,H,S)$, we have $\tilde{P} = \mathcal{P}(G,H,\tilde{S})$.
In the second subcase, the skip case, we do not add C to S. A recursive call to the basic step with S and $\bar{P} = P \setminus C$ returns the set TT_2 of all right transversals T with $\langle T\rangle = G$ and

$$\bigcup_{K\in S} K \subseteq T \subseteq \bigcup_{K\in S} K \cup \bigcup_{K\in\bar{P}} K.$$

These right transversals do not contain C as such right transversals have been computed in the extend case.

Clearly $TT_1 \cup TT_2$ is the set of all right transversals T with $\langle T \rangle = G$ and $U \subseteq T \subseteq U \cup V$. The basic step returns $TT_1 \cup TT_2$.

(3.8) Algorithm
In pseudo code the basic step looks like follows:

BasicStep(S, P)

Input: S, P with $S \in OS$ and $P \subseteq \mathcal{P}(G, H, S)$
Output: the set of all right transversals T with $\langle T \rangle = G$ and
$\bigcup_{C \in S} C \subseteq T \subseteq \bigcup_{C \in S} C \cup \bigcup_{C \in P} C$

U:=$\bigcup_{C \in S} C$;
V:=$\bigcup_{C \in P} C$;

\# Test 1: Are there enough elements in $U \cup V$ for a transversal T;
if $|U \cup P| < [G : H]$ **then**
  \# U is not the beginning of a right transversal T;
  \# return to previous level and abandon this subroutine;
  return $\emptyset$
end

\# Test 2: Do U and V generate the group G;
if $\langle U \cup V \rangle < G$ **then**
  \# U is not the beginning of a right transversal T with $\langle T \rangle = G$;
  \# return to previous level and abandon this subroutine;
  return $\emptyset$
end

\# Case $P = \emptyset$;
if $P = \emptyset$ **then**
  \# U is a right transversal with $\langle U \rangle = G$;
  \# U is clearly the only right transversal with $U \subseteq U \subseteq U \cup V$;
  return $\{U\}$
end

\# Case $P \neq \emptyset$, the sequence S is extendable;
\# We now consider both cases namely to extend U by C and to skip C;
C:=Min(P);

Extend case;
$\tilde{S}$:=Add(S,C);
$\tilde{P}$:=$P \setminus \mathcal{N}(G, H, C)$;
TT_1:=**BasicStep**($\tilde{S}$, $\tilde{P}$);

Skip case;
$\bar{P}$:=$P \setminus \{C\}$;
TT_2:=**BasicStep**(S, $\bar{P}$);

return $TT_1 \cup TT_2$;

Algorithm: BasicStep

The overall algorithm ComputeTT starts with the computation of the sets $\mathcal{C}^H(G)$ of all conjugacy classes which contain an element of H, the set $\mathcal{P}(G, H)$ of all possibly viable conjugacy classes and the set $\mathcal{N}(G, H, C)$ of all conjugacy classes non-viable for C for each conjugacy class $C \in \mathcal{P}(G, H)$. After that it executes the basic step.

(3.9) Algorithm
In pseudo code the overall algorithm looks like follows:

ComputeTT(G, H)

Input: a group G, a subgroup H of G
Output: the set $TT(G, H)$

compute $\mathcal{C}^H(G)$;
compute $\mathcal{P}(G, H)$;
Now we compute the global variables $\mathcal{N}(G, H, C)$ for the basic step;
foreach $C \in \mathcal{P}(G, H)$ **do**
| compute $\mathcal{N}(G, H, C)$
end
TT:=**BasicStep**(C_1, $\mathcal{P}(G, H)$);

return TT;

Algorithm: ComputeTT

(3.10) Lemma
Let G be a group and $H \leq G$ be a subgroup of G. Then the algorithm ComputeTT *computes the set $TT(G, H)$.*

Proof. Clearly the result of ComputeTT is a subset of $TT(G, H)$. To show that ComputeTT computes all transversals in $TT(G, H)$ we show that ComputeTT calls the basic step with S and $\mathcal{P}(G, H, S)$ for each eligible ordered

sequences $S \in OS(G,H)$ at least once. We show this by induction on the length s of S. We show two base cases of the induction because the second one illustrates the idea of the proof.
If $s = 1$ then $S = [C_1]$. Since ComputeTT starts the recursion with S and $\mathcal{P}(G,H,S) = \mathcal{P}(G,H)$, the basic step is called with them.
For $s = 2$ set $\tilde{S} = [C_1, C_j]$ with $C_j \in \mathcal{P}(G,H)$. The set $\{C_1\} \cup \mathcal{P}(G,H)$ is strictly ordered and C_j is the jth element in this order. ComputeTT starts with the sequence $S = [C_1]$ and the set $\mathcal{P}(G,H,S) = \mathcal{P}(G,H)$. After ComputeTT skipped the first $(j-1)$ elements in $\mathcal{P}(G,H)$, see the skip case in BasicStep, it calls the basic step with the sequence $S = [C_1]$ and the set

$$P = (\ldots((\mathcal{P}(G,H) \setminus \{C_2\}) \setminus \{C_3\})\ldots) \setminus \{C_{j-1}\} = \{C_k \mid k \geq j\}.$$

The conjugacy class C_j is now the smallest element of P. So the call to BasicStep(S, P) extends $S = [C_1]$ by C_j to $\tilde{S} = [C_1, C_j]$ and set

$$\tilde{P} = P \setminus \mathcal{N}(G,H,C_j) = \mathcal{P}(G,H) \setminus (\{C_k \mid k < j\} \cup \mathcal{N}(G,H,C_j)).$$

By definition we have $\{C_k \mid k < j\} \subseteq \mathcal{N}(G,H,C_j)$ and hence

$$\tilde{P} = \mathcal{P}(G,H) \setminus \mathcal{N}(G,H,C_j) = \mathcal{P}(G,H,[C_1,C_j]) = \mathcal{P}(G,H,\tilde{S}).$$

Then it calls BasicStep($\tilde{S}$, $\mathcal{P}(G,H,\tilde{S})$).
Suppose ComputeTT calls BasicStep(S, $\mathcal{P}(G,H,S)$) for all eligible ordered sequences S of length s at least once. Let $\tilde{S}$ be an eligible ordered sequence of length $s+1$,

$$\tilde{S} = [C_1, C_{k_2}, C_{k_3}, \ldots, C_{k_s}, C_{k_{s+1}}].$$

Let S be the eligible ordered sequence of length s such that $\tilde{S}$ is the extension of S by $C_{k_{s+1}}$, i.e.

$$S = [C_1, C_{k_2}, C_{k_3}, \ldots, C_{k_s}].$$

By our induction hypothesis ComputeTT calls the basic step with S and $\mathcal{P}(G,H,S)$.
Since $\tilde{S}$ is an eligible ordered sequence we have $C_{k_{s+1}} \in \mathcal{P}(G,H,S)$. The set $\mathcal{P}(G,H,S)$ is strictly ordered. Let $C_{k_{s+1}}$ be the jth element in $\mathcal{P}(G,H,S)$. After ComputeTT skipped the first $(j-1)$ elements in $\mathcal{P}(G,H,S)$, see the skip case in BasicStep, it calls the basic step with the sequence S and the set

$$P = \mathcal{P}(G,H,S) \setminus \{K \mid C_{k_s} < K < C_{k_{s+1}}\}.$$

The conjugacy class $C_{k_{s+1}}$ is now the smallest element of P. So the call to BasicStep(S, P) extends S by $C_{k_{s+1}}$ to $\tilde{S}$ and calls the basic step recursively with $\tilde{S}$ and

$$\tilde{P} = P \setminus \mathcal{N}(G,H,C_{k_{s+1}}).$$

By definition we have $\{K \mid C_{k_s} < K < C_{k_{s+1}}\} \subseteq \mathcal{N}(G,H,C_{k_{s+1}})$ and hence

$$\tilde{P} = \mathcal{P}(G,H,S) \setminus \mathcal{N}(G,H,C_{k_{s+1}}) = \mathcal{P}(G,H,\tilde{S}). \qquad \square$$

(3.11) Remark
The algorithm computes for a given group G and a subgroup $H \leq G$ the set $TT(G,H)$. By Remark (1.32), for each $T \in TT(G,H)$ the triple (G,H,T) is the envelope of an RCC loop if and only if $\mathrm{Core}_G(H) = \{1_G\}$.

3.2 The computation of small RCC loops

We employ algorithm ComputeTT to compute the envelopes of all non-associative RCC loops of order n with $n \leq 30$. As we noticed in the introduction of this chapter without loss of generality we may assume that $\mathcal{L}$ is equal to $\{1,\ldots,n\}$ as a set and that $1_{\mathcal{L}} = 1$. Therefore the right multiplication group of such an RCC loop occurs in the Gap database Transitive Groups. The following remark gives some information about this database.

(3.12) Remark
The Gap database Transitive Groups contains representatives of all transitive (permutation) groups of degree at most 30. All groups of degree n are given as subgroups of $\mathrm{Sym}(n)$. Two transitive groups of the same degree n are considered to be equivalent, if they are conjugate in the full symmetric group $\mathrm{Sym}(n)$. So the isomorphism type of the group Sym(4) occurs once with degree 4 and twice with degree 6.

Hence, to compute the non-associative RCC loops of order n we restrict the computation to the groups of degree n. Further we recall Lemma (1.16):

Lemma
Let $\mathcal{L}$ and $\mathcal{K}$ be two isomorphic loops and $\varphi : \mathcal{L} \mapsto \mathcal{K}$ a loop isomorphism. Let $(G,H,T) := \mathcal{L}\varepsilon$. Then we have $\varphi^{-1}G\varphi \leq \mathrm{Sym}(\mathcal{K})$ and

$$(\varphi^{-1}G\varphi, \varphi^{-1}H\varphi, \varphi^{-1}T\varphi) = \mathcal{K}\varepsilon.$$

So, if $\mathcal{L}$ and $\mathcal{K}$ are (arbitrary) isomorphic loops on the set $\{1,\ldots,n\}$ their right multiplication groups $\mathrm{RM}(\mathcal{L})$ and $\mathrm{RM}(\mathcal{K})$ are conjugate in $\mathrm{Sym}(n)$. This equates exactly to the definition of equivalence used in the Gap database Transitive Groups. Hence we restrict the computation to the groups in the database. For the computation we have to consider each group in the database once. Two loops arising from two different groups in the database are never isomorphic even if these two groups are isomorphic.

Recall that all loops of order less than five and all RCC loops of prime order are associative and hence groups. So from now on let

$$n \in \{6,8,9,10,12,14,15,16,18,20,21,22,24,25,26,27,28,30\}.$$

We want to compute all RCC loop folders (G, H, T) with a group G of degree n in the GAP database TRANSITIVE GROUPS and $H = \mathrm{Stab}_G(1)$ which are envelopes of a non-associative RCC loop of order n. First we eliminate all transitive groups of degree n which are clearly not right multiplication groups of a non-associative RCC loop.

Recall Remark (1.35): The envelope of a loop is a trivial loop foolder if and only if the loop is a group. If G is a group of degree n in the GAP database TRANSITIVE GROUPS and $H = \mathrm{Stab}_G(1)$ we have $|T| = n \neq 1$. Hence the computed RCC loop folders (G, H, T) leads to non-associative RCC loops if and only if $|H| \neq 1$.

Recall that $\mathcal{P}(G, H)$ is the set of all possibly viable conjugacy classes. The computation of $\mathcal{P}(G, H)$ in GAP uses the character table of G to determine the class multiplication coefficients, see Lemma (2.12). As this is only feasible for relatively small groups, we avoid the computation of $\mathcal{P}(G, H)$ and compute a slightly larger set $\mathcal{Q}(G, H)$ instead. Define $\mathcal{Q}(G, H)$ to be the set

$$\mathcal{Q}(G, H) = \{C \in \mathcal{C}(G) |\ |C| < [G : H] \text{ and } C \notin \mathcal{C}^H(G)\}.$$

We have $\mathcal{P}(G, H) \subseteq \mathcal{Q}(G, H)$, see Remark (3.4). So if there is an RCC loop folder (G, H, T) by Lemma (3.3) we have

$$T \subseteq C_1 \cup \bigcup_{C \in \mathcal{Q}(G,H)} C.$$

(3.13) Lemma
Let G be a transitive group, $G \leq \mathrm{Sym}(n)$ and $H = \mathrm{Stab}_G(1)$. If one of the following conditions is satisfied

(i) $|H| = 1$,

(ii) G *is abelian,*

(iii) $N_G(H) \neq H \cdot C_G(H)$,

(iv) $\langle C \mid C \in \mathcal{Q}(G, H)\rangle \neq G$ *or*

(v) there is no subset $\{C_{k_2}, C_{k_3}, \ldots, C_{k_s}\}$ *of* $\mathcal{Q}(G, H)$ *with* $|\cup_{i=1}^{s} C_{k_i}| + 1$ *divides the order of* G,

then there is no RCC *loop folder* (G, H, T) *which is the envelope of a non-associative* RCC *loop.*

Proof. The first three items are Remark (1.35), Lemma (1.34) and Lemma (2.7). The last two items are just the fact that $\langle T\rangle = G$, $C_1 \subseteq T$ and

$$T \subseteq C_1 \cup \bigcup_{C \in \mathcal{Q}(G,H)} C.$$ □

For each group G of degree n in the GAP database TRANSITIVE GROUPS we set $H = \mathrm{Stab}_G(1)$ and test first if the group G satisfies one of the conditions of Lemma (3.13). If G is not eliminated by this lemma we compute the set $TT(G,H)$ with algorithm COMPUTETT. If $TT(G,H)$ is not empty, G is the right multiplication group of an RCC loop of order n and for each $T \in TT(G,H)$ the loop folder (G,H,T) is the envelope of an RCC loop. Since G was not eliminated by Lemma (3.13) we have $|H| \neq 1$ and since $|T| = n$ we have $|T| \neq 1$. Hence for each right transversal $T \in TT(G,H)$ the RCC loop folder (G,H,T) is not trivial and by Remark (1.35) the RCC loop $(G,H,T)\lambda$ is non-associative.
For a given group G and $H = \mathrm{Stab}_G(1)$ the size of the set $TT(G,H)$ may be very large, e.g. for the group identified as TRANSITIVEGROUP$(28,47)$ we have $|TT(G,H)| = 7\ 712\ 194$. So the next step is to determine one RCC loop for each isomorphism class of RCC loops.

Let G be a transitive group of degree n and $H = \mathrm{Stab}_G(1)$. Let (G,H,T_1) and (G,H,T_2) be two RCC loop folders which are envelopes of RCC loops and $\mathcal{L} = (G,H,T_1)\lambda$ and $\mathcal{K} = (G,H,T_2)\lambda$. As we have seen in Lemma (1.16) and Lemma (1.21) the two RCC loops $\mathcal{L}$ and $\mathcal{K}$ are isomorphic if and only if there is a $\varphi \in \mathrm{Sym}(n)$ with

$$G = \varphi^{-1}G\varphi, \quad H = \varphi^{-1}H\varphi \quad \text{and} \quad T_2 = \varphi^{-1}T_1\varphi.$$

Hence $\mathcal{L}$ and $\mathcal{K}$ are isomorphic if and only if there is a $\varphi \in \mathrm{Sym}(n)$ with

$$\varphi \in N_{\mathrm{Sym}(n)}(G) \cap N_{\mathrm{Sym}(n)}(H) = N_{N_{\mathrm{Sym}(n)}(G)}(H)$$

and $T_2 = \varphi^{-1}T_1\varphi$.

To compute the isomorphism classes of RCC loops with right multiplication group G we have to compute the orbits of the set $TT(G,H)$ under the action of the group

$$N = N_{N_{\mathrm{Sym}(n)}(G)}(H).$$

As φ is an automorphism of G it maps conjugacy classes to conjugacy classes. So we do not consider the action of N on a transversal as a whole but as an ordered sequence of conjugacy classes. This offers a very fast computation of the orbits of N on $TT(G,H)$ in GAP.

(3.14) Remark
Table 3.1 records for every n the number nr_{RM} of groups of degree n which are the right multiplication group of an RCC loop, the number nr_{RCC} of non-isomorphic, non-associative RCC loops of order n and — for comparison — the number nr_{gr} of groups of order n.

Table 3.1: The number of non-associative RCC loops of order n

n	nr_{RM}	nr_{RCC}	nr_{gr}	n	nr_{RM}	nr_{RCC}	nr_{gr}
6	1	3	2	20	21	8 248	5
8	7	19	5	21	7	119	2
9	3	5	2	22	3	10 487	2
10	2	16	2	24	152	471 995	15
12	16	155	5	25	4	119	2
14	3	97	2	26	5	151 971	2
15	4	17	1	27	33	152 701	5
16	110	6 317	14	28	21	1 452 645	4
18	23	1 901	5	30	26	4 611 926	4

In Appendix A the GAP code of the algorithm ComputeTT and the code for the computation of the small RCC loops is described. If the transitive group G of degree n is of large order, usually most conjugacy classes of G have a size larger than n. Hence we can eliminate most of these groups by Lemma (3.13), condition (iv) or (v). But almost all groups of small order do satisfy these conditions. So we only execute this test when the order of G has reached a certain size.

Further, for $n \in \{6, 8, 9, 10, 12, 14, 15, 21\}$ we give in Appendix B the Gap database numbers of the groups G in Transitive Groups which are right multiplication groups of an RCC loop of order n, the isomorphism class of G, the order of $TT(G, H)$ where $H = \mathrm{Stab}_G(1)$ and the number of isomorphism classes of RCC loops corresponding to this group.

A GAP database of the isomorphism classes of non-associative RCC loops is published in the Gap package Loops by G. Nagy and P. Vojtěchovsky. Since there are so many non-associative RCC loops of order 28 or 30 only the non-associative RCC loops of order n with $n \leq 27$ are integrated in the GAP package Loops. The data of the RCC loops of order n with $n \in \{28, 30\}$ is available in the files published with this thesis.

Chapter 4

On the primitive action of right multiplication groups of RCC loops of order p_1p_2

In this chapter let p_1 and p_2 always be two different primes with $p_1 < p_2$. Let $\mathcal{L}$ be a non-associative RCC loop of order p_1p_2 and let (G, H, T) be the envelope of $\mathcal{L}$. As G is the right multiplication group of $\mathcal{L}$, it acts transitively on the p_1p_2 right cosets $\{Ht \mid t \in T\}$ of H in G. In this chapter we show that this action is imprimitive. Further, we give for each odd prime p_2 a group G which is the right multiplication group of a non-associative RCC loop of order $2p_2$.

Suppose G acts primitively on $\{Ht \mid t \in T\}$. We show first that in this case G is almost simple. In [LS03] Cai Heng Li and Ákos Seress classify the socle of almost simple primitive groups of squarefree degree. Referring to this paper we determine those cases where the degree of the action can possibly be p_1p_2. After that we show that these groups, which act primitively on p_1p_2 points, are not right multiplication groups of RCC loops of order p_1p_2.

Recall that the socle of a group G, denoted by $\mathrm{soc}(G)$, is the subgroup generated by the minimal normal subgroups of G. Further recall the O'Nan-Scott Theorem, see [DM96, Th. 4.1A].

Theorem (O'Nan-Scott Theorem)
Let G be a finite primitive group of degree n and denote the socle of G by $\mathrm{soc}(G)$. Then either case (i) or (ii) holds where

(i) $\mathrm{soc}(G)$ *is a regular elementary abelian r-group for some prime r and $n = r^m$ where r^m is the order of* $\mathrm{soc}(G)$*. Further G is isomorphic to a subgroup of the affine group* $\mathrm{AGL}(m, r)$*.*

(ii) $\mathrm{soc}(G)$ *is isomorphic to a direct power S^m of a non-abelian simple group*

S and one of the following holds:

(a) $m = 1$ and G is isomorphic to a subgroup of $\mathrm{Aut}(S)$, i.e. G is almost simple,

(b) $m \geq 2$ and G is a group of diagonal type with $n = |S|^{m-1}$,

(c) $m \geq 2$ and for some proper divisor d of m and some primitive group U with a socle isomorphic to S^d, the group G is isomorphic to a subgroup of the wreath product $U \wr \mathrm{Sym}(m/d)$ with the product action, and $n = l^{m/d}$ where l denotes the degree of U,

(d) $m \geq 6$, the socle $\mathrm{soc}(G)$ of G is regular and $n = |S|^m$.

(4.1) Lemma
Let p_1 and p_2 be two different primes with $p_1 < p_2$. Let $\mathcal{L}$ be a non-associative RCC *loop of order p_1p_2 and let (G, H, T) be the envelope of $\mathcal{L}$. Suppose that G acts primitively on $\{Ht \mid t \in T\}$. Then G is almost simple.*

Proof. The degree of G is p_1p_2. We peruse the cases of the O'Nan-Scott Theorem:
Suppose that Case (i) holds. Then $\mathrm{soc}(G)$ is an elementary abelian r-group for some prime r with $p_1p_2 = r^m$. Clearly this is a contradiction.
Case (ii)(a) is the statment of the lemma.
Suppose that Case (ii)(b) holds. Then $m \geq 2$ and $p_1p_2 = |S|^{m-1}$. Thus we have $m = 2$ and S is a simple group of order p_1p_2. But by Sylow's Theorem a group of order p_1p_2 is not simple. So this is a contradiction, too.
Suppose that Case (ii)(c) holds. Then we have $p_1p_2 = l^{m/d}$. Since d is a proper divisor of m we have $m/d > 1$ and $l^{m/d}$ is not squarefree whereas p_1p_2 is squarefree. So this is a contradiction.
Suppose that Case (ii)(d) holds. Then we have $m \geq 6$ and $p_1p_2 = |S|^m$. Clearly $|S|^m$ is not squarefree for $m \geq 6$ so this is a contradiction, too. □

(4.2) Assumption
Let p_1 and p_2 be two different primes with $p_1 < p_2$. Let $\mathcal{L}$ be a non-associative RCC loop of order p_1p_2 and let (G, H, T) be the envelope of $\mathcal{L}$. Suppose that G acts primitively on $\{Ht \mid t \in T\}$ and G is almost simple with socle S.

(4.3) Lemma
Suppose that assumption (4.2) holds. Then the socle of G is not an alternating group.

Proof. Suppose the socle S of G is an alternating group. Table 1 of [LS03] lists those socles of primitive groups of squarefree degree which are isomorphic to an alternating group. The following line numbers refer to this table.

Consider the case of Line 1. Then $S \cong \mathrm{Alt}(c)$ and since S is a simple group we have $c \geq 5$. In this case S acts on the set of subsets with k elements (k-sets) of

$\{1, \ldots, c\}$ for some $1 \leq k < c$. The degree of this action is $\binom{c}{k}$, so $p_1p_2 = \binom{c}{k}$. By Lemma (4.16) we know that there are exactly three cases where $\binom{c}{k}$ is the product of two different primes:

(i) $c = p_1p_2$, $k \in \{1, c-1\}$ and $\binom{c}{k} = c$,

(ii) (a) $c = p_2$ is odd, $p_1 = (p_2 - 1)/2$, $k \in \{2, c-2\}$ and $\binom{c}{k} = c(c-1)/2$,
(b) $c = p_2+1$ is even, $p_1 = (p_2+1)/2$, $k \in \{2, c-2\}$ and $\binom{c}{k} = c(c-1)/2$,

(iii) $c = 7$, $k \in \{3, 4\}$ and $\binom{c}{k} = 35 = 5 \cdot 7$.

In Case (iii) we have $S \cong \mathrm{Alt}(7)$ and so $G \cong \mathrm{Alt}(7)$ or $G \cong \mathrm{Sym}(7)$. By Lemma (4.18) neither Alt(7) nor Sym(7) is the right multiplication group of an RCC loop of order 35. Suppose that one of the cases (i) or (ii) holds. Then $S \cong \mathrm{Alt}(c)$ with $c \geq 5$. Recall $S \leq G \leq \mathrm{Aut}(S)$. Hence we have $G \cong \mathrm{Alt}(c)$, $G \cong \mathrm{Sym}(c)$ or $G \cong \mathrm{Aut}(\mathrm{Alt}(6)) = \mathrm{Sym}(6).2$. Further the degree of the action of G and hence the length of the transversal T is less than or equal to $c(c-1)/2$. By Lemma (4.17) each non-trivial conjugacy class of one of these groups has size greater than $c(c-1)/2$. Since T is a union of conjugacy classes with $\{1_G\} \subseteq T$ and $|T| = p_1p_2$, this is a contradiction.

In Line 2 the degree of the group G is $105 = 3 \cdot 5 \cdot 7$ so this case contradicts our assumption.

In Lines 3, 5, 6 and 7, the degrees of the group G are 15 or 6. Hence the order of $\mathcal{L}$ is 15 or 6. In these cases the socle of G is isomorphic to an alternating group $\mathrm{Alt}(k)$ with $k \in \{5, 6, 7, 8\}$. But the right multiplication groups of the RCC loops of order 15 and order 6 are known (see Appendix B) and none of these groups contains a subgroup isomorphic to an alternating group $\mathrm{Alt}(k)$ with $k \in \{5, 6, 7, 8\}$.

Suppose the case of Line 4. Then $S \cong \mathrm{Alt}(2a)$ with $a \in \{3, 4, 6, 9, 10, 12, 36\}$ acting on $\Pi(a, 2)$, where $\Pi(a, 2)$ denotes the set of partitions of $\{1, \ldots, 2a\}$ into two sets of size a. The degree of this action is $\frac{1}{2}\binom{2a}{a}$. For any a as above the degree is equal to the product of two different primes if and only if $a \in \{3, 4\}$. If $a = 3$ then $p_1p_2 = 10$. But the right multiplication groups of RCC loops of order 10 are known (see Appendix B) and none of these groups contains a subgroup isomorphic to Alt(6). If $a = 4$ then $p_1p_2 = 35$ and the socle S of G is isomorphic to Alt(8). So G is isomorphic to Alt(8) or to Sym(8). But, by Lemma (4.18), neither Alt(8) nor Sym(8) is the right multiplication group of an RCC loop of order 35. Hence the socle S of G is not an alternating group. □

(4.4) Lemma
Suppose assumption (4.2) holds. Then the socle of G is not a sporadic group.

Proof. Suppose that the socle of G is a sporadic group. Table 2 of [LS03] lists those socles of primitive groups of squarefree degree which are isomorphic to a sporadic group. The following line numbers refer to this table.
Only in the cases of Lines 2, 5, 6 and 10, the degree of the primitive action is equal to the product of two different primes. So if S is the socle of G we have:

(i) $S \cong M_{11}$ and $p_1p_2 = 5 \cdot 11$,

(ii) $S \cong M_{22}$ and $p_1p_2 = 2 \cdot 11$,

(iii) $S \cong M_{22}$ and $p_1p_2 = 7 \cdot 11$,

(iv) $S \cong M_{23}$ and $p_1p_2 = 11 \cdot 23$.

The Mathieu groups themselves, their subgroups and automorphism groups are well known. The outer automorphism groups of M_{11} and M_{23} are trivial so in Case (i) we have $G \cong M_{11}$ and in Case (iv) we have $G \cong M_{23}$. In Cases (ii) and (iii) we have $G \cong M_{22}$ or $G \cong M_{22}.2$. By Theorem (2.15) there is no RCC loop folder (G, H, T) with $G \in \{M_{11}, M_{22}, M_{23}\}$. So only the cases $G \cong M_{22}.2$ with $p_1p_2 = 22$ and $G \cong M_{22}.2$ with $p_1p_2 = 77$ remain. But, by Lemma (4.18), $G \cong M_{22}.2$ is neither the right multiplication group of an RCC loop of order 22 nor of one of order 77. Hence the socle S of G is not a sporadic group. □

(4.5) Lemma
Suppose assumption (4.2) holds. If G has an exceptional socle S, then S is isomorphic to the Suzuki group ${}^2B_2(q)$ with $q = 2^{2m+1} > 2$, $p_1 = 5$ and $5p_2 = q^2 + 1$.

Proof. Suppose that the socle S of G is an exceptional group. Table 4 of [LS03] lists those socles of primitive groups of squarefree degree which are isomorphic to an exceptional group. The following line numbers refer to this table. Denote the degree of the primitive action by n as in this table. We want to determine the groups where $n = p_1p_2$.

Suppose that the case of Line 1 holds. Then the socle S is isomorphic to ${}^2B_2(q)$ with $q = 2^{2m+1}$ and $n = q^2 + 1$. Since ${}^2B_2(2)$ is not simple we have $q = 2^{2m+1} > 2$. Further, 5 divides $n = 4^{2m+1} + 1$ for all $m \geq 1$ and hence $p_1 = 5$. This case is listed in the lemma.

Consider the case of Line 2. Then we have $S \cong G_2(q)$ and

$$n = (q + 1)(q^4 + q^2 + 1).$$

If q is odd then $q + 1$ is not prime. If q is even and $q + 1$ is prime, we have $q = 2^{2^f}$, $f \geq 0$. But then we have

$$q^4 + q^2 + 1 = 16^{2^f} + 4^{2^f} + 1 \equiv 3 \cdot 1 \equiv 0 \pmod 3.$$

Since $q^4+q^2+1>3$, this is not prime and hence n is not the product of two different primes.

Suppose the case of Line 3. Then we have $S \cong {}^3D_4(q)$ and

$$n=(q+1)(q^8+q^4+1).$$

Hence we have again $q=2^{2^f}$, $f \geq 0$. But then we have

$$q^8+q^4+1=256^{2^f}+16^{2^f}+1 \equiv 3 \cdot 1 \equiv 0 \pmod 3.$$

Since $q^8+q^4+1>3$, this is not prime and hence n is not the product of two different primes.

Consider the case of Line 4. Then we have $S \cong F_4(q)$ with $q=4^e$, $e \geq 1$ and

$$n=(q^{12}-1)(q^4+1)/(q-1)=(q^{11}+q^{10}+\ldots+q+1)(q^4+1).$$

We have

$$(q^{11}+q^{10}+\ldots+q+1)=4^{11e}+4^{10e}+\ldots+4^e+1 \equiv 12 \cdot 1 \equiv 0 \pmod 3.$$

Since $q^{11}+q^{10}+\ldots+q+1>3$, this is not prime and hence n is not the product of two different primes.

Suppose the case of Line 5. Then we have $S \cong {}^2E_6(q)$ with $q=4^e$, $e \geq 1$ and

$$\begin{aligned} n &= (q^{12}-1)(q^4+1)(q^6-q^3+1)/(q-1) \\ &= (q^{11}+q^{10}+\ldots+q+1)(q^4+1)(q^6-q^3+1). \end{aligned}$$

Since $q \geq 4$, each of these three factors is greater than 1. Hence n is not the product of two different primes.

Consider last the case of Line 6. Then we have $S \cong E_7(q)$ and

$$n=\frac{q^{18}-1}{q^2-1} \cdot \frac{q^{14}-1}{q-1} \cdot (q^4-q^2+1)$$

Since $q \geq 2$, each of these three factors is greater than 1. Hence n is not the product of two different primes. □

In the next lemma we examine the almost simple groups whose socle is a classical group and show which of these groups acts primitively on a set of p_1p_2 points. For this we recall the definition of a primitive prime divisor: Let $q,m \in \mathbb{N}$. A primitive prime divisor r of q^m-1 is a prime r which divides q^m-1 and which does not divide q^k-1 with $1 \leq k < m$. In [Zsi92, Sec. XII] Karl Zsigmondy showed for which numbers q and m such a primitive prime divisor exists. We recall his theorem:

Theorem (Zsigmondy's Theorem)
There is a prime r which divides $q^m - 1$ and which does not divide $q^k - 1$ with $1 \leq k < m$ execpt for

- $m = 1$,
- $m = 2$ *and* $q + 1$ *is a power of* 2,
- $m = 6$ *and* $q = 2$.

(4.6) Lemma
Suppose assumption (4.2) holds. Suppose that G has a classical socle S. Then one of the following holds:

(i) $S \cong \mathrm{PSL}(m, q)$ *and* $p_1p_2 = (q^m - 1)/(q - 1)$,

(ii) $S \cong \mathrm{PSL}(5, 2)$ *and* $p_1p_2 = 5 \cdot 31$,

(iii) $S \cong \mathrm{PSL}(4, 2)$ *and* $p_1p_2 = 5 \cdot 7$,

(iv) $S \cong \mathrm{PSL}(2, p_2)$ *and* $p_1 = (p_2 \pm 1)/2$,

(v) $S \cong \mathrm{PSL}(2, p_1^2)$ *and* $p_2 = (p_1^2 + 1)/2$,

(vi) $S \cong \mathrm{PSL}(2, p_2)$ *and*

$$p_1p_2 \in \{5 \cdot 11, 7 \cdot 13, 3 \cdot 19, 11 \cdot 23, 7 \cdot 29, 29 \cdot 59, 31 \cdot 61\},$$

(vii) $S \cong \mathrm{PSU}(3, q)$ *with* $q = 2^{2^f}$, $f \geq 1$ *and* $p_1p_2 = (q + 1)(q^2 - q + 1)$,

(viii) $S \cong \mathrm{PSp}(4, q)$ *with* $q = 2^{2^f}$, $f \geq 1$ *and* $p_1p_2 = (q + 1)(q^2 + 1)$,

(ix) $S \cong \mathrm{P}\Omega^-(2m, q)$ *with* $q = 2^{2^f}$, $m = 2^e$, $e \geq 2$ *and*

$$p_1p_2 = (q^m + 1)(q^{m-1} - 1/(q - 1)),$$

(x) $S \cong \mathrm{P}\Omega^+(2m, q)$ *with* $q = 2^{2^f}$, $m = 2^e + 1$, $e \geq 1$ *and*

$$p_1p_2 = (q^{m-1} + 1)(q^m - 1)/(q - 1).$$

Proof. Suppose that the socle S of G is a classical group. Table 3 of [LS03] lists those socles of primitive groups of squarefree degree which are isomorphic to a classical group. The following line numbers refer to this table. Denote the degree of the primitive action by n as in this table or by n_k if we want to emphasize the dependence of n on k. We want to determine the groups where the degree is equal to p_1p_2.

Suppose the case of Line 1. Then we have $S \cong \mathrm{PSL}(m, q)$ and

$$n_k = \prod_{i=0}^{k-1} (q^{m-i} - 1) / \prod_{i=1}^{k} (q^i - 1)$$

with $1 \leq k < m$. Notice that

$$\prod_{i=k+1}^{m-k}(q^i-1) = \prod_{i=k+1}^{m-k}(q^{m-(m-i)})-1 = \prod_{j=k}^{m-k-1}(q^{m-j}-1).$$

Hence we have

$$\begin{aligned}
n_k &= \frac{\prod_{i=0}^{k-1}(q^{m-i}-1)}{\prod_{i=1}^{k}(q^i-1)} \\
&= \frac{\prod_{i=0}^{k-1}(q^{m-i}-1)}{\prod_{i=1}^{k}(q^i-1)} \cdot \frac{\prod_{i=k+1}^{m-k}(q^i-1)}{\prod_{i=k+1}^{m-k}(q^i-1)} \\
&= \frac{\prod_{i=0}^{k-1}(q^{m-i}-1)\cdot\prod_{j=k}^{m-k-1}(q^{m-j}-1)}{\prod_{i=1}^{k}(q^i-1)\cdot\prod_{i=k+1}^{m-k}(q^i-1)} \\
&= \frac{\prod_{i=0}^{m-k-1}(q^{m-i}-1)}{\prod_{i=1}^{m-k}(q^i-1)} \\
&= n_{m-k}.
\end{aligned}$$

Hence, for reasons of symmetry, it suffices to consider the integers k with $1 \leq k \leq m/2$. Thus the exponents $m-i$ of q in every term $q^{m-i}-1$ in the numerator of n_k are greater than each of the exponents i of q in every term q^i-1 in the denominator of n_k as $m-i > m-(k-1) = m+1-k$.
Suppose first that $m \geq 5$ and $k \geq 3$. Consider the terms (q^m-1), $(q^{m-1}-1)$ and $(q^{m-2}-1)$. If none of the pairs (m,q), $(m-1,q)$ and $(m-2,q)$ is equal to $(6,2)$, by Zsigmondy's theorem, there are primitive prime divisors r_1 of (q^m-1), r_2 of $(q^{m-1}-1)$ and r_3 of $(q^{m-2}-1)$. The three primes r_1, r_2 and r_3 are pairwise distinct. Since the three terms (q^m-1), $(q^{m-1}-1)$ and $(q^{m-2}-1)$ occur only in the numerator and not in the denominator of n_k the degree n_k is divisible by r_1, r_2 and r_3. Hence n_k is not the product of two different primes. Suppose that $(m,q) = (6,2)$. Since $3 \leq k \leq m/2$ we have $k = 3$. But $n_3 = 3^2 \cdot 5 \cdot 31$ is not the product of two different primes. Suppose that $(m-1,q) = (6,2)$. Since $3 \leq k < m/2$ we have $k = 3$. But $n_3 = 3 \cdot 31 \cdot 127$ is not the product of two different primes. Suppose that $(m-2,q) = (6,2)$. Since $3 \leq k \leq m/2$ we have $k = 3$ or $k = 4$. But $n_3 = 3^2 \cdot 5 \cdot 17 \cdot 127$ and $n_4 = 3 \cdot 17 \cdot 31 \cdot 127$ are also not products of two different primes. Hence n_k is not the product of two different primes if $k \geq 3$.
Suppose now we have $m \geq 5$ and $k = 2$. Then we have

$$n_2 = \frac{(q^m-1)(q^{m-1}-1)}{(q-1)(q^2-1)}.$$

If $m \equiv 0 \pmod 4$ we have

$$n_2 = \frac{q^{m/2}-1}{q^2-1} \cdot (q^{m/2}+1) \cdot \frac{q^{m-1}-1}{q-1}.$$

Since $m \geq 8$, each of these three factors is greater than 1 and hence n_2 is not the product of two different primes.

If $m \equiv 1 \pmod 4$ we have

$$n_2 = \frac{q^{(m-1)/2}-1}{q^2-1} \cdot (q^{(m-1)/2}+1) \cdot \frac{q^m-1}{q-1},$$

hence if n_2 is the product of two different primes we have $m = 5$. In this case

$$n_2 = (q^2+1) \cdot \frac{q^5-1}{q-1}.$$

It follows that $q = 2^{2^f}$, $f \geq 0$. For $f \geq 2$ we have $q \equiv 1 \pmod 5$ and thus

$$(q^5-1)/(q-1) = q^4+q^3+q^2+q+1 \equiv 5 \cdot 1 \equiv 0 \pmod 5.$$

Since for $f \geq 2$ the term $(q^5-1)/(q-1)$ is greater than 5, it is not a prime. If $f = 0$ we have $q = 2$ and $n = 5 \cdot 31$. This case is listed in the lemma as Case (ii). If $f = 1$ we have $q = 4$ and $n_2 = 11 \cdot 17 \cdot 31$ which is not the product of two different primes.
If $m \equiv 2 \pmod 4$ respectively $m \equiv 3 \pmod 4$ we have

$$q^m - 1 = (q^{m/2}-1)(q^{m/2}+1)$$

respectively

$$q^{m-1} - 1 = (q^{(m-1)/2}-1)(q^{(m-1)/2}+1).$$

Since $m/2$ respectively $(m-1)/2$ are not equal to 6, by Zsigmondy's theorem, there is a primitive prime divisor r of $q^{m/2}-1$ respectively $q^{(m-1)/2}-1$. So there is $x \geq 1$ with

$$rx = q^{m/2}-1 \quad \text{respectively} \quad rx = q^{(m-1)/2}-1.$$

Since r does not divide q^2-1 we have

$$r \mid \frac{q^m-1}{q^2-1} = \frac{rx(q^{m/2}+1)}{q^2-1}$$

respectively

$$r \mid \frac{q^{m-1}-1}{q^2-1} = \frac{rx(q^{(m-1)/2}+1)}{q^2-1}.$$

Set $y := x(q^{m/2}+1)/(q^2-1)$ respectively $y := x(q^{(m-1)/2}+1)/(q^2-1)$. Since $m \geq 6$ we have $y > 1$ and

$$n_2 = r \cdot y \cdot \frac{q^{m-1}-1}{q-1} \quad \text{respectively} \quad n_2 = r \cdot y \cdot \frac{q^m-1}{q-1}.$$

Hence n_2 is not the product of two different primes.

Suppose now that $m = 4$ and $k = 2$. Then we have $n_2 = (q^2+1)(q^2+q+1)$. This implies $q = 2^{2^f}$, $f \geq 0$ and $p_1 = 2^{2^{f+1}} + 1$. If $f = 0$ we have $q = 2$ and $n = 5 \cdot 7$. This case is listed in the lemma as Case (iii). If $f \geq 1$ we have

$$q^2 + q + 1 = 4^{2^f} + 4^{2^{f-1}} + 1 \equiv 1 + 1 + 1 \equiv 0 \pmod 3.$$

Since $q^2 + q + 1 > 3$ this is a contradiction.
The case of arbitrary m and $k = 1$ is listed in the lemma as Case (i).

Consider now the case of Line 2. We have $S \cong \mathrm{PSL}(m, q)$, $m \geq 3$ and

$$n_k = \prod_{i=0}^{2k-1} (q^{m-1} - 1) / \left(\prod_{i=1}^{k} (q^i - 1) \right)^2$$

with $1 \leq k < (m/2)$.
Suppose first that $m \geq 5$ and $k \geq 2$. Consider the terms $(q^m - 1)$, $(q^{m-1} - 1)$ and $(q^{m-2} - 1)$. If none of the pairs (m, q), $(m-1, q)$ and $(m-2, q)$ is equal to $(6, 2)$, by Zsigmondy's theorem, there are primitive prime divisors r_1 of $(q^m - 1)$, r_2 of $(q^{m-1} - 1)$ and r_3 of $(q^{m-2} - 1)$. The three primes r_1, r_2 and r_3 are pairwise distinct. Since the three terms $(q^m - 1)$, $(q^{m-1} - 1)$ and $(q^{m-2} - 1)$ occur only in the numerator and not in the denominator of n_k the degree n_k is divisible by r_1, r_2 and r_3. Hence n_k is not the product of two different primes. Suppose that $(m, q) = (6, 2)$. Since $2 \leq k < m/2$ we have $k = 2$. But $n_2 = 3 \cdot 5 \cdot 7^2 \cdot 31$ is not the product of two different primes. Suppose that $(m-1, q) = (6, 2)$. Since $2 \leq k < m/2$ we have $k = 2$ or $k = 3$. But $n_2 = 3 \cdot 5 \cdot 7 \cdot 31 \cdot 127$ and $n_3 = 3^2 \cdot 5 \cdot 31 \cdot 127$ are not products of two different primes. Suppose that $(m-2, q) = (6, 2)$. Since $2 \leq k < m/2$ we have $k = 2$ or $k = 3$. But $n_2 = 3 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 127$ and $n_3 = 3^2 \cdot 5^2 \cdot 17 \cdot 31 \cdot 127$ are not products of two different primes. Hence n_k is not the product of two different primes if $k \geq 2$.
Suppose now that m is arbitrary and $k = 1$. Then we have

$$n_1 = \frac{(q^m - 1)(q^{m-1} - 1)}{(q-1)(q-1)}.$$

If m is even we have

$$n_1 = (q^{m/2} + 1) \cdot \frac{q^{m/2} - 1}{q - 1} \cdot \frac{q^{m-1} - 1}{q - 1}.$$

Since $m \geq 4$ each of these three factors is greater than 1 and thus n_1 is not the product of two different primes.
If m is odd we have

$$n_1 = (q^{(m-1)/2} + 1) \cdot \frac{q^{(m-1)/2} - 1}{q - 1} \cdot \frac{q^m - 1}{q - 1}.$$

If $m \geq 5$ each of these three factors is greater than 1 and thus n_1 is not the product of two different primes. Hence $m = 3$ and $n_1 = (q+1)(q^2+q+1)$

with q even, $q = 2^{2^f}$. If $f = 0$ we have $q = 2$ and $n_1 = 3 \cdot 7$. But the right multiplication groups of the RCC loops of order 21 are known (see Appendix B) and none of these groups contain a subgroup isomorphic to $\mathrm{PSL}(3, 2)$. If $f \geq 1$ the term $(q^2 + q + 1)$ is again divisible by 3 and greater than 3. Hence it is not a prime and n_1 is not the product of two different primes.

Consider the cases of the Lines 3 and 4. Then $S \cong \mathrm{PSL}(2, q)$ and

$$n = q(q + 1)/2 \quad \text{respectively} \quad n = q(q - 1)/2.$$

Suppose that q is even, $q = 2^e$, $e \geq 1$. If $e = 1$ we have $n = 3$ respectively $n = 1$. But these degrees are not products of two different primes. If $e = 2$ we have $n = 10$ respectively $n = 6$. But the right multiplication groups of the RCC loops of order 10 respectively 6 are known (see Appendix B) and none of these groups contains a subgroup isomorphic to $\mathrm{PSL}(2, 4)$. If $e \geq 3$ then n is divisible by 4 and hence not the product of two different primes. Hence q is odd. This case is listed in the lemma as Case (iv).

The case of Line 5 is listed in the lemma as Case (v).

Suppose now the cases of the Lines 6, 7, and 8. Then $S \cong \mathrm{PSL}(2, q)$ and $n = q(q^2 - 1)/d$ with $d \in \{24, 48, 120\}$. If $q - 1 > d$ the degree

$$n = \frac{(q - 1)q(q + 1)}{d}$$

is a product of three factors and each factor is greater than 1. Hence n is not the product of two different primes. So we have to consider the prime powers q with $q \leq d + 1$ such that q satisfies the conditions given in [LS03, Tbl. 3]. The only q which satisfy that the degree n is equal to the product of two different primes and which satisfy the conditions given in [LS03, Tbl. 3] are listed below:

$d = 24$	$q = 11$	$n = 5 \cdot 11$
	$q = 13$	$n = 7 \cdot 13$
$d = 48$	$q = 9$	$n = 3 \cdot 5$
	$q = 23$	$n = 11 \cdot 23$
$d = 120$	$q = 9$	$n = 2 \cdot 3$
	$q = 19$	$n = 3 \cdot 19$
	$q = 29$	$n = 7 \cdot 29$
	$q = 59$	$n = 29 \cdot 59$
	$q = 61$	$n = 31 \cdot 61$

The right multiplication groups of order 6 respectively 15 are known (see Appendix B) and none of these groups contain a subgroup isomorphic to $\mathrm{PSL}(2,9)$. The remaining cases are listed in the lemma as Case (vi).

Consider now the case of Line 9. Then $S \cong \mathrm{PSU}(m,q)$ and

$$n = \frac{(q^m-(-1)^m)(q^{m-1}-(-1)^{m-1})}{q^2-1}.$$

If $m = 2$ we have $S \cong \mathrm{PSU}(2,q) \cong \mathrm{PSL}(2,q)$ by [KL90, Prop. 2.9.1] and $n = q+1 = (q^2-1)/(q-1)$. This case is already listed in the lemma as Case (i). If $m = 3$ we have

$$n = q^3+1 = (q+1)(q^2-q+1).$$

Hence we have $q = 2^{2^f}$, $f \geq 0$. If $f = 0$ we have $n = 9$ which is not the product of two different primes. Hence $f \geq 1$. This case is listed in the lemma as Case (vii).
If $m \geq 4$ and m even we have

$$\begin{aligned} n &= (q^m-1)(q^{m-1}+1)/(q^2-1) \\ &= \frac{q^m-1}{q^2-1} \cdot (q+1)(q^{m-2}-q^{m-3}+q^{m-4}-\ldots-q+1). \end{aligned}$$

Since $q \geq 2$ and $m \geq 4$ each of these three factors is greater than 1 and thus n is not the product of two different primes.
If $m \geq 5$ and m odd we have

$$\begin{aligned} n &= \frac{(q^m+1)(q^{m-1}-1)}{q^2-1} \\ &= \frac{q^{m-1}-1}{q^2-1} \cdot (q+1)(q^{m-1}-q^{m-2}+q^{m-3}-\ldots-q+1). \end{aligned}$$

Since $q \geq 2$ and $m \geq 5$ each of these three factors is again greater than 1 and thus n is not the product of two different primes.

Consider now the case of Line 10. Then we have $S \cong \mathrm{PSp}(2m,q)$. Further we have $n = (q^{2m}-1)/(q-1)$. If $m = 1$ we have $\mathrm{PSp}(2,q) \cong \mathrm{PSL}(2,q)$ by [KL90, Prop. 2.9.1] and $n = (q^2-1)/(q-1)$. This case is already listed in the lemma as Case (i). If $m = 2$ we have $n = (q+1)(q^2+1)$. Hence $q = 2^{2^f}$. For $f = 0$ we have $q = 2$ and $S \cong \mathrm{PSp}(4,2)$ which is not simple. The case $f \geq 1$ is listed in the lemma as Case (viii).
If $m \geq 3$ and m odd we have

$$\begin{aligned} n &= (q^{2m}-1)/(q-1) \\ &= \frac{q^m-1}{q-1} \cdot (q+1)(q^{m-1}-q^{m-2}+q^{m-3}-\ldots-q+1). \end{aligned}$$

Since $m \geq 3$ each of these three factors is greater than 1 and hence n is not the product of two different primes.

If $m \geq 4$ and m even we have

$$n = (q^{2m} - 1)/(q - 1) = (q^m + 1) \cdot (q^{m/2} + 1) \cdot (q^{m/2} - 1)/(q - 1).$$

Since $m \geq 4$ each of these three factors is greater than 1 and hence n is again not the product of two different primes.

Suppose now the case of Line 11. Then we have $S \cong \mathrm{PSp}(2m, q)$ and $m \geq 2$ and

$$n = \frac{(q^{2m} - 1)(q^{2m-2} - 1)}{(q^2 - 1)(q - 1)}.$$

If $m = 2$ we have $n = (q + 1)(q^2 + 1)$ as in the case of Line 10. This case is already listed in the lemma as Case (viii). If $m \geq 3$ we have

$$n = \frac{(q^m + 1)(q^{m-1} + 1)}{q + 1} \cdot \frac{q^m - 1}{q - 1} \cdot \frac{q^{m-1} - 1}{q - 1}.$$

Since $m \geq 3$ each of these three factors is greater than 1 and hence n is not the product of two different primes.

Suppose the cases of the Lines 12 and 13. Then we have $S \cong \mathrm{PSp}(4, 2)'$ and $n \in \{6, 10\}$. But the right multiplication groups of the RCC loops of order 6 respectively 10 are known (see Appendix B) and none of these groups contains a subgroup isomorphic to $\mathrm{PSp}(4, 2)'$.

Suppose now the case of Line 14. Then we have $S \cong \Omega(2m + 1, q)$. Further we have $n = (q^{2m} - 1)/(q - 1)$. As in the case of Line 10 we have again $m = 1$ or $m = 2$. If $m = 1$ we have

$$S \cong \Omega(3, q) \cong \mathrm{PSL}(2, q)$$

by [KL90, Prop. 2.9.1] and $n = (q^2 - 1)/(q - 1)$. This case is already listed in the lemma as Case (i). If $m = 2$ we have $q = 2^{2^f}$, $f \geq 0$. Further, for q a power of 2, we have

$$S \cong \Omega(5, q) \cong \mathrm{PSp}(4, q)$$

by [KL90, Prop. 2.9.1] and $n = (q + 1)(q^2 + 1)$. This case is already listed in the lemma as Case (viii).

Consider now the case of Line 15. Then we have $S \cong \Omega(2m+1, q)$ with $m \geq 2$ and

$$n = \frac{(q^{2m} - 1)(q^{2m-2} - 1)}{(q^2 - 1)(q - 1)}.$$

If $m = 2$ we have $n = (q+1)(q^2+1)$ and $\Omega(5, q) \cong \mathrm{PSp}(4, q)$ by [KL90, Prop. 2.9.1]. This case is already listed in the lemma as Case (viii). If $m \geq 3$ the

degree n is not the product of two different primes as we have seen in the case of Line 11.

Suppose the case of Line 16. Then we have $S \cong \mathrm{P}\Omega^-(2m, q)$ with m even and $n = (q^m + 1)(q^{m-1} - 1)/(q - 1)$. If $m = 2$ we have

$$S \cong \mathrm{P}\Omega^-(4, q) \cong \mathrm{PSL}(2, q^2)$$

by [KL90, Prop. 2.9.1] and $n = q^2 + 1$. This case is included in Case (i) of the lemma. If $m \geq 4$ we have

$$n = (q^m + 1)(q^{m-2} + q^{m-3} + \ldots + q + 1).$$

Hence we have $q^m = 2^{2^k}$ with $k \geq 0$ and thus $q = 2^{2^f}$ and $m = 2^e$. This case is listed in the lemma as Case (ix).

Consider now the case of Line 17. Then we have $S \cong \mathrm{P}\Omega^-(2m, q)$ with q even and $m \geq 3$ and

$$n = (q^m + 1) \cdot \frac{q^{2m-2} - 1}{q^2 - 1} \cdot \frac{q^{m-2} - 1}{q - 1}.$$

If $m = 3$ we have $n = (q^2 + 1)(q^3 + 1)$. Hence $q = 2^{2^f}$ and $q^2 + 1 = 2^{2^{f+1}}$ is prime. But then $q^3 + 1 = 2^{3 \cdot 2^f} + 1$ is not a prime. If $m \geq 3$ each of the three factors is greater than 1 and hence n is not the product of two different primes.

Suppose now the case of Line 18. Then we have $S \cong \mathrm{P}\Omega^-(2m, q)$ with q even and 4 divides m. Further we have

$$n = (q^m + 1) \cdot \frac{(q^{2m-2} - 1)(q^{2m-4} - 1)(q^{m-3} - 1)}{(q - 1)(q^2 - 1)(q^3 - 1)}.$$

If $m = 4$ we have $n = (q^5 + 1)(q^3 + 1)(q^2 + 1)$ which is not the product of two different primes. For $m \geq 8$ the factor

$$\frac{(q^{2m-2} - 1)(q^{2m-4} - 1)(q^{m-3} - 1)}{(q - 1)(q^2 - 1)(q^3 - 1)}$$

is a product of three factors greater than 1 and hence n is not the product of two different primes.

Consider now the case of Line 19. Then we have $S \cong \mathrm{P}\Omega^+(2m, q)$ with m odd and $n = (q^{m-1} + 1) \cdot (q^m - 1)/(q - 1)$. If $m = 1$ we have $n = 2$ which is not the product of two different primes. If $m \geq 3$ we have q even and if $q^{m-1} + 1$ is prime we have $q = 2^{2^f}$ and $m = 2^e + 1$. This case is listed in the lemma as Case (x).

Suppose now the case of Line 20. Then we have $S \cong \mathrm{P}\Omega^+(2m, q)$ with q even and $m \geq 2$ and

$$n = (q^{m-2} + 1) \cdot \frac{q^m - 1}{q - 1} \cdot \frac{q^{2m-2} - 1}{q^2 - 1}.$$

If $m = 2$, by [KL90, Prop. 2.9.1], we have $S \cong \mathrm{P}\Omega^+(4,q) \cong \mathrm{PSL}(2,q) \times \mathrm{PSL}(2,q)$ which is not a simple group. For $m \geq 3$ each of the three factors in greater than 1 and hence not the product of two different primes.

Consider finally the case of Line 21. Then $S \cong \mathrm{P}\Omega^+(2m,q)$ with q even and $m \equiv 3 \pmod 4$ and

$$n = (q^{m-3}+1) \cdot \frac{(q^{2m-2}-1)(q^{2m-4}-1)(q^m-1)}{(q-1)(q^2-1)(q^3-1)}.$$

If $m = 3$ we have $n = 2(q^2+1)(q+1)$ which is not the product of two different primes. For $m \geq 7$ the factor

$$\frac{(q^{2m-2}-1)(q^{2m-4}-1)(q^m-1)}{(q-1)(q^2-1)(q^3-1)}.$$

is the product of three factors greater than 1 and hence n is not the product of two different primes. □

In the previous lemmas we determined the socles of the almost simple groups which act on p_1p_2 points. Hence these groups are possibly the right multiplication group of an RCC loop of order p_1p_2. Now we want to show that we can rule out these groups.

Suppose G is an almost simple group and the socle S and p_1p_2 are as in Case (iii) or (vi) of Lemma (4.6). For all these socles S we have $[\mathrm{Aut}(S) : S] = 2$. This implies $G = S$ or $G = \mathrm{Aut}(S)$. In Case (vi) where $S \cong \mathrm{PSL}(2,p_2)$ we further have $\mathrm{Aut}(S) = \mathrm{PGL}(2,p_2)$. For these groups and pairs (p_1,p_2) of Lemma (4.6)(iii) and (vi) we refer to Lemma (4.18) which shows that none of these groups is the right multiplication group of an RCC loop of order p_1p_2. So by now we showed that if the right multiplication group G of an RCC loop of order p_1p_2 acts primitively on $\{Ht \mid t \in T\}$, then G is almost simple and the socle S of G and the integer p_1p_2 are one of the following:

- $S \cong {}^2B_2(q)$ and $5p_2 = q^2+1$ where $q = 2^{2m+1} > 2$,
- $S \cong \mathrm{PSL}(5,2)$ and $p_1p_2 = 5 \cdot 31$,
- $S \cong \mathrm{PSL}(2,p_2)$ and $p_1 = (p_2 \pm 1)/2$,
- $S \cong \mathrm{PSL}(2,p_1^2)$ and $p_2 = (p_1^2+1)/2$,
- $S \cong \mathrm{PSL}(m,q)$ and $p_1p_2 = (q^m-1)/(q-1)$,
- $S \cong \mathrm{PSU}(3,q)$ and $p_1p_2 = (q+1)(q^2-q+1)$with $q = 2^{2^f}$, $f \geq 1$,
- $S \cong \mathrm{PSp}(4,q)$ and $p_1p_2 = (q+1)(q^2+1)$ with $q = 2^{2^f}$, $f \geq 1$,

- $S \cong \mathrm{P}\Omega^-(2m,q)$ and $p_1p_2 = (q^m+1)(q^{m-1}-1/(q-1))$ where $q = 2^{2^f}$, $m = 2^e$, $e \geq 2$ or
- $S \cong \mathrm{P}\Omega^+(2m,q)$ and $p_1p_2 = (q^{m-1}+1)(q^m-1)/(q-1)$ where $q = 2^{2^f}$, $m = 2^e+1$, $e \geq 1$.

In the following lemmas we will show that these cases do not lead to right multiplication groups of RCC loops of order p_1p_2.

To eliminate the almost simple groups G as right multiplication groups of an RCC loop of order p_1p_2, we need information about the sizes of the conjugacy classes of G. Since the socle S is a normal subgroup of G the conjugacy classes of G either contain only elements of S or contain no element of S. Hence the non-trivial conjugacy classes which consists of elements of S have size at least the minimal size of a non-trivial conjugacy class of S. For the socles S which we have to consider the sizes of the conjugacy classes are known. We further recall Lemma (2.26):

Lemma
Let G be an almost simple group with socle S, i.e. $S \cong \mathrm{Inn}(S) \leq G \leq \mathrm{Aut}(S)$. Let $\alpha \in G \setminus \mathrm{Inn}(S)$ and denote the conjugacy class of α in G by α^G. We have $C_{\mathrm{Inn}(S)}(\alpha) < \mathrm{Inn}(S)$ and

$$|\alpha^G| = [G : \mathrm{Inn}(S)\, C_G(\alpha)] \cdot [\mathrm{Inn}(S) : C_{\mathrm{Inn}(S)}(\alpha)].$$

In particular if c denotes the smallest index of any proper subgroup of S, then the size of the non-trivial conjugacy classes of G is at least c.

(4.7) Lemma
Suppose assumption (4.2) holds. Then the socle S of G is not an exceptional group.

Proof. Suppose that S is an exceptional group. By Lemma (4.5) we have $S \cong {}^2B_2(q)$ with $q = 2^{2m+1} > 2$ and $p_1p_2 = q^2+1$.
Consider the group S. The maximal subgroups of the Suzuki groups are well known, see [Suz62, Th. 9]. Let M be a maximal subgroup of S. Then we have

$$[S : M] \in \{q^2+1, \frac{q^2}{2}(q^2+1), \frac{q^2}{4}(q^2 \mp q\sqrt{2q} \pm \sqrt{2q} - 1)\}$$

or $M \cong {}^2B(q_0)$ with $q = q_0^r$, r prime and $q_0 > 2$.
We want to show that each maximal subgroup M of S has index at least q^2+1. Clearly this is true if $[S : M] \in \{q^2+1, q^2/2 \cdot (q^2+1)\}$. Suppose $[S : M] = q^2/4 \cdot (q^2 \mp q\sqrt{2q} \pm \sqrt{2q} - 1)$. Since $q \geq 8$ we have

$$[S : M] = \frac{q^2}{4}(q^2 \mp q\sqrt{2q} \pm \sqrt{2q} - 1) \geq \frac{q^2}{4}(q^2 - q\sqrt{2q} - \sqrt{2q} - 1)$$

$$\geq \frac{q^2}{4}(q^2 - 4q - 4 - 1) = \frac{1}{4}q^4 - q - \frac{5}{4} \geq q^2 + 1.$$

Suppose $M \cong {}^2B(q_0)$. Since $q_0 < \sqrt{q}$ we have

$$\begin{aligned}[S : M] &= \frac{q^2(q^2+1)(q-1)}{q_0^2(q_0^2+1)(q_0-1)} > \frac{q^2(q^2+1)(q-1)}{\sqrt{q}^2(\sqrt{q}^2+1)(\sqrt{q}-1)} \\ &= \frac{q(\sqrt{q}+1)}{q+1} \cdot (q^2+1) > q^2 + 1.\end{aligned}$$

Hence the index of an arbitrary proper subgroup U of S is at least $q^2 + 1$. By Lemma (2.26) the conjugacy classes of G have size at least $q^2 + 1$.
If G is the right multiplication group of a non-associative RCC loop $\mathcal{L}$ of order $q^2 + 1$ then there are $H \leq G$ and $T \subseteq G$ such that (G, H, T) is the envelope of $\mathcal{L}$. The transversal T is a union of conjugacy classes of G with $\{1_G\} \subseteq T$ and $|T| = q^2 + 1$. But this is a contradiction. □

(4.8) Lemma
Suppose assumption (4.2) holds. Then the socle S of G is not isomorphic to $\mathrm{PSL}(5, 2)$.

Proof. Suppose $S = \mathrm{PSL}(5, 2)$. Then, by Lemma (4.6), we have $p_1p_2 = 155$. Further, by [Con+85, p. 70] we have $[\mathrm{Aut}(S) : S] = 2$. Hence we have $G = S$ or $G = \mathrm{Aut}(S)$. The conjugacy classes of S are known and available in GAP, the non-trival conjugacy classes of S have size at least 465. Hence $G = \mathrm{Aut}(S)$. Let $\alpha \in G \setminus S$. By Lemma (2.26) we have $|\alpha^G| \geq [S : C_S(\alpha)]$. The subgroups of S are known and available in GAP; the only subgroups of index less than 155 are subgroups of index 31. Hence the size of the conjugacy class of α is at least 155 or it is 31.
If G is the right multiplication group of a non-associative RCC loop $\mathcal{L}$ of order 155 then there are $H \leq G$ and $T \subseteq G$ such that (G, H, T) is the envelope of $\mathcal{L}$. The transversal T is a union of conjugacy classes of G with $\{1_G\} \subseteq T$ and $|T| = 155 = 5 \cdot 31$. But this is a contradiction. □

(4.9) Lemma
Suppose assumption (4.2) holds. Then $S \ncong \mathrm{PSL}(2, p_2)$, p_2 an odd prime, $p_2 > 5$ and $p_1 = (p_2 \pm 1)/2$ as in Lemma (4.6)(iv).

Proof. Suppose $S \leq G \leq \mathrm{Aut}(S) = \mathrm{PGL}(2, p_2)$ with $p_2 \geq 5$ a prime and $(p_2 + 1)/2$ or $(p_2 - 1)/2$ is a prime. Denote this prime by p_1. By Theorem (2.20) we have $G = \mathrm{PGL}(2, p_2)$. The conjugacy classes of $\mathrm{PGL}(2, q)$ are well known, see [Sch07, Sec. 6] and [Ste51]. They are also provided in CHEVIE. The group $\mathrm{PGL}(2, p_2)$ has the following conjugacy classes:

- the trivial conjugacy class,
- one class of size $(p_2 - 1)(p_2 + 1)$,

- one class of size $p_2(p_2+1)/2$,
- one class of size $p_2(p_2-1)/2$,
- $(p_2-3)/2$ classes of size $p_2(p_2+1)$ and
- $(p_2-1)/2$ classes of size $p_2(p_2-1)$.

The transversal T is a union of conjugacy classes. We have $\{1_G\} \subseteq T$ and $|T| = p_1p_2$. If $p_1 = (p_2-1)/2$ then every non-trivial conjugacy class of G has size greater than or equal to p_1p_2. This contradicts our assumption. Suppose $p_1 = (p_2+1)/2$. Then only the trivial conjugacy class C_1 and the class C_2 of size $p_2(p_2-1)/2$ have a size less than p_1p_2. But

$$|T| = p_2 \cdot \frac{p_2+1}{2} = p_2 \cdot \frac{p_2-1}{2} + p_2 > p_2 \cdot \frac{p_2-1}{2} + 1 = |C_2| + |C_1|.$$

So this is a contradiction. □

In the following remark we give a summary of the maximal subgroups of $\mathrm{PSL}(2,q)$ so we are able to eliminate Case (v) of Lemma (4.6).

(4.10) Remark
The subgroups of $\mathrm{PSL}(2,q)$, $q = r^f \geq 5$ and r an odd prime, are classified in Dickson's Theorem, see [Hup67, Th. 8.27]. The maximal subgroups are also listed in [Giu07, Th. 2.2] and given by

- $M \cong \mathrm{Cyc}(r)^f \rtimes \mathrm{Cyc}((q-1)/2)$ with index $[S:M] = q+1$,
- $M \cong D(q-1)$, for $q \geq 13$, with index $[S:M] = q(q+1)/2$,
- $M \cong D(q+1)$, for $q \neq 7, 9$, with index $[S:M] = q(q-1)/2$,
- $M \cong \mathrm{PGL}(2, \sqrt{q})$, for q a square, with index $[S:M] = \sqrt{q}(q+1)/2$,
- $M \cong \mathrm{PSL}(2, q_0)$, for $q = q_0^e$, where e is an odd prime, with index

  $$[S:M] > \sqrt{q}(q+1),$$

- $M \cong \mathrm{Alt}(5)$, for $q \geq 9$, with index $[S:M] = (q-1)q(q+1)/120$,
- $M \cong \mathrm{Alt}(4)$ with index $[S:M] = (q-1)q(q+1)/24$,
- $M \cong \mathrm{Sym}(4)$ with index $[S:M] = (q-1)q(q+1)/48$.

In particular, if $q \geq 13$ then each maximal subgroup has an index at least $q+1$. Further, if $q \geq 17$ then only the maximal subgroups of index $q+1$ have an index less than $\sqrt{q} \cdot (q+1)/2$.

(4.11) Lemma
Suppose assumption (4.2) holds. Then $S \ncong \mathrm{PSL}(2, p_1^2)$, p_1 an odd prime and $p_2 = (p_1^2+1)/2$ as in Lemma (4.6)(v).

Proof. Suppose $S \cong \mathrm{PSL}(2, p_1^2)$, p_1 an odd prime and $p_2 = (p_1^2+1)/2$. By Theorem (2.20) we have $S < G$. The non-trivial conjugacy classes of S are known, see [Sch07, Sec. 6], and they are provided in CHEVIE. They have size at least p_1p_2. Hence the size of a non-trivial conjugacy class of G which contains elements of S is also at least p_1p_2.
Let $\alpha \in G \setminus S$. By Lemma (2.26) we have $|\alpha^G| = x \cdot [S : C_S(\alpha)]$ with $x \in \mathbb{N}$. Suppose $p_1 > 3$. Then, by Remark (4.10), $[S : C_S(\alpha)] > p_1p_2$ execpt if $C_S(\alpha) \leq M$ where M is a maximal subgroup of M with $[S : M] = p_1^2 + 1$. In this case there is y with $[S : C_S(\alpha)] = y(p_1^2+1)$. Hence if the size of α^G is less than p_1p_2 it is multiple of $p_1^2 + 1$.
If G is the right multiplication group of a non-associative RCC loop $\mathcal{L}$ of order p_1p_2 then there are $H \leq G$ and $T \subseteq G$ such that (G, H, T) is the envelope of $\mathcal{L}$. The transversal T is a union of conjugacy classes of G with $\{1_G\} \subseteq T$ and $|T| = p_1p_2$. But a union of conjugacy classes of sizes less than p_1p_2 with $\{1_G\} \subseteq T$ has a size congruent to 1 modulo p_1^2+1 and is therefore not divisible by the prime $p_2 = (p_1^2+1)/2$. So this is a contradiction.
Suppose finally that $p_1 = 3$. Then we have $p_1p_2 = 15$. But the right multiplication groups of order 15 are known (see Appendix B) and none of these groups contain a subgroup isomorphic to $\mathrm{PSL}(2, 9)$. □

Finally we eliminate the Cases (i), (vii), (viii), (ix) and (x) of Lemma (4.6).

(4.12) Lemma
Suppose assumption (4.2) holds. Then the socle S of G and the integer p_1p_2 are none of the following:

- $S \cong \mathrm{PSL}(m, q)$ *and* $p_1p_2 = (q^m - 1)/(q - 1)$,
- $S \cong \mathrm{PSU}(3, q)$ *and* $p_1p_2 = (q + 1)(q^2 - q + 1)$ *with* $q = 2^{2^f}$, $f \geq 1$,
- $S \cong \mathrm{PSp}(4, q)$ *and* $p_1p_2 = (q + 1)(q^2 + 1)$ *with* $q = 2^{2^f}$, $f \geq 1$,
- $S \cong \mathrm{P\Omega}^-(2m, q)$ *and* $p_1p_2 = (q^m + 1)(q^{m-1} - 1/(q - 1))$ *where* $q = 2^{2^f}$, $m = 2^e$, $e \geq 2$ *or*
- $S \cong \mathrm{P\Omega}^+(2m, q)$ *and* $p_1p_2 = (q^{m-1} + 1)(q^m - 1)/(q - 1)$ *where* $q = 2^{2^f}$, $m = 2^e + 1$, $e \geq 1$.

Proof. Suppose S and p_1p_2 are one of the listed groups respectively integers. Denote by c the smallest index of any proper subgroup of S. Then c is also the degree of the minimal non-trivial permutation representation of S. In [KL90, Th. 5.2.2] these degrees are listed. In each of the listed cases we have $c = p_1p_2$. By Lemma (2.26) we have that each non-trivial conjugacy class of G has size

at least p_1p_2. The transversal T is a union of conjugacy classes of G with $\{1_G\} \subseteq T$ and $|T| = p_1p_2$. But this is a contradiction. □

Now we are able to formulate the main theorem as a corollary of the previous lemmas.

(4.13) Theorem
Let p_1 and p_2 be two different primes with $p_1 < p_2$. Let $\mathcal{L}$ be a non-associative RCC *loop of order p_1p_2 and let (G, H, T) be the envelope of $\mathcal{L}$. Then G acts imprimitively on $\{Ht \mid t \in T\}$.*

We want to give an infinite series of right multiplication groups of RCC loops of order $2p$ for an odd prime p. We will show that for each odd prime p the group $\mathrm{Cyc}(p) \wr \mathrm{Cyc}(2)$ is the right multiplication group of a non-associative RCC loop of order $2p$. For this, we will examine this group in the following remark.

(4.14) Remark
Let p be an odd prime and $G = \mathrm{Cyc}(p) \wr \mathrm{Cyc}(2)$. We write

$$G = \{(\sigma; (y, z)) \mid \sigma \in \mathrm{Sym}(2),\ y, z \in \langle x \rangle\}$$

where $|\langle x \rangle| = p$. The group $\mathrm{Sym}(2)$ permutes the two components of the elementary abelian group $\langle x \rangle \times \langle x \rangle = \{(y, z) \mid y, z \in \langle x \rangle\}$ and the multiplication in G is defined by

$$(\sigma_1; (y_1, z_1)) \cdot (\sigma_2; (y_2, z_2)) = (\sigma_1\sigma_2; (y_1, z_1)^{\sigma_1} \cdot (y_2, z_2)).$$

Set $d := ((); (x^{-1}, x))$ and $c = ((1\ 2); (1, x))$. Then d is an element of order p and c is an element of order $2p$. Further we have:

$$\begin{aligned} d^c &= ((1\ 2); (x^{-1}, 1)) \cdot ((); (x^{-1}, x)) \cdot ((1\ 2); (1, x)) \\ &= ((1\ 2); (x^{-2}, x)) \cdot ((1\ 2); (1, x)) \\ &= ((); (x, x^{-2}) \cdot (1, x)) \\ &= ((); (x, x^{-1})) \\ &= d^{-1}. \end{aligned}$$

We show that $G = \langle d, c \rangle$. We have

$$\begin{aligned} d^{(p-1)/2}c^{p+1} &= ((); (x^{-(p-1)/2}, x^{(p-1)/2})) \cdot ((); (x^{(p+1)/2}, x^{(p+1)/2})) \\ &= ((); (x, x^p)) = ((); (x, 1)) \end{aligned}$$

and

$$\begin{aligned} d^{(p+1)/2}c^{p+1} &= ((); (x^{-(p+1)/2}, x^{(p+1)/2},) \cdot ((); (x^{(p+1)/2}, x^{(p+1)/2})) \\ &= ((); (1, x^{p+1})) = ((); (1, x)) \end{aligned}$$

and

$$\begin{aligned} d^{(p+1)/2}c^{p} &= ((); (x^{-(p+1)/2}, x^{(p+1)/2})) \cdot ((1\ 2); (x^{(p-1)/2}, x^{(p+1)/2})) \\ &= ((1\ 2); (x^{(p+1)/2}, x^{-(p+1)/2}) \cdot (x^{(p-1)/2}, x^{(p+1)/2})) \\ &= ((1\ 2); (x^{p}, 1)) = ((1\ 2); (1, 1)). \end{aligned}$$

Hence we have $G = \langle d, c\rangle$. Clearly we have $\langle d\rangle \trianglelefteq G$. Since $G/\langle d\rangle \cong \langle c\rangle$ is abelian and $G' \neq \{1_G\}$ we have $G' = \langle d\rangle$.
Set $H = \langle dc^2\rangle$. Then we have $H = \{1_G, dc^2, d^2c^4, d^3c^6, \ldots, d^{p-1}c^{2p-2}\}$ and $|H| = p$. Additionally we have $H \cap G' = \{1_G\}$. Since

$$(dc^2)^c = c^{-1}dc^2c = d^{-1}c^{-1}c^2 = d^{p-1}c^2 \notin H,$$

and since $|H| = p$ we have $\mathrm{Core}_G(H) = \{1_G\}$.

(4.15) Theorem
Let p be an odd prime and $G = \mathrm{Cyc}(p) \wr \mathrm{Cyc}(2)$. Then G is the right multiplication group of a non-associative RCC *loop of order $2p$.*

Proof. We adopt the notation of Remark (4.14) for G, H, c and d. We have $[G : G'H] = 2$ and $c \notin G'H$, so $S := \{1_G, c\}$ is a right transversal of $G'H$ in G. Hence, by Remark (2.6), the triple (G, H, T) with $T := SG'$ is an RCC loop folder with $|T| = |S| \cdot |G'| = 2p$. Since $c, d \in T$ we have $\langle T\rangle = G$ and since further $\mathrm{Core}_G(H) = \{1_G\}$ the RCC loop folder (G, H, T) is the envelope of an RCC loop of order $2p$. Since $|H| = p$ and $|T| = 2p$ the RCC loop folder (G, H, T) is not trivial. By Remark (1.35) the loop $(G, H, T)\lambda$ is non-associative. □

Technical lemmas

(4.16) Lemma
Let $c, k \in \mathbb{N}$ with $k \leq c/2$. Suppose that $\binom{c}{k} = p_1p_2$ is the product of two different primes p_1 and p_2 with $p_1 < p_2$. Then one of the following holds:

(i) $c = p_1p_2$, $k = 1$ *and* $\binom{c}{k} = c$,

(ii) *(a)* $c = p_2$ *is odd,* $p_1 = (p_2 - 1)/2$, $k = 2$ *and* $\binom{c}{k} = c(c-1)/2$,
(b) $c = p_2 + 1$ *is even,* $p_1 = (p_2 + 1)/2$, $k = 2$ *and* $\binom{c}{k} = c(c-1)/2$,

(iii) $c = 7$, $k = 3$ *and* $\binom{c}{k} = 35 = 5 \cdot 7$.

Proof. Suppose that $\binom{c}{k} = p_1 p_2$ is the product of two different primes p_1 and p_2 with $p_1 < p_2$.
If $k = 1$ then $p_1 p_2 = \binom{c}{k} = c$. This case is listed in the lemma as Case (i).
So suppose that $2 \leq k \leq c/2$. By [Ple82, Th. 4] the number of distinct prime factors of $\binom{c}{k}$ with $k \geq 2$ is greater than the number of distinct prime factors of c execpt for

- $k = 2$, $c \equiv 2 \pmod 4$ and $c - 1$ is a prime power or
- $k = 3$, $c - 1$ is a prime of the form $2^{2^f} + 1$ with f odd.

Suppose that (c, k) is none of these both exceptions. Since $\binom{c}{k}$ is the product of two different primes, c is an odd prime. This implies that c is the greatest prime factor of $\binom{c}{k}$. Hence we have $c = p_2$.
Consider the case $k = 2$. Then $p_1 p_2 = \binom{c}{k} = c \cdot (c-1)/2$. Hence $p_1 = (c-1)/2$. This case is listed in the lemma as Case (ii)(a). Consider the case $k = 3$ and $c = 7$. Then we have $\binom{7}{3} = 35 = 5 \cdot 7$. This case is listed in the lemma as Case (iii).
Consider the case $k = 3$ and $c > 7$. Then we have,

$$p_1 c = \binom{c}{3} = c \cdot \frac{(c-1)(c-2)}{6}.$$

Hence $p_1 = (c-1)(c-2)/6$. Since c is a prime we have $c \equiv 1 \pmod 6$ or $c \equiv 5 \pmod 6$. If $c \equiv 1 \pmod 6$ we have $(c-1)/6 \in \mathbb{N}$ and $(c-1)/6$ as well as $(c-2)$ are greater than 1. Hence p_1 is not prime. But this is a contradiction. If $c \equiv 5 \pmod 6$ we have $(c-1)/2, (c-1)/3 \in \mathbb{N}$ and both numbers are greater than 1. Hence p_1 is again not a prime which contradicts our assumption. Thus the number of distinct prime factors of $\binom{c}{k}$ with $c > 7$ and $k = 3$ is at least three. By [Ple82, Th. 3] the numbers of distinct prime factors of $\binom{c}{k}$ with $c > 7$ and $k > 3$ is also at least three. So if (c, k) is none of the both exceptions of [Ple82, Th. 4] and $k \geq 2$ then $\binom{c}{k}$ is not the product of two different primes.
Consider now the two exceptions of [Ple82, Th. 4]. Suppose first that $k = 2$ and $c \equiv 2 \pmod 4$ where $c - 1$ is a prime power. Let r be the odd prime with $c - 1 = r^e$. We have

$$p_1 p_2 = \binom{c}{2} = \frac{c(c-1)}{2} = \frac{(r^e + 1) r^e}{2}.$$

Hence $e = 1$, $p_2 = r$ and $c = p_2 + 1$ is even and $p_1 = (p_2 + 1)/2$. This case is listed in the lemma as Case (ii)(b). Suppose finally that $k = 3$ and $c - 1$ is a prime of the form $2^{2^f} + 1$ with f odd. Then we have

$$\binom{c}{3} = \frac{(2^{2^f} + 2) \cdot (2^{2^f} + 1) \cdot 2^{2^f}}{2 \cdot 3} = \frac{2^{2^f - 1} + 1}{3} \cdot (2^{2^f} + 1) \cdot 2^{2^f}.$$

Since $2^{2^f - 1} + 1 \equiv 0 \pmod 3$ the number $\binom{c}{3}$ is a product of three factors greater than one if $f > 1$, and hence not the product of two different primes. If $f = 1$ we have $\binom{6}{3} = 20 = 2^2 \cdot 5$ which is not the product of two different primes. □

(4.17) Lemma
Let $n \geq 5$. Then each non-trivial conjugacy class of the alternating group $\mathrm{Alt}(n)$ *as well as each conjugacy class of the symmetric group* $\mathrm{Sym}(n)$ *has a size greater than or equal to $n(n-1)/2$. Further each non-trivial conjugacy class of the automorphism group* $\mathrm{Aut}(\mathrm{Alt}(6))$ *of* $\mathrm{Alt}(6)$ *has a size greater than* $15 = 6(6-1)/2$.

Proof. For $n \geq 5$ consider the group $\mathrm{Alt}(n)$. If $5 \leq n \leq 8$ the conjugacy classes and their sizes are well known and available in GAP. The statemant of the lemma is true for these n. So suppose that $n \geq 9$. By [DM96, Th. 5.2A] every proper subgroup of $\mathrm{Alt}(n)$ with an index less than $n(n-1)/2$ is a point stabilizer. Since the point stabilizers are not centralizers, each non-trivial conjugacy class of the alternating group $\mathrm{Alt}(n)$ has a size greater than or equal to $n(n-1)/2$.
For $n \geq 5$ consider the group $\mathrm{Sym}(n)$. If $n \in \{5, 6\}$, the conjugacy classes and their sizes are well known and available in GAP. The statement of the lemma is true for these n. So suppose that $n \geq 7$. By [DM96, Th. 5.2B] the subgroups of $\mathrm{Sym}(n)$ with an index less than $n(n-1)/2$ are the following:

- $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$,
- the point stabilizers in $\mathrm{Sym}(n)$,
- the point stabilizers in $\mathrm{Alt}(n)$.

Since these subgroups are clearly not centralizers, each non-trivial conjugacy class of the alternating group $\mathrm{Sym}(n)$ has a size greater than or equal to $n(n-1)/2$.
We have $\mathrm{Aut}(\mathrm{Alt}(6)) = \mathrm{Sym}(6).2$ and this group is well known. The minimal size of a non-trivial conjugacy class of $\mathrm{Aut}(\mathrm{Alt}(6))$ is 30 which is greater than 15. □

(4.18) Lemma
Let G and n be one of the following pairs:

(i) $G \cong \mathrm{Alt}(7)$ *and* $n = 35$,

(ii) $G \cong \mathrm{Sym}(7)$ *and* $n = 35$,

(iii) $G \cong \mathrm{Alt}(8)$ *and* $n = 35$,

(iv) $G \cong \mathrm{Sym}(8)$ *and* $n = 35$,

(v) $G \cong M_{22}.2$ *and* $n = 22$,

(vi) $G \cong M_{22}.2$ *and* $n = 77$,

(vii) $G \cong \mathrm{PSL}(5, 2)$ *and* $n = 155$,

(viii) $G \cong \mathrm{PSL}(4, 2)$ *and* $n = 35$,

(ix) $G \cong \mathrm{Aut}(\mathrm{PSL}(4,2))$ *and* $n = 35$,

(x) $G \cong \mathrm{PSL}(2,11)$ *and* $n = 55$,

(xi) $G \cong \mathrm{PGL}(2,11)$ *and* $n = 55$,

(xii) $G \cong \mathrm{PSL}(2,13)$ *and* $n = 91$,

(xiii) $G \cong \mathrm{PGL}(2,13)$ *and* $n = 91$,

(xiv) $G \cong \mathrm{PSL}(2,19)$ *and* $n = 57$,

(xv) $G \cong \mathrm{PGL}(2,19)$ *and* $n = 57$,

(xvi) $G \cong \mathrm{PSL}(2,23)$ *and* $n = 253$,

(xvii) $G \cong \mathrm{PGL}(2,23)$ *and* $n = 253$,

(xviii) $G \cong \mathrm{PSL}(2,29)$ *and* $n = 203$,

(xix) $G \cong \mathrm{PGL}(2,29)$ *and* $n = 203$,

(xx) $G \cong \mathrm{PSL}(2,59)$ *and* $n = 841$,

(xxi) $G \cong \mathrm{PGL}(2,59)$ *and* $n = 841$,

(xxii) $G \cong \mathrm{PSL}(2,61)$ *and* $n = 1891$,

(xxiii) $G \cong \mathrm{PGL}(2,61)$ *and* $n = 1891$.

Then G is not the right multiplication group of a non-associative RCC *loop of order n.*

Proof. Suppose that G is the right multiplication group of a non-associative RCC loop $\mathcal{L}$ of order n and let (G, H, T) be the envelope of $\mathcal{L}$. Then T is a union of conjugacy classes with $\{1_G\} \subseteq T$ and $|T| = n$.
For the given pairs G and n the conjugacy classes and their sizes are well known and available in GAP. Only for the following pairs of G and n the group G has non-trivial conjugacy classes of a size less than n:

(ii) $G \cong \mathrm{Sym}(7)$ and $n = 35$ and one class of size 21,

(iv) $G \cong \mathrm{Sym}(8)$ and $n = 35$ and one class of size 28,

(viii) $G \cong \mathrm{PSL}(4,2)$ and $n = 35$ and one class of size 28,

(xii) $G \cong \mathrm{PSL}(2,13)$ and $n = 91$ and two classes of size 84,

(xiii) $G \cong \mathrm{PGL}(2,13)$ and $n = 91$ and one class of size 78,

(xxii) $G \cong \mathrm{PSL}(2,61)$ and $n = 1891$ and two classes of size 1860,

(xxiii) $G \cong \mathrm{PGL}(2,61)$ and $n = 1891$ and one class of size 1830.

Clearly in these cases there is no T which is a union of conjugacy classes and $|T| = n$. □

Appendix A

Source Code

To compute the RCC loops of small orders there are several GAP functions available with this thesis. These functions are described in this appendix. For more information about GAP see [Gap].

Let $\mathcal{L}$ be a non-associative RCC loop of order n with $2 \leq n \leq 30$. The right multiplication group $G := \mathrm{RM}(\mathcal{L})$ is a transitive group on n points and occurs in the GAP database TRANSITIVE GROUPS. By Lemma (3.13) G is non-abelian. Set $H = \mathrm{Stab}_G(1)$. Then, also by Lemma (3.13), we have $|H| > 1$ and since $[G : H] = n$ we have $|G| > n$. Further G and H satisfy the necessary condition

$$N_G(H) = H \cdot C_G(H)$$

by Lemma (2.7). The function call

```
ComputeGroups(n)
```

returns for an integer n with $2 \leq n \leq 30$ the list `li` of all integers i such that the groups G with

```
G:=TransitiveGroup(n,i)
```

satisfy these conditions, i.e.

$$|G| > n, \quad G \text{ is non-abelian}, \quad N_G(H) = H \cdot C_G(H).$$

Thus the transitive groups of degree n corresponding to the numbers in `li` are the putative right multiplication groups of a non-associative RCC loop of order n.

For a given group G and its subgroup H the function call

```
ComputeTT(G,H)
```

returns a record `result` with three components, called

```
CharTable, Classes, Transversals.
```

The value of the component `CharTable` is the character table of G, the value of the component `Classes` is the list of conjugacy classes of G corresponding to `result.CharTable`. Further the value of the component `Transversals` is a list corresponding to the set $TT(G, H)$ defined in Definition (3.1). Here corresponding means that for each $T \in TT(G, H)$ there is exactly one list t of integers in `result.Transversals` such that

```
x:=List(result.Classes{t}, Elements);
T:=Concatenation(x);
```

i.e. T is the union of the j-th conjugacy classes of G with $j \in t$. Notice that the list `result.Transversals` is sorted in the sense of GAP MANUAL, Chapter 21, Section 10.

For a given group G with $G \leq \mathrm{Sym}(n)$, $2 \leq n \leq 30$, the function call

```
ComputeRCCLoops(G)
```

returns a record `result` with four components, called

```
CharTable, Classes, Transversals,  IsoClassesRep.
```

The values of the components `CharTable`, `Classes` and `Transversals` agree with the values of the corresponding components of

```
ComputeTT(G, Stabilizer(G,1)),
```

i.e. `result.CharTable` is the character Table of G, `result.Classes` is the list of conjugacy classes of G corresponding to `result.CharTable` and the list `result.Transversals` corresponds to the set $TT(G, \mathrm{Stab}_G(1))$.
The value of the component `IsoClassesRep` is a list `lk` of integers which correspond to the isomorphism classes of non-associative RCC loops of order n with right multiplication group G. Here corresponding means that for each such isomorphism class with representative $\mathcal{L}$ there is excatly one k in `lk` such that the triple (G, H, T) is isomorphic to the envelope of $\mathcal{L}$, where $H = \mathrm{Stab}_G(1)$ and T is the transversal to the k-th element of `result.Transversals`.

The function call

```
ComputeOrbits(G,H,result)
```

takes as input a group G, a subgroup H of G and a record `result` of the form

```
result:=ComputeTT(G,H).
```

Here it is necessary that $G \leq \mathrm{Sym}(n)$ with $n = [G : H]$. Notice that for efficiency reasons `ComputeOrbits` does **not** test if the input is correct. For a correct input the function call

```
ComputeOrbits(G,H,result)
```

returns the list `lk` of integers corresponding to the isomorphism classes of non-associative RCC loops of order n similar to `ComputeRCCLoops(G)`.

This function is available for the convenience of the user to be able to compute the result of `ComputeRCCLoops` in two steps with `ComputeTT` and `ComputeOrbits` if required.

Now we demonstrate how to use these functions in some examples. We choose $n = 8$ and compute first all groups G which may be a right multiplication group of a non-associative RCC loop of order n.

```
gap> n:=8;;
gap> all:=ComputeGroups(n);; Length(all);
44
```

So we have to test which of these 44 groups are indeed right multiplication groups of a non-associative RCC loop of order 8, i.e. for which of these groups the set $TT(G, \mathrm{Stab}_G(1))$ is not empty.

```
gap> rmgrps:=[];;
gap> for i in all do
>       G:=TransitiveGroup(n,i);
>       H:=Stabilizer(G,1);
>       result:=ComputeTT(G,H);
>       if Length(result.Transversals)>0 then
                    Add(rmgrps,i);
                fi;
>    od;
gap> rmgrps;
[ 7, 9, 10, 11, 13, 17, 23 ]
```

Hence the groups of the GAP database TRANSITIVE GROUPS of degree 8 identified by the numbers in `rmgrps` are right multiplications groups of a non-associative RCC loop of order 8. Let us take a look at the group with number 17. First we call the functions `ComputeTT` and `ComputeOrbits` as well as the function `ComputeRCCLoops`.

```
gap> i:=17;;
gap> G:=TransitiveGroup(n,i);;
gap> H:=Stabilizer(G,1);;
gap>
gap> result1:=ComputeTT(G,H);;
gap> TT1:=result1.Transversals;
[ [ 1, 5, 9, 10 ],  [ 1, 5, 9, 11 ],
  [ 1, 5, 9, 12 ], [ 1, 5, 9, 13 ],
  [ 1, 6, 10, 14 ], [ 1, 6, 11, 14 ],
  [ 1, 6, 12, 14 ], [ 1, 6, 13, 14 ] ]
gap> lk1:=ComputeOrbits(G,H,result1);
[ 1, 2, 3, 4 ]
gap> result2:=ComputeRCCLoops(G);;
gap> TT2:=result2.Transversals;
[ [ 1, 5, 9, 10 ],  [ 1, 5, 9, 11 ],
```

```
  [ 1, 5, 9, 12 ],  [ 1, 5, 9, 13 ],
  [ 1, 6, 10, 14 ], [ 1, 6, 11, 14 ],
  [ 1, 6, 12, 14 ], [ 1, 6, 13, 14 ] ]
gap> lk2:=result2.IsoClassesRep;
[ 1, 2, 3, 4 ]
gap> TT1=TT2; lk1=lk2;
true
true
```

Now we set

```
gap> result:=result1;; TT:=TT1;; lk:=lk1;;
```

The first four elements of `TT` correspond to representatives of the isomorphism classes of non-associative RCC loops of order 8 with right multiplication group G. To get these representatives we first have to compute the transversals as a list of elements of G.

```
gap> conj:=result.Classes;;
gap> elem:=List(conj, Elements);;
gap> T:=TT{lk};
[ [ 1, 5, 9, 10 ], [ 1, 5, 9, 11 ],
  [ 1, 5, 9, 12 ], [ 1, 5, 9, 13 ] ]
gap> T:=List(T, t->Concatenation(elem{t}));;
gap> T[1];
[ (), (1,2,3,8)(4,5,6,7), (1,3)(2,8)(4,7,6,5),
 (1,8,3,2)(4,6)(5,7), (1,4)(2,5)(3,6)(7,8),
 (1,5)(2,6)(3,7)(4,8),  (1,6)(2,7)(3,4)(5,8),
 (1,7)(2,4)(3,5)(6,8) ]
```

Now we have to compute the RCC loops from these transversals. For this we use the function `LoopByRightSection` of the GAP package LOOPS. For more information about the package LOOPS see [NV15]. The package has to be loaded in GAP before using it. To ensure that the right multiplication group of the computed loops is the given group G as a set and not just as an isomorphic group we have to sort the transversals.

```
gap> for t in T do Sort(t); od;
gap> LoadPackage("loops");;
gap> LL:=List(T, LoopByRightSection);
[ <loop of order 8>, <loop of order 8>,
<loop of order 8>, <loop of order 8> ]
gap> ForAll(LL, L->RightMultiplicationGroup(L)=G);
true
```

Let G be a group and $H \leq G$ be a subgroup of G. Recall the definition of the set $\mathcal{Q}(G,H)$:

$$\mathcal{Q}(G,H) = \{C \in \mathcal{C}(G) |\ |C| < [G:H] \text{ and } C \notin \mathcal{C}^H(G)\}.$$

By Lemma (3.13) we know that G is not the right multiplication group of an RCC loop of order $[G : H]$ if

$$\langle C \mid C \in \mathcal{Q}(G, H)\rangle \neq G$$

or if there is no subset $\{C_{k_2}, C_{k_3}, \ldots, C_{k_s}\}$ of $\mathcal{Q}(G, H)$ for which $|\cup_{i=1}^{s} C_{k_i}| + 1$ divides the order of G. These are the conditions (3.13)(iv) and (v). The function call

```
QGeneratesGroup(G,H)
```

returns `true` if

$$\langle C \mid C \in \mathcal{Q}(G, H)\rangle = G$$

and `false` otherwise. The function call

```
QCombinesIndex(G,H)
```

returns `true` if there is a subset $\{C_{k_2}, C_{k_3}, \ldots, C_{k_s}\}$ of $\mathcal{Q}(G, H)$ for which $|\cup_{i=1}^{s} C_{k_i}| + 1$ divides the order of G. Hence, if one of these functions returns `false`, the group G is not the right multiplication group of an RCC loop of order $[G : H]$.

Appendix B

Data of Small RCC loops

The data of the non-associative RCC loops of order n with

$$n \in \{6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30\}$$

is available with this thesis. The data is stored in ASCII format and is readable independently of the computer algebra system GAP. But we will illustrate how to read them with GAP. For more information about GAP see [Gap]. For each of the above n there is one file, named `RCCLoopsn`, i.e. there are the files `RCCLoops6`, `RCCLoops8`, ..., `RCCLoops30`. These files contain encodings of the envelopes of the non-associative RCC loops of order n.

Fix one of the n above and consider the file `RCCLoopsn`. It contains two lists named `grps` and `classlists`. Let nr_{RM} be the number of groups which are right multiplication groups of a non-associative RCC loop of order n. Then each of the lists `grps` and `classlists` contains exactly nr_{RM} entries; one for each of these groups.

Each entry of the list `grps` encodes one group G (as a subgroup of $\mathrm{Sym}(n)$) which is the right multiplication group of a non-associative RCC loop of order n. An entry of the list `grps` is a list, called `conj`, of lists. This list `conj` corresponds to the conjugacy classes of the group G. For example let $n = 9$. The second entry of the list `grps` is:

```
[ [ () ],
  [ (2,5,8)(3,9,6), (1,4,7)(2,8,5), (1,7,4)(3,6,9) ],
  [ (2,8,5)(3,6,9), (1,4,7)(3,9,6), (1,7,4)(2,5,8) ],
  [ (1,2,3,4,5,6,7,8,9), (1,5,9,4,8,3,7,2,6), (1,8,6,4,2,9,7,5,3) ],
  [ (1,2,6,4,5,9,7,8,3), (1,5,3,4,8,6,7,2,9), (1,8,9,4,2,3,7,5,6) ],
  [ (1,2,9,4,5,3,7,8,6), (1,5,6,4,8,9,7,2,3), (1,8,3,4,2,6,7,5,9) ],
  [ (1,3,8,7,9,5,4,6,2), (1,6,5,7,3,2,4,9,8), (1,9,2,7,6,8,4,3,5) ],
  [ (1,3,5,7,9,2,4,6,8), (1,6,2,7,3,8,4,9,5), (1,9,8,7,6,5,4,3,2) ],
  [ (1,3,2,7,9,8,4,6,5), (1,6,8,7,3,5,4,9,2), (1,9,5,7,6,2,4,3,8) ],
  [ (1,4,7)(2,5,8)(3,6,9) ],
  [ (1,7,4)(2,8,5)(3,9,6) ]
]
```

This means the group G has eleven conjugacy classes. Clearly G as a set is the union of its conjugacy classes.

Corresponding to each group G encoded in the list `grps` there is an entry in the list `classlists`. This entry is a list, called R, of lists of integers. For example let $n = 9$. The second entry of the list `classlists` is

```
[ [ 1, 4, 7, 10, 11 ], [ 1, 4, 9, 10, 11 ] ]
```

Each list t in R corresponds to a transversal T, such that (G, H, T), where G is the group of the corresponding entry in the list `grps` and $H = \mathrm{Stab}_G(1)$, is the envelope of a non-associative RCC loop of order n. Here T is the union of the conjugacy classes of G whose numbers are in t.

We illustrate how to read these files with GAP:

```
gap> Read("RCCLoops9");
gap> Length(grps);
3
gap> j:=2;;
gap> conj:=grps[j];
[ [ () ],
  [ (2,5,8)(3,9,6), (1,4,7)(2,8,5), (1,7,4)(3,6,9) ],
  [ (2,8,5)(3,6,9), (1,4,7)(3,9,6), (1,7,4)(2,5,8) ],
  [ (1,2,3,4,5,6,7,8,9), (1,5,9,4,8,3,7,2,6), (1,8,6,4,2,9,7,5,3) ],
  [ (1,2,6,4,5,9,7,8,3), (1,5,3,4,8,6,7,2,9), (1,8,9,4,2,3,7,5,6) ],
  [ (1,2,9,4,5,3,7,8,6), (1,5,6,4,8,9,7,2,3), (1,8,3,4,2,6,7,5,9) ],
  [ (1,3,8,7,9,5,4,6,2), (1,6,5,7,3,2,4,9,8), (1,9,2,7,6,8,4,3,5) ],
  [ (1,3,5,7,9,2,4,6,8), (1,6,2,7,3,8,4,9,5), (1,9,8,7,6,5,4,3,2) ],
  [ (1,3,2,7,9,8,4,6,5), (1,6,8,7,3,5,4,9,2), (1,9,5,7,6,2,4,3,8) ],
  [ (1,4,7)(2,5,8)(3,6,9) ],
  [ (1,7,4)(2,8,5)(3,9,6) ]
]
gap> R:=classlists[j];
[ [ 1, 4, 7, 10, 11 ], [ 1, 4, 9, 10, 11 ] ]
gap> transversals:=List(R, t->Concatenation(grps[j]{t}));;
gap> for T in transversals do Sort(T); od;
gap> transversals;
[ [ (), (1,2,3,4,5,6,7,8,9), (1,3,8,7,9,5,4,6,2),
    (1,4,7)(2,5,8)(3,6,9), (1,5,9,4,8,3,7,2,6),
    (1,6,5,7,3,2,4,9,8), (1,7,4)(2,8,5)(3,9,6),
    (1,8,6,4,2,9,7,5,3), (1,9,2,7,6,8,4,3,5) ],
  [ (), (1,2,3,4,5,6,7,8,9), (1,3,2,7,9,8,4,6,5),
    (1,4,7)(2,5,8)(3,6,9), (1,5,9,4,8,3,7,2,6),
    (1,6,8,7,3,5,4,9,2), (1,7,4)(2,8,5)(3,9,6),
    (1,8,6,4,2,9,7,5,3), (1,9,5,7,6,2,4,3,8) ]
]
```

Then each of the triples (G, H, T) with $H = \mathrm{Stab}_G(1)$ and T in `transversals` is the envelope of a non-associative RCC loop of order n. Further, let $\mathcal{C}$ be an isomorphism class of non-associative RCC loops of order with right multiplication group G. Then there is exactly one T in `transversals` such that (G, H, T) with $H = \mathrm{Stab}_G(1)$ is the envelope of a representative of $\mathcal{C}$.

The next tables display for every n with

$$n \in \{6, 8, 9, 10, 12, 14, 15\}$$

the GAP database numbers nr_{GAP} of the groups G in TRANSITIVE GROUPS which are right multiplication groups of an RCC loop of order n, a description of the isomorphism type of G, the order of G, the size of the set $TT(G, H)$

with $H = \mathrm{Stab}_G(1)$ and the number nr_{RCC} of isomorphism classes of non-associative RCC loops corresponding to this group. So the first table describes the following facts:

For $n = 6$ there is one group G which is the right multiplication group of a non-associative RCC loop, namely

```
G := TransitiveGroup(6,5).
```

The group G is isomorphic to the wreath product of a cyclic group of order 3 and a cyclic group of order 2. For $H = \mathrm{Stab}_G(1)$ the set $TT(G, H)$ has size 5 and there are three isomorphism classes of non-associative RCC loops $\mathcal{L}$ with right multiplication group $\mathrm{RM}(\mathcal{L}) = G$.

The description of the isomorphism type of G correspond to the names of the transitive groups up to degree 15 given in [CHM98].

For $n = 21$ quite a similar table is given, but here there is no isomorphism type of G listed.

Table B.1: $\mathrm{RM}(\mathcal{L})$ of the RCC loops $\mathcal{L}$ of order 6

nr_{GAP}	Isomorphism type	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
5	$3wr2$	18	5	3

Table B.2: $\mathrm{RM}(\mathcal{L})$ of the RCC loops $\mathcal{L}$ of order 8

nr_{GAP}	Isomorphism type	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
7	$1/2[2^3]4$	16	6	3
9	$D(4)[x]2$	16	4	3
10	$[2^2]4$	16	6	3
11	$Q_8 : 2$	16	4	3
13	$E(8) : 3$	24	2	1
17	$[4^2]2$	32	8	4
23	$GL(2, 3)$	48	2	2

Table B.3: RM($\mathcal{L}$) of the RCC loops $\mathcal{L}$ of order 9

nr_{GAP}	Isomorphism type	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
4	$S(3)[x]3$	18	3	2
6	$1/3[3^3]3$	27	6	2
7	$[3^2]3$	27	6	1

Table B.4: RM($\mathcal{L}$) of the RCC loops $\mathcal{L}$ of order 10

nr_{GAP}	Isomorphism type	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
4	$1/2[F(5)]2$	20	2	2
6	$[5^2]2$	50	49	14

Table B.5: RM($\mathcal{L}$) of the RCC loops $\mathcal{L}$ of order 12

nr_{GAP}	Isomorphism type	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
6	$A_4(12)x2$	24	3	2
10	$S(3)[x]E(4)$	24	4	2
11	$S(3)[x]C(4)$	24	6	4
14	$D(4)[x]C(3)$	24	30	18
15	$1/2[3:2]dD(4)$	24	2	2
18	$[3^2]E(4)$	36	71	27
19	$[3^2]4$	36	71	27
20	$A(4)[x]C(3)$	36	6	2
26	$A_4(12)x2^2$	48	22	7
28	$D(4)[x]S(3)$	48	2	2
37	$[3^2:2]E(4)$	72	8	2

39	$[3^2:2]4$	72	8	2
42	$6wr2$	72	106	54
85	$[1/4E(4)^3:3]3$	144	4	1
117	$[3^3:2]E(4)$	216	3	1
124	$[2]L(6):2_12$	240	2	2

Table B.6: RM($\mathcal{L}$) of the RCC loops $\mathcal{L}$ of order 14

nr_{GAP}	Isomorphism type	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
4	$2[1/2]F_42(7)$	42	2	2
5	$F_21(7)[x]2$	42	2	2
8	$7wr2$	98	531	93

Table B.7: RM($\mathcal{L}$) of the RCC loops $\mathcal{L}$ of order 15

nr_{GAP}	Isomorphism type	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
3	$D(5)[x]3$	30	3	2
4	$5[x]S(3)$	30	15	5
8	$F(5)[x]3$	60	12	7
15	$GL(2,4)$	180	6	3

Table B.8: RM($\mathcal{L}$) of the RCC loops $\mathcal{L}$ of order 21

nr_{GAP}	$\lvert G\rvert$	$\lvert TT(G,H)\rvert$	nr_{RCC}
3	42	3	2
4	42	3	3
6	42	63	13
7	63	6	4
9	126	18	10
13	147	489	83
21	441	8	4

Bibliography

[Asc05] Michael Aschbacher. *On Bol loops of exponent 2. J. Algebra* 288.1 (2005), pp. 99–136. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2005.03.005. URL: http://dx.doi.org/10.1016/j.jalgebra.2005.03.005.

[Bae39] Reinhold Baer. *Nets and groups. Trans. Amer Math. Soc* 46 (1939), pp. 110–141.

[Bae40] Reinhold Baer. *Nets and groups II. Trans. Amer Math. Soc* 47 (1940), pp. 435–439.

[BBT07] Andrew M. Bruckner, Judith B. Bruckner, and Brian S. Thomson. *Real Analysis*. 2007. ISBN: 013458886X.

[Cam99] Peter J. Cameron. *Permutation Groups*. Vol. 45. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1999, pp. x+220. ISBN: 0-521-65302-9; 0-521-65378-9. DOI: 10.1017/CBO9780511623677. URL: http://dx.doi.org/10.1017/CBO9780511623677.

[CHM98] John H. Conway, Alexander Hulpke, and John McKay. *On transitive permutation groups. LMS J. Comput. Math.* 1 (1998), 1–8 (electronic). ISSN: 1461-1570. DOI: 10.1112/S1461157000000115. URL: http://dx.doi.org/10.1112/S1461157000000115.

[Con] Keith Conrad. *Simplicity of A_n*. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.210.8512&rep=rep1&type=pdf.

[Con+85] J. H. Conway et al. *Atlas of finite groups*. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985, pp. xxxiv+252. ISBN: 0-19-853199-0.

[DK89] Aleš Drápal and Tomáš Kepka. *Alternating groups and Latin squares. European J. Combin.* 10.2 (1989), pp. 175–180. ISSN: 0195-6698. DOI: 10.1016/S0195-6698(89)80045-9. URL: http://dx.doi.org/10.1016/S0195-6698(89)80045-9.

[DM96] John D. Dixon and Brian Mortimer. *Permutation Groups*. Vol. 163. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, pp. xii+346. ISBN: 0-387-94599-7. DOI: 10.1007/978-1-4612-0731-3. URL: http://dx.doi.org/10.1007/978-1-4612-0731-3.

[Drá01] Aleš Drápal. *Multiplication groups of finite loops that fix at most two points. Journal of Algebra* 235 (2001), pp. 154–175.

[Drá04] Aleš Drápal. *On multiplication groups of left conjugacy closed loops. Comment. Math. Univ. Carolin.* 45.2 (2004), pp. 223–236. ISSN: 0010-2628.

[Drá08] Aleš Drápal. *Structural interaction of conjugacy closed loops. Transactions of the american mathematical society* 360.2 (2008), pp. 671–689.

[Gap] *GAP – Groups, Algorithms, and Programming, Version 4.8.6*. The GAP Group. 2016. URL: \verb+(http://www.gap-system.org)+.

[Gec+96] M. Geck et al. CHEVIE – *A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. Appl. Algebra Engrg. Comm. Comput.* 7 (1996), pp. 175–210.

[Giu07] Michael Giudici. *Maximal subgroups of almost simple groups with socle* PSL$(2, q)$. 2007. URL: https://arxiv.org/abs/math/0703685.

[GR82] Egar G. Goodaire and Daniel A. Robinson. *A class of loops which are isomorphic to all loop isotopes. Can.J.Math* 34.3 (1982), pp. 662–672.

[Hup67] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967, pp. xii+793.

[Isa06] I. Martin Isaacs. *Character Theory of Finite Groups*. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. AMS Chelsea Publishing, Providence, RI, 2006, pp. xii+310. ISBN: 978-0-8218-4229-4; 0-8218-4229-3. DOI: 10.1090/chel/359. URL: http://dx.doi.org/10.1090/chel/359.

[KÖ7] Sebastian M. Köhler. "Multiplikationsgruppen von Quasigruppen". MA thesis. RWTH Aachen, 2007.

[KL90] Peter Kleidman and Martin Liebeck. *The Subgroup Structure of the Finite Classical Groups*. Vol. 129. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1990, pp. x+303. ISBN: 0-521-35949-X. DOI: 10.1017/CBO9780511629235. URL: http://dx.doi.org/10.1017/CBO9780511629235.

[LS03] Cai Heng Li and Ákos Seress. *The primitive permutation groups of squarefree degree. Bull. London Math. Soc.* 35.5 (2003), pp. 635–644. ISSN: 0024-6093. DOI: 10.1112/S0024609303002145. URL: http://dx.doi.org/10.1112/S0024609303002145.

[MN] Peter Müller and Gábor P. Nagy. *A note on the group of projectivities of finite projective planes* (). URL: https://www.mathematik.uni-wuerzburg.de/~mueller/Papers/m24final.pdf.

[NV15] G. Nagy and P. Vojtechovsky. *Loops, Computing with quasigroups and loops in GAP, Version 3.0.0.* Refereed GAP package. 2015. URL: http://www.math.du.edu/loops.

[Pfl90] Hala O. Pflugfelder. *Quasigroups and Loops: Introduction.* Vol. 7. Sigma Series in Pure Mathematics. Heldermann Verlag, Berlin, 1990, pp. viii+147. ISBN: 3-88538-007-2.

[Ple82] P. A. B. Pleasants. *The Number of Prime Factors of Binomial Coefficients. J. Number Theory* 15.2 (1982), pp. 203–225. ISSN: 0022-314X. DOI: 10.1016/0022-314X(82)90026-9. URL: http://dx.doi.org/10.1016/0022-314X(82)90026-9.

[Sch07] J. Schur. *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. J. Reine Angew. Math.* 132 (1907), pp. 85–137. ISSN: 0075-4102. DOI: 10.1515/crll.1907.132.85. URL: http://dx.doi.org/10.1515/crll.1907.132.85.

[Ste51] Robert Steinberg. *The representations of* $\mathrm{GL}(3,q)$, $\mathrm{GL}(4,q)$, $\mathrm{PGL}(3,q)$, *and* $\mathrm{PGL}(4,q)$. *Canadian J. Math.* 3 (1951), pp. 225–235. ISSN: 0008-414X.

[Suz62] Michio Suzuki. *On a class of doubly transitive groups. Ann. of Math. (2)* 75 (1962), pp. 105–145. ISSN: 0003-486X.

[Wal07] Rolf Walter. *Einführung in die Analysis. 1.* de Gruyter Lehrbuch. [de Gruyter Textbook]. Walter de Gruyter & Co., Berlin, 2007, pp. x+567. ISBN: 978-3-11-019539-2.

[Zsi92] K. Zsigmondy. *Zur Theorie der Potenzreste. Monatsh. Math. Phys.* 3.1 (1892), pp. 265–284. ISSN: 0026-9255. DOI: 10.1007/BF01692444. URL: http://dx.doi.org/10.1007/BF01692444.