Quasigroups and Related Systems **23** (2015), 129 − 163

Three lectures on automorphic loops

Petr Vojtěchovský

Abstract. These notes accompany a series of three lectures on automorphic loops to be delivered by the author at Workshops Loops '15 (Ohrid, Macedonia, 2015). Automorphic loops are loops in which all inner mappings are automorphisms.

The first paper on automorphic loops appeared in 1956 and there has been a surge of interest in the topic since 2010. The purpose of these notes is to introduce the methods used in the study of automorphic loops to a wider audience of researchers working in nonassociative mathematics.

In the first lecture we establish basic properties of automorphic loops (flexibility, power-associativity and the antiautomorphic inverse property) and discuss relations of automorphic loops to Moufang loops.

In the second lecture we expand on ideas of Glauberman and investigate the associated operation $(x^{-1}\backslash(y^2x))^{1/2}$ and similar concepts, using a more modern approach of twisted subgroups. We establish many structural results for commutative and general automorphic loops, including the Odd Order Theorem.

In the last lecture we look at enumeration and constructions of automorphic loops. We show that there are no nonassociative simple automorphic loops of order less than 4096, we study commutative automorphic loops of order pq and p^3, and introduce two general constructions of automorphic loops.

The material is newly organized and sometimes new, shorter proofs are given.

Contents

2010 Mathematics Subject Classification: Primary: 20N05.

Keywords: Automorphic loop, commutative automorphic loop, Γ-loop, Moufang loop, Bruck loop, Bol loop, Lie ring, twisted subgroup.

Research partially supported by the Simons Foundation Collaboration Grant 210176.

Introduction

The purpose of these notes is to give a gentle introduction into the theory of automorphic loops that nevertheless captures the main ideas of current investigation. Due to the limited scope of the lectures, not all proofs are included and not all known results about automorphic loops are stated. A survey article on automorphic loops that attempts to remedy both of these shortcomings is under preparation by the author and will appear elsewhere.

Let $Q = (Q, \cdot, \backslash, /, 1)$ be a loop, where we also write xy to denote the product $x \cdot y$. For $x \in Q$, let

$$L_x : Q \to Q,\ L_x(y) = xy \qquad \text{and} \qquad R_x : Q \to Q,\ R_x(y) = yx$$

be the *left* and *right translation by* x, respectively. The permutation group

$$\mathrm{Mlt}(Q) = \langle L_x, R_x \,:\, x \in Q\rangle$$

is called the *multiplication group of* Q, and its subloop

$$\mathrm{Inn}(Q) = \langle \varphi \in \mathrm{Mlt}(Q) \,:\, \varphi(1) = 1\rangle$$

is the *inner mapping group of* Q.

Denote by $\mathrm{Aut}(Q)$ the automorphism group of Q. An *automorphic loop* (or *A-loop*) is a loop Q in which every inner mapping is an automorphism, that is, $\mathrm{Inn}(Q) \le \mathrm{Aut}(Q)$. Note that groups are automorphic loops, but the converse is certainly not true.

The following multiplication table specifies a nonassociative automorphic loop of the smallest possible order, which we will call Q_6:

Q_6	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	6	3	5
3	3	5	1	2	6	4
4	4	3	6	5	1	2
5	5	6	2	1	4	3
6	6	4	5	3	2	1

.

Properties of Q_6 can be checked in the `GAP` [19] package `LOOPS` [38], for instance.

Bruck proved [5] that in any loop

$$\mathrm{Inn}(Q) = \langle L_{x,y},\, R_{x,y},\, T_x \,:\, x,\, y \in Q\rangle,$$

where

$$L_{x,y}(z) = (yx)\backslash(y(xz)), \quad R_{x,y}(z) = ((zx)y)/(xy), \quad \text{and} \quad T_x(y) = x\backslash(yx).$$

It is also well known that a mapping between two loops is a homomorphism of loops if and only if it respects the multiplication operation. Because this fact is of crucial importance for automorphic loops, we give a short proof:

Let $f : (A, \cdot_A, \backslash_A, /_A, 1_A) \to (B, \cdot_B, \backslash_B, /_B, 1_B)$ be a mapping between loops such that $f(x \cdot_A y) = f(x) \cdot_B f(y)$ for every x, $y \in A$. Then $f(x) \cdot_B f(x\backslash_A y) = f(x \cdot_A (x\backslash_A y)) = f(y)$ and therefore $f(x\backslash_A y) = f(x)\backslash_B f(y)$ for every x, $y \in Q$. The argument for right division is dual, and the property $f(1_A) = 1_B$ is obtained by cancelation from $f(1_A) = f(1_A \cdot_A 1_A) = f(1_A) \cdot_B f(1_A)$.

It follows that a loop Q is an automorphic loop if and only if for every x, $y \in Q$ the inner mappings $L_{x,y}$, $R_{x,y}$ and T_x respect multiplication. Consequently, the class of automorphic loops is a subvariety of the variety of loops, consisting of all loops satisfying the axioms

$$(yx)\backslash(y(x(uv))) = ((yx)\backslash(y(xu)))((yx)\backslash(y(xv))), \tag{A$_\ell$}$$

$$(((uv)x)y)/(xy) = (((ux)y)/(xy))(((vx)y)/(xy)), \tag{A$_r$}$$

$$x\backslash((uv)x) = (x\backslash(ux))(x\backslash(vx)). \tag{A$_m$}$$

In particular, subloops, factor loops and homomorphic images of automorphic loops are again automorphic loops.

We call a loop *left automorphic* if (A$_\ell$) holds, *right automorphic* if (A$_r$) holds, and *middle automorphic* if (A$_m$) holds.

The axioms (A$_\ell$), (A$_r$), (A$_m$) are somewhat long and intimidating, certainly much more so than the axiom

$$(xy)(zx) = (x(yz))x \tag{M}$$

defining Moufang loops, for instance. But the message of the axioms is easy to remember—“inner mappings respect multiplication”—and, as we shall see, automorphic loops are very much amenable to algebraic investigation.

Such an investigation started in earnest in 1956 with the work of Bruck and Paige [6]. We will retrace some of their steps, for instance by proving that automorphic loops are power-associative. The main contribution of [6], which we will not follow here, was to demonstrate that diassociative automorphic loops share many properties with Moufang loops (which are always diassociative, by Moufang's theorem [36]).

The conjecture that every diassociative automorphic loop is Moufang is implicit in [6], but its proof remained elusive for 45 years. The conjecture was established for the special case of commutative loops by Osborn in 1958 [41]. Since commutative Moufang loops are automorphic by [5] (or see Proposition 1.14), it follows from Osborn's result that commutative Moufang loops are precisely commutative diassociative automorphic loops. The full conjecture was finally confirmed by Kinyon, Kunen and Phillips in 2002 [33].

Following a few sporadic results in late 1900s and early 2000s, of which we mention [14, 17, 32, 39, 43], automorphic loops became one of the focal areas in loop theory after the work of Jedlička, Kinyon and the author on commutative automorphic loops [25, 26] was circulated. It is worth mentioning that some results of [25] were first obtained by automated deduction [35], which remains influential in this field. But once the initial hurdles were cleared, the theory opened up to more traditional modes of investigation.

New results by many authors followed in quick succession. We mention two highlights: Odd Order Theorem for automorphic loops [34], and solvability of finite commutative automorphic loops [23].

The field remains active and we hope that these survey notes will attract new researchers to automorphic loops and related areas. Open problems can be found in the last section of this paper.

From now on we will employ the following notational conventions in order to save parentheses and improve legibility. The division operations are less binding than juxtaposition, and the explicit $\cdot$ multiplication is less binding than divisions and juxtaposition. For instance, $x/y\cdot y\backslash zy$ means $(x/y)(y\backslash(zy))$.

Lecture 1: Basic properties

In this section we establish some basic properties of automorphic loops. Most of these properties were known already to Bruck and Paige [6], except that they were not aware of the fact that automorphic loops have the antiautomorphic inverse property (see [29] or Proposition 1.4) and its consequences (one of the axioms (A_ℓ), (A_r) can be ommitted by Theorem 1.6, and the left and right nuclei coincide by Theorem 1.11). Of course, they also did not know that diassociative automorphic loops are Moufang [33], a result that we have incorporated without proof into Theorem 1.12.

Many proofs presented in this section shorten older arguments. We do not hesitate to prove even folklore results to better show to the reader that most result in this section can be derived quickly from first principles. In this spirit, consider:

Lemma 1.1. *Let Q be a loop and $\varphi\in\mathrm{Aut}(Q)$. Then*

$$\varphi L_x^{\pm1}\varphi^{-1}=L_{\varphi(x)}^{\pm1},\quad \varphi R_x^{\pm1}\varphi^{-1}=R_{\varphi(x)}^{\pm1},$$
$$\varphi T_x^{\pm1}\varphi^{-1}=T_{\varphi(x)}^{\pm1},\quad \varphi L_{x,y}^{\pm1}\varphi^{-1}=L_{\varphi(x),\varphi(y)}^{\pm1},\quad \varphi R_{x,y}^{\pm1}\varphi^{-1}=R_{\varphi(x),\varphi(y)}^{\pm1}$$

for every x, $y\in Q$.

Proof. We have $\varphi L_x\varphi^{-1}(y)=\varphi(x\cdot\varphi^{-1}(y))=\varphi(x)\cdot\varphi(\varphi^{-1}(y))=\varphi(x)\cdot y=L_{\varphi(x)}(y)$, so $\varphi L_x\varphi^{-1}=L_{\varphi(x)}$. Then $\varphi L_x^{-1}\varphi^{-1}=(\varphi L_x\varphi^{-1})^{-1}=L_{\varphi(x)}^{-1}$. The argument for R_x is similar. Then $\varphi T_x\varphi^{-1}=\varphi L_x^{-1}R_x\varphi^{-1}=\varphi L_x^{-1}\varphi^{-1}\varphi R_x\varphi^{-1}=L_{\varphi(x)}^{-1}R_{\varphi(x)}=T_{\varphi(x)}$, and so on. □

Thus in any loop Q, the automorphism group $\mathrm{Aut}(Q)$ acts on $\mathrm{Mlt}(Q)$ and on $\mathrm{Inn}(Q)$ by conjugation, mapping left inner mappings to left inner mappings, and so on. If Q is an automorphic loop, then the action of $\mathrm{Aut}(Q)$ induces an action of $\mathrm{Inn}(Q)$.

1.1. Flexibility and power-associativity

A loop Q is *flexible* if $x(yx) = (xy)x$ holds for every x, $y \in Q$. A consequence of flexibility is that every element x has a (unique) two-sided inverse x^{-1}. Indeed, if x^{ℓ}, x^{r} ar the left and right inverses of x, respectively, then $x = x(x^{\ell}x) = (xx^{\ell})x$, so $xx^{\ell} = 1 = xx^{r}$ and $x^{\ell} = x^{r}$.

Proposition 1.2 ([6, p. 311]). *Every middle automorphic loop is flexible.*

Proof. Suppose that Q satisfies (A_m). Then $T_x(xy) = T_x(x) \cdot T_x(y)$, and multiplying this equality by x on the left yields $(xy)x = x(x\backslash xx \cdot x\backslash yx) = x(x \cdot x\backslash yx) = x(yx)$. □

We remark that there exists a loop (of order 6) that is both left and right automorphic, yet does not posses two-sided inverses, so is also not flexible.

A loop Q is said to be *power-associative* if for every $x \in Q$ the subloop $\langle x\rangle$ of Q generated by x is associative. For a prime p, a power-associative loop Q is said to be a *p-loop* if every element of Q has order that is a power of p.

Assuming two-sided inverses, a general strategy for proving power-associativity is as follows: Define *nominal powers* $x^{[n]}$ by letting $x^{[0]} = 1$, $x^{[k+1]} = xx^{[k]}$ and $x^{[-k]} = (x^{[k]})^{-1}$. Then it is not hard to show by induction that Q is power-associative if and only if

$$x^{[i]}(x^{[j]}x^{[k]}) = (x^{[i]}x^{[j]})x^{[k]} \tag{1.1}$$

for all i, j, $k \in \mathbb{Z}$. A typical proof of (1.1) in a given variety of loops is based on a careful induction. In automorphic loops, however, Bruck and Paige [6] employed an ingenious argument that we will essentially follow here.

Note that for any loop Q and a subset A of $\mathrm{Aut}(Q)$ the set

$$\mathrm{Fix}(A) = \{x \in Q \,:\, \varphi(x) = x \text{ for every } \varphi \in A\}$$

of common fixed points of automorphisms from A is a subloop of Q.

Proposition 1.3 ([6, Theorems 2.4 and 2.6]). *Every automorphic loop is power-associative and satisfies $(x^iy)x^j = x^i(yx^j)$, $x^i(x^jy) = x^j(x^iy)$, $(yx^i)x^j = (yx^j)x^i$ for every i, $j \in \mathbb{Z}$.*

Proof. Our loop Q is flexible by Proposition 1.2, which implies that $x \in \mathrm{Fix}(L_{y,x})$ and hence $\langle x\rangle \leq \mathrm{Fix}(L_{y,x})$. In particular, $(xy)x^{[j]} = x(yx^{[j]})$. (Note that we have not used (A_r) yet.) This means that the inner mapping $R^{-1}_{yx^{[j]}}R_{x^{[j]}}R_y$ fixes x, thus also $x^{[i]}$, and we have $(x^{[i]}y)x^{[j]} = x^{[i]}(yx^{[j]})$. As a special case we obtain (1.1), which implies power-associativity. Then x^i is well-defined, coincides with $x^{[i]}$, and $(x^iy)x^j = x^i(yx^j)$ follows.

The inner mapping $R_{xy}^{-1}L_xR_y$ trivially fixes x, so also x^i. This shows that $R_{x^iy}^{-1}L_{x^i}R_y$ fixes x, so also x^j, and $x^i(x^jy) = x^j(x^iy)$ follows. The last identity is proved dually. □

Note that the identities of Proposition 1.3 say that for a fixed x in an automorphic loop Q, the group $\langle L_{x^i},\, R_{x^i} \,:\, i \in \mathbb{Z}\rangle$ is commutative.

1.2. Antiautomorphic inverse property

A loop with two-sided inverses has the *antiautomorphic inverse property* if it satisfies the identity

$$(xy)^{-1} = y^{-1}x^{-1}. \tag{1.2}$$

We are now going to show that every automorphic loop has the antiautomorphic inverse property. For reasons that become clear, we prove a seemingly stronger result, assuming only (A_ℓ) and (A_m). We give a shorter proof than in [29].

Proposition 1.4 (compare [29, Proposition 7.4]). *Every loop that is both left and middle automorphic has the antiautomorphic inverse property.*

Proof. In the proof of Proposition 1.3 we established $(xy)x^{[j]} = x(yx^{[j]})$ using only (A_ℓ) and (A_m). In particular, we can use $(xy)x^{-1} = x(yx^{-1})$ below. Consider $\psi = L_y^{-1}L_xL_{x\backslash y} = L_{x\backslash y,x} \in \mathrm{Aut}(Q)$. Since $\psi((x\backslash y)^{-1}) = y\backslash x$, we also have $\psi(x\backslash y) = (y\backslash x)^{-1}$. Then $(y\backslash x)^{-1}\cdot y^{-1} = (y\backslash x)^{-1}\cdot y\backslash 1 = \psi(x\backslash y)\psi((x\backslash y)\backslash x^{-1}) = \psi(x^{-1}) = y\backslash(x\cdot(x\backslash y)x^{-1}) = y\backslash(x(x\backslash y)\cdot x^{-1}) = y\backslash yx^{-1} = x^{-1}$. Then (1.2) follows by substituting yx for x. □

In general, the antiautomorphic inverse property has a similar effect as commutativity in the sense that it allows one to deduce properties about right concepts from properties of left concepts, and vice versa. In the following well-known lemma, let J be the inversion mapping $x \mapsto x^{-1}$.

Lemma 1.5. *Let Q be an antiautomorphic inverse property loop. Then the inversion mapping J is an involutory antiautomorphism of Q. Moreover, $JL_xJ = R_{x^{-1}}$ and $JL_{x,y}J = R_{x^{-1},y^{-1}}$ for every x, $y \in Q$.*

Proof. With x, $y \in Q$ we have $JL_xJ(y) = (xy^{-1})^{-1} = yx^{-1} = R_{x^{-1}}(y)$, so $JL_xJ = R_{x^{-1}}$. Then $JL_{x,y}J = JL_{yx}^{-1}J\cdot JL_yJ\cdot JL_xJ = R_{(yx)^{-1}}^{-1}R_{y^{-1}}R_{x^{-1}} = R_{x^{-1}y^{-1}}^{-1}R_{y^{-1}}R_{x^{-1}} = R_{x^{-1},y^{-1}}$. □

We now easily arrive at the following important result:

Theorem 1.6 (compare [29, Theorem 7.1]). *The following properties are equivalent for a loop Q:*

(*i*) *Q is automorphic,*

(*ii*) *Q is left and middle automorphic,*

(*iii*) *Q is right and middle automorphic.*

Proof. Thanks to the duality, it suffices to establish the implication (ii) $\Rightarrow$ (i). Suppose that Q is left and middle automorphic. By Proposition 1.4, Q has the antiautomorphic inverse property. By Lemma 1.5, J is an antiautomorphism and $R_{x^{-1},y^{-1}} = JL_{x,y}J$ is an automorphism, being a composition of an automorphism and two antiautomorphisms. □

We can further exploit the inversion mapping J.

Lemma 1.7 ([34, Lemma 2.7]). *Let Q be an automorphic loop. Then J centralizes* Inn(Q). *Moreover, $L_{x,y} = R_{x^{-1},y^{-1}}$ and $T_x^{-1} = T_{x^{-1}}$ for every x, $y \in Q$.*

Proof. Because $\varphi(x^{-1}) = \varphi(x)^{-1}$ for every $x \in Q$ and $\varphi \in \mathrm{Aut}(Q)$, the inversion mapping J centralizes $\mathrm{Inn}(Q) \le \mathrm{Aut}(Q)$. Combining this with Lemma 1.5 yields $L_{x,y} = JL_{x,y}J = R_{x^{-1},y^{-1}}$. Using this fact and Proposition 1.3 yields $T_xT_{x^{-1}} = L_x^{-1}R_xL_{x^{-1}}^{-1}R_{x^{-1}} = R_xR_{x^{-1}}L_x^{-1}L_{x^{-1}}^{-1} = R_{x^{-1},x}L_{x,x^{-1}}^{-1} = R_{x^{-1},x}R_{x^{-1},x}^{-1} = 1$. □

1.3. Nuclei

As usual, define the *left*, *middle* and *right nucleus* of a loop Q by

$$N_\ell(Q) = \{a \in Q \,:\, a(xy) = (ax)y \text{ for all } x,\, y \in Q\},$$
$$N_m(Q) = \{a \in Q \,:\, x(ay) = (xa)y \text{ for all } x,\, y \in Q\},$$
$$N_r(Q) = \{a \in Q \,:\, x(ya) = (xy)a \text{ for all } x,\, y \in Q\},$$

respectively, and the *nucleus* of Q by $N(Q) = N_\ell(Q) \cap N_m(Q) \cap N_r(Q)$.

It is easy to observe that all the nuclei are associative subloops of Q. In general loops, there is no relationship between the three nuclei $N_\ell(Q)$, $N_m(Q)$ and $N_r(Q)$. On the other hand, it is well known (see below) that in inverse property loops all nuclei coincide.

Recall that a loop with two-sided inverses has the *left inverse property* if $x^{-1}(xy) = y$ holds, the *right inverse property* if $(xy)y^{-1} = x$ holds, and the *inverse property* if it has both the left and right inverse properties.

Proposition 1.8 ([5, Theorem VII.2.1]). *In antiautomorphic inverse property loops the left and right nuclei coincide. In inverse property loops all nuclei coincide.*

Proof. Suppose that Q satisfies (1.2). Then the condition $ax{\cdot}y = a{\cdot}xy$ is equivalent to $y^{-1} \cdot x^{-1}a^{-1} = y^{-1}x^{-1} \cdot a^{-1}$, so $N_\ell(Q) = N_r(Q)$. Now suppose that Q has the inverse property. From $(xy)^{-1}x = (xy)^{-1}(xy \cdot y^{-1}) = y^{-1}$ we deduce (1.2), so it remains to show that $N_\ell(Q) = N_m(Q)$. If $ax \cdot y = a \cdot xy$ then $y = (ax)^{-1}(a \cdot xy)$, and substituting $x = a^{-1}u^{-1}$, $y = ua \cdot v$ yields $ua \cdot v = y = u \cdot av$. The other inclusion follows by a similar argument. □

Suppose that Q is an automorphic loop. We know from Proposition 1.4 that Q has the antiautomorphic inverse property, and thus that $N_\ell(Q) = N_r(Q)$ by Proposition 1.8. But taking $x = 2$ and $y = 3$ in Q_6 shows that Q does not necessarily have the left or right inverse property, so there is no *a priori* reason why the nuclei of Q should coincide. In fact, there are automorphic loops Q satisfying the strict inclusion $N(Q) = N_\ell(Q) = N_r(Q) < N_m(Q)$. Theorem 1.11 shows that no other inclusions among nuclei arise in automorphic loops.

Call a subloop S of a loop Q *characteristic* if $\varphi(S) = S$ for every $\varphi \in \mathrm{Aut}(Q)$.

In general loops, nuclei are not necessarily normal subloops, but they are always characteristic subloops. For instance, if $a \in N_\ell(Q)$ and $\varphi \in \mathrm{Aut}(Q)$ then $\varphi(a) \cdot \varphi(x)\varphi(y) = \varphi(a \cdot xy) = \varphi(ax \cdot y) = \varphi(a)\varphi(x) \cdot \varphi(y)$ shows that $\varphi(a) \in N_\ell(Q)$.

In automorphic loops, nuclei are therefore normal subloops thanks to this easy but important fact:

Lemma 1.9 ([6, Theorem 2.2])**.** *Let Q be an automorphic loop and S a characteristic subloop of Q. Then S is normal in Q.*

Proof. A subloop S is normal in Q if and only if $\varphi(S) = S$ for every $\varphi \in \mathrm{Inn}(Q)$. □

Lemma 1.10. *Let Q be an automorphic loop. Then $T_xT_y(a) = T_{yx}(a)$ for every $a \in N_\ell(Q) = N_r(Q)$.*

Proof. We have already shown that $N_\ell(Q) = N_r(Q)$ is a characteristic subloop of Q. Let $u = T_x(y)$ (that is, $xu = yx$). Because $a \in N_r(Q)$, we also have $T_{xu}(a) \in N_r(Q)$, and so $x(uT_{xu}(a)) = (xu)T_{xu}(a) = a(xu)$. Since $a \in N_\ell(Q)$, we then have $T_xT_y(a) = T_x(y\backslash ay) = T_x(y)\backslash T_x(ay) = T_x(y)\backslash(x\backslash(ay)x) = T_x(y)\backslash(x\backslash a(yx)) = u\backslash(x\backslash a(xu)) = u\backslash(x\backslash x(uT_{xu}(a))) = T_{xu}(a) = T_{yx}(a)$. □

Theorem 1.11. *Let Q be an automorphic loop. Then $N(Q) = N_\ell(Q) = N_r(Q) \leq N_m(Q)$ and all nuclei are normal subloops of Q.*

Proof. All nuclei are normal by Lemma 1.9. Let $A = N_\ell(Q) = N_r(Q)$. It remains to prove that $A \leq N_m(Q)$. Note that $L_{x,y}$ and $R_{x,y}$ fix A pointwise, while $(xa)y = x(ay)$ holds if and only if $M_{x,y}(a) = a$, where $M_{x,y} = L_x^{-1}R_y^{-1}L_xR_y$.

Given $a \in A$, we want to show that $M_{x,y}(a) = a$. Now,

$$M_{x,y} = (L_x^{-1}R_x)(R_x^{-1}R_y^{-1}R_{xy})(R_{xy}^{-1}L_{xy})(L_{xy}^{-1}L_xL_y)(L_y^{-1}R_y),$$

and thus $M_{x,y} = T_xR_{x,y}^{-1}T_{xy}^{-1}L_{y,x}T_y$. While evaluating $M_{x,y}$ at a, we never leave the normal subloop A, so $M_{x,y}(a) = T_xT_{xy}^{-1}T_y(a)$. By Lemma 1.10, $M_{x,y}(a) = T_xT_{xy}^{-1}T_y(a) = T_x(T_yT_x)^{-1}T_y(a) = a$. □

The middle nucleus is important in automorphic loops but its role is not fully understood.

1.4. Diassociativity and the Moufang property

Up to this point we have carefully proved all the results. In this subsection we skip some proofs and refer the reader to the literature.

A loop has the *left alternative property* if it satisfies $x(xy) = (xx)y$ and the *right alternative property* if $x(yy) = (xy)y$ holds. A loop Q is *diassociative* if any two elements of Q generate an associative subloop.

By Moufang's theorem [36], Moufang loops are diassociative. The loop Q_6 with $x = 2$ and $y = 3$ shows that automorphic loops need not have the left alternative property nor the right alternative property so, in particular, they need not be diassociative.

Bruck and Paige proved in [6, Theorem 2.4] that the following properties are equivalent for an automorphic loop Q: Q is diassociative; Q satisfies both left and right inverse properties; Q satisfies both left and right alternative properties. Moreover, as we have already mentioned in the introduction, every diassociative automorphic loop is Moufang [33]. Thanks to Proposition 1.4, we can refine these results as follows:

Theorem 1.12. *The following properties are equivalent for an automorphic loop Q:*

(i) *Q has the left alternative property*

(ii) *Q has the right alternative property,*

(iii) *Q has the left inverse property,*

(iv) *Q has the right inverse property,*

(v) *Q is diassociative,*

(vi) *Q is Moufang.*

Proof. Suppose that Q has the left alternative property. Then Proposition 1.4 implies that $(yx \cdot x)^{-1} = x^{-1} \cdot x^{-1}y^{-1} = x^{-1}x^{-1} \cdot y^{-1} = (y \cdot xx)^{-1}$, so Q has the right alternative property. A similar argument finishes the equivalence of (i) and (ii), and also proves the equivalence of (iii) and (iv). The rest follows from [6, 33]. □

We conclude this section with Bruck's proof of the fact that commutative Moufang loops are automorphic. The argument is based on nice observations about autotopisms and companions of pseudo-automorphisms, which we review.

Let Q be a loop. A triple (f, g, h) of bijections $Q \to Q$ is an *autotopism* if $f(x)g(y) = h(xy)$ holds for every x, $y \in Q$. It is easy to see that the coordinatewise product (composition) of autotopisms is an autotopism.

If a bijection f of Q and $c \in Q$ satisfy the identity $f(x) \cdot f(y)c = f(xy)c$, then f is called a *pseudo-automorphism* of Q with *companion* c.

Lemma 1.13 (compare [5, Lemma VII.2.1]). *Let Q be a loop and (f, g, h) an autotopism of Q such that $f(1) = 1$. Then $g = h$ and $g(x) = f(x)c$, where $c = g(1)$. Hence f is a pseudo-automorphism with companion $c = g(1)$.*

Proof. We have $g(x) = f(1)g(x) = h(1 \cdot x) = h(x)$, so $g = h$. Also, $f(x)c = f(x)g(1) = h(x) = g(x)$. Finally, $f(x) \cdot f(y)c = f(x)g(y) = h(xy) = g(xy) = f(xy)c$. □

Proposition 1.14 ([5, Lemma VII.3.3]). *Commutative Moufang loops are automorphic.*

Proof. Let Q be a commutative Moufang loop. Let f be a pseudo-automorphism of Q with companion c. Then $f(x) \cdot cf(y) = f(x) \cdot f(y)c = f(xy)c = f(yx)c = f(y) \cdot f(x)c = f(x)c \cdot f(y)$ for every x, $y \in Q$, so $c \in N_m(Q)$. Since Q is an inverse property loop, its nuclei coincide by Proposition 1.8 and we have $c \in N_r(Q)$. Then c can be canceled in $f(x) \cdot f(y)c = f(xy)c$ and $f \in \mathrm{Aut}(Q)$ follows.

It therefore suffices to prove that the mappings $L_{x,y}$ are pseudo-automorphisms. The Moufang identity (M) is equivalent to the statement that $\varphi_x = (L_x, R_x, R_xL_x)$ is an autotopism of Q. Then $\varphi_{yx}^{-1}\varphi_y\varphi_x$ is an autotopism with first component $L_{x,y}$. By Lemma 1.13, $L_{x,y}$ is a pseudo-automorphism. □

Lecture 2: Associated operations

Many of the concepts presented in this section can be traced to two influential papers [20, 21] on loops of odd order written by Glauberman in the 1960s. In his study of Moufang loops $(Q, \cdot)$ of odd order [21], the most important idea was to associate another loop $(Q, \bullet)$ with $(Q, \cdot)$, defined by $x \bullet y = x^{1/2}yx^{1/2}$, where $x^{1/2}$ is the unique square root of x in $(Q, \cdot)$. The resulting loop $(Q, \bullet)$ is an instance of what would nowadays be called a Bruck loop (or a K-loop). This made Glauberman study Bruck loops of odd order and their left multiplication groups in detail [20] and establish a number of key results for them (see Theorem 2.2). He then transferred the results from Bruck loops to Moufang loops.

We follow a similar approach but in a more general setting of twisted subgroups. We show how to associate left Bruck loops with uniquely 2-divisible left Bol loops and with uniquely 2-divisible automorphic loops. We then follow [22] and establish a one-to-one correspondence between left Bruck loops of odd order and a certain class of commutative loops containing commutative automorphic loops of odd order. This will allow us to prove an analog of Theorem 2.2 for commutative automorphic loops. Finally, as in [34] we establish a one-to-one correspondence between uniquely 2-divisible automorphic loops whose associated left Bruck loop is associative and a certain class of uniquely 2-divisible Lie rings. This eventually leads to the Odd Order Theorem for automorphic loops. For the convenience of the reader, the correspondence results are visualized in Figure 2.

2.1. Bruck loops

A loop Q is a *left Bol loop* if it satisfies the *left Bol identity*

$$x(y(xz)) = (x(yx))z. \tag{2.3}$$

It is well known that left Bol loops have the left inverse property.

The following result gives a nice axiomatization of left Bol loops in the variety of magmas with inverses.

Lemma 2.1 ([31, (3.10)] and [42, Theorem 4.1])**.** *Let $(Q,\cdot)$ be a groupoid with an identity element and two-sided inverses satisfying* (2.3)*. Then $(Q,\cdot)$ is a left Bol loop.*

Consequently, a nonempty subset of a left Bol loop is a subloop if it is closed under mutiplication and inverses.

A *left Bruck loop* is a left Bol loop with the *automorphic inverse property* $(xy)^{-1} = x^{-1}y^{-1}$.

Here is an omnibus result on Bruck loops of odd order compiled from [20, 21]. Recall that the *left multiplication group* of Q is defined by $\mathrm{Mlt}_\ell(Q) = \langle L_x : x \in Q\rangle$.

Theorem 2.2 (Glauberman)**.** *Let Q be a left Bruck loop of odd order. Then Q is solvable. If $H \leq Q$ then $|H|$ divides $|Q|$. If p is a prime dividing $|Q|$ then there is $x \in Q$ such that $|x| = p$. Sylow p-subloops and Hall π-subloops of Q exist. The left multiplication group $\mathrm{Mlt}_\ell(Q)$ of Q is of odd order.*

If also $|Q| = p^k$ for an odd prime p, then Q is centrally nilpotent.

2.2. Twisted subgroups

A subset S of a group G is a *twisted subgroup* of G if it contains the identity element of G, is closed under inverses, and is closed under the binary operation $(x, y) \mapsto xyx$.

Note that a twisted subgroup is not necessarily a subgroup, but every twisted subgroup S is closed under powers. Indeed, it suffices to show that all positive powers of $x \in S$ belong to S, and we get this by induction on k from $x^{k+2} = xx^kx$.

Call a subset U of a loop Q *uniquely* 2*-divisible* if the squaring map $Q \to Q$, $x \mapsto x^2$ restricts to a bijection on U. In this case, for every $x \in U$ there is a unique element $x^{1/2} \in U$ such that $(x^{1/2})^2 = x$. If U happens to be power associative and $x \in U$ has odd order n, then $x^{1/2} = x^{(n+1)/2}$, so the square root of x is a positive power of x. If U happens to be closed under inverses, then $((x^{-1})^{1/2})^2 = x^{-1} = (x^{1/2}x^{1/2})^{-1} = (x^{1/2})^{-1}(x^{1/2})^{-1} = ((x^{1/2})^{-1})^2$ shows that $(x^{-1})^{1/2}$ is equal to $(x^{1/2})^{-1}$.

Proposition 2.3 (compare [20, Lemma 3])**.** *Let G be a group and S a uniquely* 2*-divisible twisted subgroup of G. Then $(S,\circ)$ with multiplication*

$$x \circ y = (xy^2x)^{1/2}$$

is a left Bruck loop. Moreover, the powers in $(S,\cdot)$ and $(S,\circ)$ coincide.

Proof. If x, $y \in S$ then $y^2 \in S$, $xy^2x \in S$ and $(xy^2x)^{1/2} \in S$. Hence $(S, \circ)$ is a groupoid. Since $1 \circ x = x = x \circ 1$ and $x^{-1} \circ x = (x^{-1}x^2x^{-1})^{1/2} = 1 = (xx^{-2}x)^{1/2} = x \circ x^{-1}$, we see that $(S, \circ)$ has identity element 1 and two-sided inverses. Note that $x \circ (y \circ x) = (xyx^2yx)^{1/2} = ((xyx)^2)^{1/2} = xyx$. Thus $x \circ (y \circ (x \circ z)) = (xyxz^2xyx)^{1/2} = (xyx) \circ z = (x \circ (y \circ x)) \circ z$. By Lemma 2.1, $(S, \circ)$ is a left Bol loop in which inverses coincide with those of $(S, \cdot)$. It is a left Bruck loop thanks to $(x \circ y)^{-1} = ((xy^2x)^{1/2})^{-1} = ((xy^2x)^{-1})^{1/2} = (x^{-1}y^{-2}x^{-1})^{1/2} = x^{-1} \circ y^{-1}$. The inductive step $x \circ x^{n+1} = (xx^{2n+2}x)^{1/2} = x^{n+2}$ shows that powers in $(S, \cdot)$ and $(S, \circ)$ coincide. □

A twisted subgroup of a uniquely 2-divisible group need not be uniquely 2-divisible (consider $\mathbb{Z}$ in $(\mathbb{Q}, +)$). But note that if G is a group of odd order then any twisted subgroup S of G is uniquely 2-divisible.

The next result shows that in many varieties of loops the concepts “uniquely 2-divisible” and “of odd order” coincide for finite loops.

Lemma 2.4. *Let Q be a finite power-associative loop in which $|x|$ divides $|Q|$ for every $x \in Q$. Then the following conditions are equivalent:*

(*i*) *Q is uniquely 2-divisible,*

(*ii*) *$|Q|$ is odd,*

(*iii*) *$|x|$ is odd for every $x \in Q$.*

Proof. Condition (*ii*) implies (*iii*) by the assumption that $|x|$ divides $|Q|$. Conversely, if (*iii*) holds then the inversion mapping $x \mapsto x^{-1}$ is an involution with a unique fixed point $x = 1$, so $|Q|$ is odd.

If (*i*) holds then $x^2 = 1$ implies $x = 1$, so (*iii*) holds. Conversely, if (*iii*) holds, then $|x| = 2n + 1$ implies $(x^{n+1})^2 = x^{2n+2} = x$, so the squaring map is onto Q. Thanks to finiteness of Q, it is also one-to-one, and (*i*) follows. □

2.3. Bruck loops associated with Bol and automorphic loops

If G is a uniquely 2-divisible group, Proposition 2.3 with $S = G$ yields a uniquely 2-divisible left Bruck loop $(G, \circ)$, the (*left*) *Bruck loop associated with* G.

Proposition 2.3 cannot be used directly to associate left Bruck loops with nonassociative loops Q. The trick is to work with a certain twisted subgroup S of $\mathrm{Mlt}(Q)$ instead and then project the operation $\circ$ from S to Q. The classical example is that of uniquely 2-divisible left Bol loops, which we recall in Proposition 2.5.

Proposition 2.5 ([18]). *Let $(Q, \cdot)$ be a left Bol loop. Then $L_Q = \{L_x : x \in Q\}$ is a twisted subgroup of $\mathrm{Mlt}_\ell(Q)$ satisfying*

$$L_xL_yL_x = L_{x(yx)}. \tag{2.4}$$

If $(Q,\cdot)$ is also uniquely 2-divisible, then L_Q is uniquely 2-divisible and $(Q,\circ)$ with multiplication

$$x\circ y = (x(y^2x))^{1/2} \tag{2.5}$$

is a left Bruck loop in which powers coincide with those of $(Q,\cdot)$. When Q is finite then any subloop of $(Q,\cdot)$ is a subloop of $(Q,\circ)$.

Proof. We have $1 = L_1 \in L_Q$, $L_x^{-1} = L_{x^{-1}} \in L_Q$ thanks to the left inverse property, and (2.4) follows from (2.3). Therefore L_Q is a twisted subgroup of $\mathrm{Mlt}_\ell(Q)$. An easy induction with (2.4) shows that $L_x^n = L_{x^n}$ for every $n\ge 0$.

Suppose that $(Q,\cdot)$ is uniquely 2-divisible. The mapping $Q\to L_Q$, $x\mapsto L_x$ is a bijection since $L_x(1)=x$. Since $(L_{x^{1/2}})^2 = L_{(x^{1/2})^2} = L_x$, it follows that L_Q is uniquely 2-divisible with $L_x^{1/2} = L_{x^{1/2}}$. By Proposition 2.3, $(L_Q,\circ)$ with multiplication $L_x\circ L_y = (L_xL_y^2L_x)^{1/2} = L_{(x(y^2x))^{1/2}}$ is a left Bruck loop with powers coinciding with those of $\mathrm{Mlt}_\ell(Q)$.

We claim that $\varphi : (L_Q,\circ)\to(Q,\circ)$, $L_x\mapsto x$ is an isomorphism of loops. Indeed, φ is clearly a bijection and $\varphi(L_x\circ L_y) = \varphi(L_{(x(y^2x))^{1/2}}) = (x(y^2x))^{1/2} = x\circ y = \varphi(L_x)\circ\varphi(L_y)$.

Finally, suppose that Q is finite and $S\le(Q,\cdot)$. To show that S is a subloop of $(Q,\circ)$, it suffices to prove that it is closed under inverses and under the multiplication $\circ$. The former is true because the inverses in $(Q,\cdot)$ and $(Q,\circ)$ coincide, and the latter is true because $(S,\cdot)$ is closed under $\cdot$ and square roots (being positive integral powers in the finite case). □

A twisted subgroup in $\mathrm{Mlt}(Q)$ is harder to find for automorphic loops. For $x\in Q$ define

$$P_x = R_xL_{x^{-1}}^{-1}.$$

Note that in automorphic loops we have $P_x = L_{x^{-1}}^{-1}R_x$ by Proposition 1.3.

Proposition 2.6 ([34, Proposition 4.2])**.** *Let $(Q,\cdot)$ be an automorphic loop. Then $P_Q = \{P_x : x\in Q\}$ is a twisted subgroup of $\mathrm{Mlt}(Q)$ satisfying*

$$P_xP_yP_x = P_{P_x(y)} = P_{(x^{-1}\backslash y)x}. \tag{2.6}$$

If $(Q,\cdot)$ is also uniquely 2-divisible, then P_Q is uniquely 2-divisible and $(Q,\circ)$ with multiplication

$$x\circ y = ((x^{-1}\backslash y^2)x)^{1/2} = (x^{-1}\backslash y^2x)^{1/2} \tag{2.7}$$

is a left Bruck loop in which powers coincide with those of $(Q,\cdot)$. When Q is finite then any subloop of $(Q,\cdot)$ is a subloop of $(Q,\circ)$.

Proof. We have $1 = P_1\in P_Q$. Proposition 1.3 and Lemma 1.7 yield

$$P_xP_{x^{-1}} = R_xL_{x^{-1}}^{-1}R_{x^{-1}}L_x^{-1} = L_{x^{-1}}^{-1}R_{x^{-1}}L_x^{-1}R_x = T_{x^{-1}}T_x = 1,$$

so $P_x^{-1} = P_{x^{-1}} \in P_Q$. The identity (2.6) is nontrivial; see [34, Proposition 3.4] for a proof. Therefore P_Q is a twisted subgroup of $\mathrm{Mlt}(Q)$. An easy induction with (2.6) yields $P_x^n = P_{x^n}$ for every $n \geq 0$, using $P_x(x^i) = (x^{-1}\backslash x^i)x = x^{i+2}$.

Suppose that $(Q, \cdot)$ is uniquely 2-divisible. The mapping $Q \to P_Q$, $x \mapsto P_x$ is a bijection since $P_x(1) = x^2$. Since $P_{x^{1/2}}^2 = P_{(x^{1/2})^2} = P_x$, it follows that P_Q is uniquely 2-divisible with $P_x^{1/2} = P_{x^{1/2}}$. By Proposition 2.3, $(P_Q, \circ)$ with multiplication $P_x \circ P_y = (P_x P_y^2 P_x)^{1/2} = P_{((x^{-1}\backslash y^2)x)^{1/2}}$ is a left Bruck loop with powers coinciding with those of $\mathrm{Mlt}(Q)$. Note that $(x^{-1}\backslash y)x = x^{-1}\backslash yx$ by Proposition 1.3.

We conclude as in the proof of Proposition 2.5, using the bijection $P_x \mapsto x$. □

When $(Q, \cdot)$ is a uniquely 2-divisible automorphic loop, we call $(Q, \circ)$ from Proposition 2.6 the *left Bruck loop associated with* $(Q, \cdot)$.

It is worth noting that in left Bol loops we have $x^{-1}\backslash y^2 = xy^2$ thanks to the left inverse property. So, in left Bol loops, the operation (2.5) of Proposition 2.5 coincides with the operation (2.7) of Proposition 2.6. But neither result is a special case of the other.

We can now easily deduce Cauchy's and Lagrange's theorems for automorphic loops of odd order from Theorem 2.2.

Theorem 2.7. *Let Q be an automorphic loop of odd order. If S is a subloop of Q then $|S|$ divides $|Q|$. If p is a prime dividing $|Q|$ then Q contains an element of order p.*

Proof. Let $(Q, \circ)$ be the left Bruck loop associated with Q. If $S \leq Q$ then $(S, \circ) \leq (Q, \circ)$ by Proposition 2.6. By Theorem 2.2, $|S|$ divides $|Q|$. Let p be a prime dividing $|Q|$. Then there is $x \in (Q, \circ)$ of order p by Theorem 2.2. Because powers in Q and $(Q, \circ)$ coincide, x has also order p in Q. □

Corollary 2.8. *Every automorphic loop of prime order is associative.*

Note that we cannot easily use Proposition 2.6 to obtain the Odd Order Theorem for automorphic loops from the Odd Order Theorem for Bruck loops, for instance. The difficulty lies in the fact that it is not clear how subloops of $(Q, \circ)$ are related to subloops of $(Q, \cdot)$.

2.4. Correspondence with Bruck loops

By Proposition 2.6, if $(Q, \cdot)$ is a uniquely 2-divisible automorphic loop then P_Q is a twisted subgroup of $\mathrm{Mlt}(Q)$ satisfying (2.6), which induces a left Bruck loop operation $(Q, \circ)$ by $x \circ y = (x^{-1}\backslash y^2 x)^{1/2}$. However, there exist distinct uniquely 2-divisible automorphic loops with the same associated left Bruck loops, so it is not possible to find an inverse to the mapping $(Q, \cdot) \mapsto (Q, \circ)$.

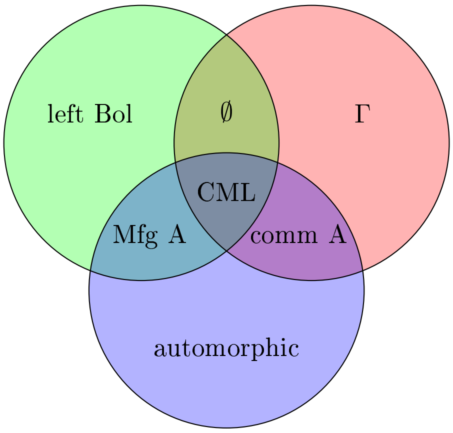

Figure 1: Intersections among left Bol loops, automorphic loops and Γ-loops.

In an attempt to find a correspondence between uniquely 2-divisible left Bruck loops and some class of loops, Greer [22] defined a technical variety of loops as follows.

A loop Q is a Γ-*loop* if it is commutative, has the automorphic inverse property, satisfies $L_xL_{x^{-1}} = L_{x^{-1}}L_x$ and $P_xP_yP_x = P_{P_x(y)}$. Note that the last condition is just (2.6). By [22, Theorem 3.5], Γ-loops are power-associative.

Figure 1 gives a Venn diagram of intersections of the varieties of left Bol loops, automorphic loops and Γ-loops. Here is a full justification for the diagram. If Q is an automorphic Γ-loop then it is a commutative automorphic loop; conversely, a commutative automorphic loop is certainly automorphic and it satisfies the automorphic inverse property by Proposition 1.4, the relation $L_xL_{x^{-1}} = L_{x^{-1}}L_x$ by Proposition 1.3, and (2.6) by [34, Proposition 3.4]. If Q is left Bol and automorphic then the antiautomorphic inverse property implies that Q is Moufang (and automorphic); the converse is trivial. If Q is left Bol and a Γ-loop then it is a commutative Moufang loop. If Q is Moufang and a Γ-loop then it is a commutative Moufang loop. Finally, a commutative Moufang loop is automorphic by Proposition 1.14.

When $(Q,\cdot)$ is a uniquely 2-divisible Γ-loop, we can use the same construction as in the case of uniquely 2-divisible automorphic loops to obtain the *associated left Bruck loop* $(Q,\circ)$, namely $x\circ y = (x^{-1}\backslash y^2x)^{1/2}$. In the end, the variety of Γ-loops was chosen so that the proof of this result can mimic the proof in the automorphic case. (For instance, the difficult identity (2.6) is part of the definition of Γ-loops.) See [22, Theorem 4.9] for details.

Following Greer, we will now show how to construct a left Bruck loop Q from a Γ-loop of odd order. (See the discussion after Lemma 2.11 for an obstacle in the more general uniquely 2-divisible case.) We will actually use the twisted subgroup

L_Q again, but with a different operation.

On a uniquely 2-divisible group $(G,\cdot)$, let

$$x * y = xy[y,x]^{1/2}, \tag{2.8}$$

where $[x,y] = x^{-1}y^{-1}xy$ is the usual commutator.

Straightforward, albeit nontrivial calculation with the commutator in groups yields:

Lemma 2.9 ([22, Theorem 2.5])**.** *Let $(G,\cdot)$ be a uniquely 2-divisible group. Then $(G,*)$ defined by* (2.8) *is a Γ-loop. Powers in $(G,\cdot)$ and $(G,*)$ coincide.*

Let us now consider a twisted subgroup seemingly unrelated to L_Q; see [4, 18, 20]. For a group G and $\tau \in \mathrm{Aut}(G)$ let

$$K(\tau) = \{x \in G \,:\, \tau(x) = x^{-1}\}.$$

We claim that $K(\tau)$ is a twisted subgroup of G. Indeed, $1 \in K(\tau)$ is clear, if $x \in K(\tau)$ then $\tau(x^{-1}) = \tau(x)^{-1} = (x^{-1})^{-1}$, so $x^{-1} \in K(\tau)$, and if x, $y \in K(\tau)$ then $\tau(xyx) = \tau(x)\tau(y)\tau(x) = x^{-1}y^{-1}x^{-1} = (xyx)^{-1}$, so $xyx \in K(\tau)$.

Lemma 2.10 (compare [18, Theorem 4.3])**.** *Let G be a group and $\tau \in \mathrm{Aut}(G)$. Let S be a twisted subgroup of G such that $S \subseteq K(\tau)$ and $\langle S\rangle = G$. Then $\{x^2 \,:\, x \in K(\tau)\} \subseteq S$. In particular, if G is a uniquely 2-divisible group then $S = K(\tau)$.*

Proof. Let $x \in K(\tau)$. Then $x^2 = x\tau(x^{-1})$. Since $\langle S\rangle = G$, there are $x_1, \ldots, x_n \in S$ such that $x = x_1 \cdots x_n$. Then $x\tau(x^{-1}) = x_1 \cdots x_n\tau(x_n^{-1} \cdots x_1^{-1}) = x_1 \cdots x_n\tau(x_n^{-1}) \cdots \tau(x_1^{-1}) = x_1 \cdots x_n x_n \cdots x_1$, where we have used $x_i \in S \subseteq K(\tau)$. An easy induction on n shows that the element $x_1 \cdots x_n x_n \cdots x_1$ belongs to the twisted subgroup S.

We have proved $\{x^2 \,:\, x \in K(\tau)\} \subseteq S \subseteq K(\tau)$. Suppose that G is uniquely 2-divisible. The squaring map is then injective on any twisted subgroup, and we claim that it is surjective on $K(\tau)$, so that $K(\tau)$ is uniquely 2-divisible. Indeed, if $x \in K(\tau)$ then $\tau(x^{1/2}) = \tau(x)^{1/2} = (x^{-1})^{1/2} = (x^{1/2})^{-1}$, so $x^{1/2} \in K(\tau)$. It follows that $K(\tau) = \{x^2 \,:\, x \in K(\tau)\}$, and $S = K(\tau)$. □

Lemma 2.11 (compare [22, Lemma 4.3])**.** *Let G be a uniquely 2-divisible group and let $\tau \in \mathrm{Aut}(G)$. Then $K(\tau)$ is a subloop of the Γ-loop $(G,*)$.*

Proof. By Lemma 2.9, $(G,*)$ is a Γ-loop. If x, $y \in K(\tau)$ then $\tau(x*y) = \tau(xy[y,x]^{1/2}) = \tau(x)\tau(y)[\tau(y),\tau(x)]^{1/2} = x^{-1}y^{-1}[y^{-1},x^{-1}]^{1/2} = x^{-1} * y^{-1} = (x*y)^{-1}$, where we have used the automorphic inverse property in the last step.

Let us now consider left division in $(G,*)$. The following statements are equivalent: $x * a = y$, $xa[a,x]^{1/2} = y$, $[a,x] = (a^{-1}x^{-1}y)^2$, $ax = ya^{-1}x^{-1}y$, $ay^{-1}a = x^{-1}yx^{-1}$, $(ay^{-1})^2 = x^{-1}yx^{-1}y^{-1}$, $a = (x^{-1}yx^{-1}y^{-1})^{1/2}y$. Since this is a term in $(G,\cdot)$, we can easily show that $K(\tau)$ is closed under left division in $(G,*)$. □

We would now like to apply Lemmas 2.9 and 2.11. However, there are examples of uniquely 2-divisible left Bruck loops Q with $G = \mathrm{Mlt}_\ell(Q)$ not uniquely 2-divisible, so the lemmas cannot be applied directly. We therefore focus on the odd case.

Proposition 2.12 ([22]). *Let $(Q,\cdot)$ be a left Bruck loop of odd order and let $G = \mathrm{Mlt}_\ell(Q,\cdot)$. Then $(L_Q,*)$ is a Γ-loop, and $(Q,*)$ with multiplication*

$$x * y = (L_x * L_y)(1) = (L_xL_y[L_y,L_x]^{1/2})(1)$$

is a Γ-loop.

Proof. Proposition 2.5 shows that L_Q is a twisted subgroup of $\mathrm{Mlt}_\ell(Q,\cdot)$. Let τ be the conjugation on $\mathrm{Sym}(Q)$ by the inversion map J of $(Q,\cdot)$. For x, $y \in Q$, we have $JL_xJ(y) = J(xy^{-1}) = x^{-1}y = L_{x^{-1}}(y) = L_x^{-1}(y)$ by the automorphic inverse property and the left inverse property. Because $\langle L_Q\rangle = G$, the established identity $\tau(L_x) = JL_xJ = L_{x^{-1}} = L_x^{-1}$ shows that $\tau \in \mathrm{Aut}(G)$ and also that $L_Q \subseteq K(\tau)$.

By Theorem 2.2, $|G|$ is odd. By Lemma 2.4, G is uniquely 2-divisible. Lemma 2.10 with $S = L_Q$ then gives $L_Q = K(\tau)$. By Lemma 2.11, $(L_Q,*) = (K(\tau),*)$ is a subloop of the Γ-loop $(G,*)$. Finally, as usual, we transfer the operation $*$ from $(L_Q,*)$ to $(Q,*)$ by the isomorphism $L_x \mapsto x$. □

For a left Bruck loop $(Q,\cdot)$ of odd order, we call $(Q,*)$ from Proposition 2.12 the *Γ-loop associated with* $(Q,\cdot)$.

Greer went on to establish the announced one-to-one correspondence, and more:

Theorem 2.13 ([22, Theorem 5.2]). *There is a categorical equivalence between left Bruck loops of odd order and Γ-loops of odd order. Given a Γ-loop $(Q,\cdot)$ of odd order, we let $(Q,\circ)$ be the associated left Bruck loop with multiplication $x \circ y = (x^{-1}\backslash y^2x)^{1/2}$. Conversely, given a Bruck loop $(Q,\circ)$ of odd order, we let $(Q,\cdot)$ be the associated Γ-loop with multiplication $x \cdot y = (L_xL_y[L_y,L_x]^{1/2})(1)$, where L_x is the left translation in $(Q,\circ)$.*

Solvability, Lagrange and Cauchy theorems for commutative automorphic loops of odd order were for the first time established in [25]. (See Theorems 3.11 and 3.12 for the even case.) The fact that commutative automorphic loops of odd order p^k (p a prime) are centrally nilpotent was proved independently in [9] and [27].

Theorem 2.13 allows us to obtain these and additional results from Glauberman's Theorem 2.2 not only for commutative automorphic loops of odd order but also for the larger class of Γ-loops of odd order.

Theorem 2.14 ([22, Section 6]). *Let Q be a Γ-loop of odd order. Then Q is solvable and the Lagrange and Cauchy theorems hold for Q. Moreover, there are Sylow p- and Hall π-subloops in Q.*

If also $|Q| = p^k$ for an odd prime p, then Q is centrally nilpotent.

2.5. Correspondence with Lie rings

The correspondence between left Bruck loops of odd order and Γ-loops of odd order covered all commutative automorphic loops of odd order as a subclass of Γ-loops, but it did not cover all automorphic loops of odd order. In [34], a one-to-one correspondence was found between uniquely 2-divisible automorphic loops whose associated left Bruck loop is an abelian group on the one hand, and uniquely 2-divisible Lie rings satisfying conditions (2.10), (2.11) on the other hand (see Theorem 2.18). This partial correspondence is sufficient to establish the Odd Order Theorem for automorphic loops (Theorem 2.21). In this subsection we sketch the proofs of these results.

We start with a construction of Wright [46]. Let us call $(Q,+,[.,.])$ an *algebra* if $(Q,+)$ is a an abelian group and $[.,.]$ is biadditive, that is $[x+y,z]=[x,z]+[y,z]$ and $[x,y+z]=[x,y]+[x,z]$ for every x, y, $z\in Q$. In this situation, for every $x\in Q$ define

$$\mathrm{ad}^{\ell}_x : Q\to Q,\ \mathrm{ad}^{\ell}_x(y)=[x,y],\quad \mathrm{ad}^{r}_x : Q\to Q,\ \mathrm{ad}^{r}_x(y)=[y,x]$$

to be the *left* and *right adjoint maps of* x, respectively. Note that ad^{ℓ}_x, ad^{r}_x are just the left and right translations with respect to the binary operation $[.,.]$, respectively. Finally, for $x\in Q$ define

$$\ell_x=\mathrm{id}_Q-\mathrm{ad}^{\ell}_x,\quad r_x=\mathrm{id}_Q-\mathrm{ad}^{r}_x.$$

Proposition 2.15 (see [46, Proposition 8] and [34, Lemma 5.1])**.** *Let $(Q,+,[.,.])$ be an algebra. Define a groupoid $(Q,\cdot)$ by*

$$x\cdot y=x+y-[x,y]. \tag{2.9}$$

Then $(Q,\cdot)$ is a loop (necessarily with identity element 0) if and only if

$$\ell_x \text{ and } r_x \text{ are bijections of } Q \tag{2.10}$$

for every $x\in Q$.

When $(Q,\cdot)$ is a loop with left and right translations L_x, R_x, respectively, then

$$L_x(y)=x+\ell_x(y),\ R_x(y)=x+r_x(y),\ L_x^{-1}(y)=\ell_x^{-1}(y-x),\ R_x^{-1}(y)=r_x^{-1}(y-x).$$

Moreover, $L_{x,y}=\ell_{yx}^{-1}\ell_y\ell_x$, $R_{x,y}=r_{xy}^{-1}r_yr_x$ and $T_x=\ell_x^{-1}r_x$.

Proof. We have $0\cdot x=x=x\cdot 0$ for every $x\in Q$. Note that $x\cdot y=x+\ell_x(y)=y+r_y(x)$. Hence L_x bijects if and only if ℓ_x bijects, and R_y bijects if and only if r_y bijects.

The formulas for L_x, R_x, L_x^{-1}, R_x^{-1} are straightforward. Let us calculate $L_{x,y}$. Note that every ℓ_x is additive, being a sum of two additive maps. We have

$$\begin{aligned}L_{x,y}(z)&=L_{yx}^{-1}L_yL_x(z)=L_{yx}^{-1}L_y(x+\ell_x(z))=L_{yx}^{-1}(y+\ell_y(x+\ell_x(z)))\\&=\ell_{yx}^{-1}(y+\ell_y(x)+\ell_y\ell_x(z)-yx)=\ell_{yx}^{-1}(yx+\ell_y\ell_x(z)-yx)\\&=\ell_{yx}^{-1}\ell_y\ell_x(z).\end{aligned}$$

Similarly for $R_{x,y}$ and T_x. □

Following Wright, we call $(Q,\cdot)$ the *linear groupoid* of the algebra $(Q,+,[.,.])$, and the *linear loop* of $(Q,+,[.,.])$ if (2.10) holds. In view of Proposition 2.15, it is easy to express but difficult to understand in terms of properties of $[.,.]$ when the linear loop $(Q,\cdot)$ is automorphic. We therefore specialize to the setting of Lie rings.

An algebra $(Q,+,[.,.])$ is *alternating* if $[x,x]=0$ for every $x\in Q$. Every alternating algebra is *skew-symmetric*, that is, $[x,y]=-[y,x]$. (Proof: Expand $0=[x+y,x+y]$.)

We say that an algebra $(Q,+,[.,.])$ is *uniquely* 2*-divisible* if the abelian group $(Q,+)$ is uniquely 2-divisible.

If $(Q,+,[.,.])$ is alternating, then $x\cdot x=x+x-[x,x]=2x$, so the associated linear groupoid is uniquely 2-divisible if and only if $(Q,+,[.,.])$ is uniquely 2-divisible.

A *Lie ring* is an alternating algebra $(Q,+,[.,.])$ in which $[.,.]$ satisfies the *Jacobi identity* $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$.

Even for Lie rings it is not easy to characterize when the associated linear loop is automorphic. We therefore analyze a stronger condition, namely ℓ_x and r_x being automorphisms.

Lemma 2.16 (compare [34, Proposition 5.2])**.** *Let* $(Q,+,[.,.])$ *be a Lie ring and let* $(Q,\cdot)$ *be defined by* (2.9)*. Then* $(Q,\cdot)$ *is a loop and all mappings* ℓ_x*,* r_x *are automorphisms of* $(Q,\cdot)$ *if and only if conditions* (2.10) *and*

$$[[x,Q],[x,Q]]=0 \tag{2.11}$$

hold for every $x\in Q$*. In such a case,* $(Q,\cdot)$ *is automorphic.*

Proof. By Proposition 2.15, $(Q,\cdot)$ is a loop if and only if (2.10) holds. We therefore assume that (2.10) holds and investigate when the bijections ℓ_x, r_x are automorphisms of $(Q,\cdot)$. Using skew-symmetry and the Jacobi identity freely, we have

$$\begin{aligned}
\ell_x(u)\ell_x(v) &= \ell_x(u)+\ell_x(v)-[\ell_x(u),\ell_x(v)]\\
&= u-[x,u]+v-[x,v]-[u-[x,u],v-[x,v]]\\
&= (u+v-[u,v])-[x,u+v]+([u,[x,v]]+[[x,u],v])-[[x,u],[x,v]]\\
&= (u+v-[u,v])-[x,u+v]+[x,[u,v]]-[[x,u],[x,v]]\\
&= (u+v-[u,v])-[x,u+v-[u,v]]-[[x,u],[x,v]]\\
&= uv-[x,uv]-[[x,u],[x,v]]=\ell_x(uv)-[[x,u],[x,v]].
\end{aligned}$$

Therefore $\ell_x\in\mathrm{Aut}(Q,\cdot)$ if and only if (2.11) holds. The calculation for r_x is similar.

By Proposition 2.15, $\mathrm{Inn}(Q,\cdot)\le\langle\ell_x,\,r_x\,:\,x\in Q\rangle$. Therefore, if ℓ_x, $r_x\in\mathrm{Aut}(Q,\cdot)$ for every $x\in Q$, the loop $(Q,\cdot)$ is automorphic. □

Our eventual goal is to prove the Odd Order Theorem for automorphic loops, so we focus on the uniquely 2-divisible case.

Lemma 2.17. *Let $(Q,+,[.,.])$ be a uniquely 2-divisible Lie ring satisfying* (2.10) *and* (2.11). *Let $(Q,\cdot)$ be the (uniquely 2-divisible automorphic) linear loop of $(Q,+,[.,.])$. Let $(Q,\circ)$ be the (uniquely 2-divisible) left Bruck loop associated with $(Q,\cdot)$. Then $(Q,\circ)=(Q,+)$ is an abelian group.*

Proof. We have $x^2=x+x-[x,x]=2x$, so $x^{1/2}=x/2$. Also, $x(-x)=x+(-x)+[x,-x]=0$ shows $x^{-1}=-x$. Then $x\circ y=(x^{-1}\backslash y^2x)^{1/2}=((-x)\backslash(2y)x)/2$. Therefore, the condition $x\circ y=x+y$ is equivalent to $(2y)x=(-x)\cdot(2(x+y))$, which is equivalent to $2y+x-[2y,x]=-x+2(x+y)-[-x,2(x+y)]$, which follows easily because $[.,.]$ is alternating and biadditive. □

We have shown how to construct uniquely 2-divisible automorphic loops from certain uniquely 2-divisible Lie rings. In order to build a correspondence, we now need to return from uniquely 2-divisible automorphic loops $(Q,\cdot)$ to Lie rings, i.e., we need to build operations $+$ and $[.,.]$ on $(Q,\cdot)$. Lemma 2.17 suggests to restrict our attention to the class of uniquely 2-divisible automorphic loops whose associated left Bruck loop is an abelian group, and set $x+y=x\circ y$. This approach works. See [34] for a proof.

Theorem 2.18 ([34, Theorem 5.7])**.** *Suppose that $(Q,+,[\cdot,\cdot])$ is a uniquely 2-divisible Lie ring satisfying* (2.10) *and* (2.11). *Then $(Q,\cdot)$ defined by* (2.9) *is a uniquely 2-divisible automorphic loop whose associated left Bruck loop $(Q,\circ)$ is an abelian group (in fact, $(Q,\circ)=(Q,+)$).*

Conversely, suppose that $(Q,\cdot)$ is a uniquely 2-divisible automorphic loop whose associated left Bruck loop $(Q,\circ)$ is an abelian group. Then $(Q,\circ,[\cdot,\cdot])$ defined by

$$[x,y]=x\circ y\circ(xy)^{-1} \tag{2.12}$$

is a uniquely 2-divisible Lie ring satisfying (2.10) *and* (2.11).

Furthermore, the two constructions are inverse to one another. Subrings (resp. ideals) of the Lie ring are subloops (resp. normal subloops) of the corresponding automorphic loop, and subloops (resp. normal subloops) closed under square roots are subrings (resp. ideals) of the corresponding Lie ring.

Figure 2 summarizes what we have learned so far. In the figure, all algebras are of odd order, left Bruck loops are blue, Γ-loops are red, automorphic loops are green, and Lie rings satisfying (2.10) and (2.11) are cyan. Dotted lines represent abelian groups. Automorphic loops whose associated left Bruck loops are associative are dashed green. Shaded regions represent one-to-one correspondences. Except for the associated operation $x\cdot y=L_xL_y[L_y,L_x]^{1/2}(1)$, all associated operations make sense in the uniquely 2-divisible case, too.

We now work toward the Odd Order Theorem for automorphic loops.

Lemma 2.19 ([34, Lemma 5.8])**.** *Let $(Q,+,[.,.])$ be a uniquely 2-divisible Lie ring. Then* (2.11) *holds if and only if $(Q,+,[.,.])$ is solvable of length 2, that is, $[[Q,Q],[Q,Q]]=0$.*

pgf@stop

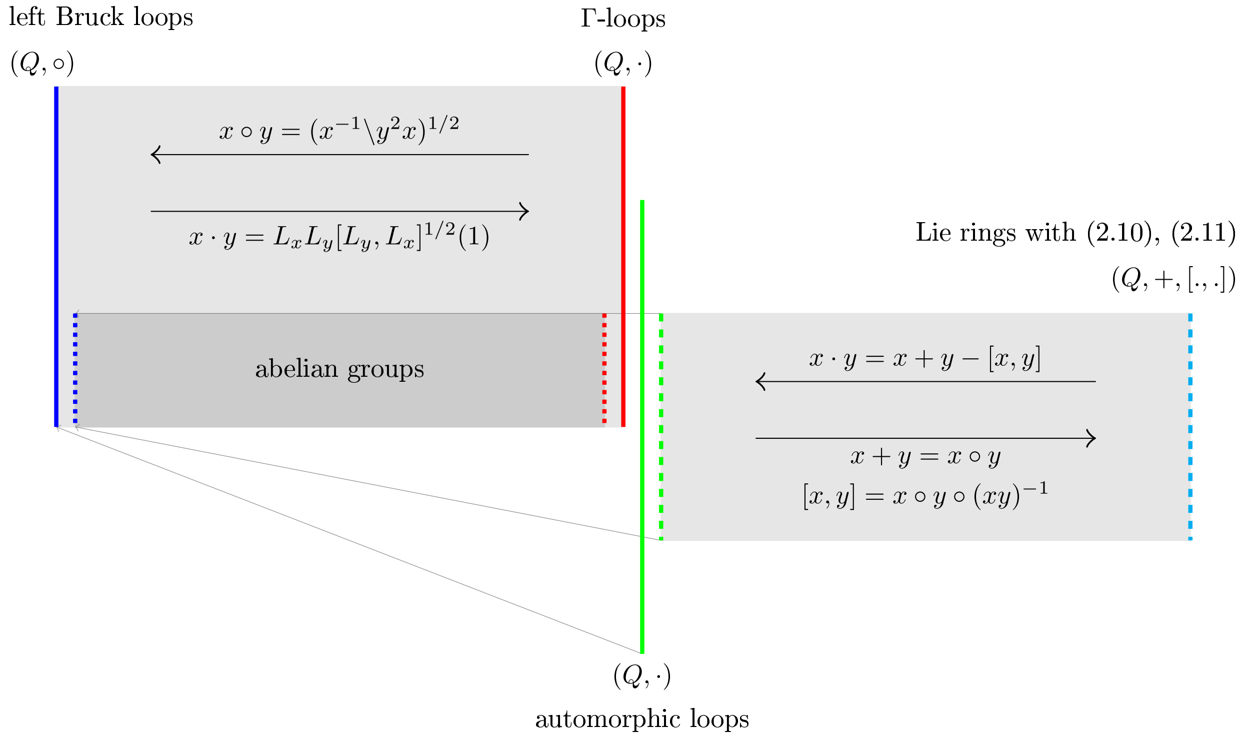
left Bruck loops
$(Q,\circ)$
Γ-loops
$(Q,\cdot)$
$x \circ y = (x^{-1}\backslash y^2 x)^{1/2}$
$x \cdot y = L_x L_y [L_y, L_x]^{1/2}(1)$
abelian groups
Lie rings with (2.10), (2.11)
$(Q,+,[.,.])$
$x \cdot y = x + y - [x,y]$
$x + y = x \circ y$
$[x,y] = x \circ y \circ (xy)^{-1}$
$(Q,\cdot)$
automorphic loops

Figure 2: Associated operations between left Bruck loops, Γ-loops, automorphic loops and Lie rings of odd order.

Lemma 2.20 ([34, Lemma 6.5]). *Let $(Q,\cdot)$ be an automorphic loop of odd order, let $(Q,\circ)$ be the associated left Bruck loop, and let S be a characteristic subloop of $(Q,\circ)$. Then S is a normal subloop of $(Q,\cdot)$.*

Proof. Since $x\circ y = (x^{-1}\backslash y^2x)^{1/2}$, we have $\mathrm{Aut}(Q,\cdot)\le\mathrm{Aut}(Q,\circ)$. Thus S is invariant under $\mathrm{Inn}(Q,\cdot)\le\mathrm{Aut}(Q,\cdot)$. Let u, $v\in S$. We will show that vu and $v/u\in S$. Let $w=v^{1/2}$. Since powers in $(Q,\cdot)$ and $(Q,\circ)$ coincide, $w\in S$. Then $T_u((u\circ w)^2)=(T_u(u\circ w))^2=(T_u(u)\circ T_u(w))^2=(u\circ T_u(w))^2=u^{-1}\backslash T_u(w)^2u=u^{-1}\backslash T_u(v)u=L_{u^{-1}}^{-1}R_uT_u(v)=L_{u^{-1}}^{-1}L_u^{-1}R_u^2(v)$ is an element of S, where we have used Proposition 1.3 in the last equality. Since $L_uL_{u^{-1}}\in\mathrm{Inn}(Q,\cdot)$, it follows that $R_u^2(v)\in S$. By induction, $R_u^{2m}(v)\in S$ for every m. By Lemma 2.4, $|u|=2m+1$ for some m. Then $R_u^{2m+1}\in\mathrm{Inn}(Q,\cdot)$, so also $R_u^{-2m}R_u^{2m+1}(v)=vu$ and $R_u^{-2m-2}R_u^{2m+1}(v)=v/u\in S$. By the antiautomorphic inverse property for $(Q,\cdot)$, $v\backslash u\in S$, too.

We have shown that S is a subloop of $(Q,\cdot)$. It is a normal subloop because S is invariant under $\mathrm{Inn}(Q,\cdot)$. □

Theorem 2.21 ([34, Theorem 6.6]). *Automorphic loops of odd order are solvable.*

Proof. Let $(Q,\cdot)$ be a minimal counterexample. If S is a nontrivial, proper normal subloop of $(Q,\cdot)$ then, by minimality, both S and $(Q,\cdot)/S$ are solvable automorphic loops of odd order. This contradicts the nonsolvability of $(Q,\cdot)$. Therefore $(Q,\cdot)$ is simple.

Let $(Q,\circ)$ be the associated left Bruck loop. By Theorem 2.2, $(Q,\circ)$ is solvable and so the derived subloop $D=(Q,\circ)'$ is a proper subloop of $(Q,\circ)$. Since D is a characteristic subloop of $(Q,\circ)$, Lemma 2.20 shows that D is normal in $(Q,\cdot)$. Since $(Q,\cdot)$ is simple, $D=1$ and $(Q,\circ)$ is an abelian group.

Recall that powers in $(Q,\cdot)$ and $(Q,\circ)$ agree. Let p be a prime divisor of $|Q|$ and let $Q_p=\{x\in Q\,:\,x^p=1\}$. Then Q_p is a characteristic subloop of $(Q,\circ)$, hence a normal subloop of $(Q,\cdot)$. By Theorem 2.7, Q_p is nontrivial, so $Q_p=Q$ because $(Q,\cdot)$ is simple. Thus $(Q,\cdot)$ has exponent p, $(Q,\circ)$ has exponent p, and $(Q,\circ)$ is an elementary abelian p-group.

By Theorem 2.18, $(Q,\circ,[\cdot,\cdot])$ defined by (2.12) is a Lie ring satisfying (2.10) and (2.11). By Lemma 2.19, $(Q,\circ,[\cdot,\cdot])$ is solvable (of class 2). Since $(Q,\circ)$ is an elementary abelian p-group, we may view $(Q,\circ,[\cdot,\cdot])$ as a finite dimensional Lie algebra over $GF(p)$. Since $(Q,\cdot)$ is simple, Theorem 2.18 also implies that $(Q,\circ,[\cdot,\cdot])$ is either a simple Lie algebra or an abelian Lie algebra (that is, $[Q,Q]=0$). The former case contradicts solvability of $(Q,\circ,[\cdot,\cdot])$, and so $(Q,\circ,[\cdot,\cdot])$ is an abelian Lie algebra. But then $x\cdot y=x\circ y\circ[x,y]=x\circ y$, so $(Q,\cdot)$ is an abelian group, a contradiction with nonsolvability of $(Q,\cdot)$. □

Lecture 3: Enumerations and constructions

In this section we first show how to efficiently search for finite simple automorphic loops, temporarily suspending the notation $\circ$ and $*$ from previous sections. Then we discuss (commutative) automorphic loops of order pq and p^3. Finally, we give two useful constructions of automorphic loops.

3.1. Enumerating all left automorphic loops

Let G be a permutation group on a finite set $Q = \{1, \dots, d\}$, and let $H \leq G$. The first goal of this section is to present a naive algorithm for constructing all loops $(Q, *)$ on Q with identity element 1 so that $\mathrm{Mlt}_\ell(Q, *) \leq G$ and $H \leq \mathrm{Aut}(Q, *)$. Since $\mathrm{Mlt}_\ell(Q, *)$ acts transitively on Q and $\varphi(1) = 1$ holds for every $\varphi \in H$, let us assume from the start that G is transitive on Q and $H \leq G_1$.

We then specialize this algorithm to construct all left automorphic loops $(Q, *)$ on Q satisfying $\mathrm{Mlt}_\ell(Q, *) = G$. In the next subsection we will add the requirement that $(Q, *)$ be simple. The exposition follows [29].

Lemma 3.1. *Let $Q = \{1, \dots, d\}$ be a finite set and let $L = \{\ell_x : x \in Q\}$ be a subset of* $\mathrm{Sym}(Q)$. *Then $(Q, *)$ defined by $x * y = \ell_x(y)$ is a loop with identity element* 1 *if and only if*

(i) *ℓ_1 is the identity mapping on Q, and*

(ii) *$\ell_x(1) = x$ for every $x \in Q$, and*

(iii) *$\ell_x^{-1}\ell_y$ is fixed-point free for every x, $y \in Q$ with $x \neq y$.*

Proof. Condition (i) holds iff $x = \ell_1(x) = 1 * x$ for every $x \in Q$. Condition (ii) hold iff $x = \ell_x(1) = x * 1$ for every $x \in Q$. So (i) and (ii) together are equivalent to $(Q, *)$ having 1 as the identity element. Since $L \subseteq \mathrm{Sym}(Q)$, all the left translations of $(Q, *)$ are bijections. Let $z \in Q$. Then z is not a fixed point of $\ell_x^{-1}\ell_y$ if and only if $x * z \neq y * z$. Therefore condition (iii) holds if and only if all right translations of $(Q, *)$ are one-to-one. We are done by finiteness of Q. □

We therefore have the following naive algorithm for constructing all loops on Q with identity element 1: Construct all subsets $\{\ell_x : x \in Q\}$ of $\mathrm{Sym}(Q)$ and check that conditions (i) – (iii) of Lemma 3.1 hold.

We will show how to speed up the algorithm if we are only interested in left automorphic loops, essentially by adding left translation not one at a time but rather one conjugacy class at a time.

Lemma 3.2. *Let Q be a loop.*

(i) *A bijection $\varphi : Q \to Q$ is an automorphism of Q if and only if $\varphi L_x \varphi^{-1} = L_{\varphi(x)}$ for every $x \in Q$.*

(ii) *If $\varphi \in \mathrm{Aut}(Q)$ fixes x then $L_x\varphi = \varphi L_x$.*

Proof. The following conditions, universally quantified for $y \in Q$, are equivalent: $\varphi L_x \varphi^{-1} = L_{\varphi(x)}$, $\varphi(x\varphi^{-1}(y)) = \varphi(x)y$, $\varphi(xy) = \varphi(x)\varphi(y)$. To prove (ii), consider $\varphi \in \mathrm{Aut}(Q)$ that fixes x, and note that $L_x\varphi(y) = x\varphi(y) = \varphi(x)\varphi(y) = \varphi(xy) = \varphi L_x(y)$ for every $y \in Q$. □

Algorithm 3.3.
Input: A set $Q = \{1, \dots, d\}$, a transitive permutation group G on Q, and $H \le G_1$.

Output: All loops $(Q, *)$ on Q with identity element 1 such that $\mathrm{Mlt}_\ell(Q, *) \le G$ and $H \le \mathrm{Aut}(Q, *)$.

Step 1: Let $\ell_1 = 1_G$, and let $X \subseteq Q \setminus \{1\}$ be a set of orbit representatives for the natural action of H on $Q \setminus \{1\}$. (The condition $\ell_1 = 1_G$ is forced by Lemma 3.1(i).)

Step 2: For all $x \in X$, let

$$\mathcal{L}_x = \{\ell_x \in G : \ell_x(1) = x,\ \ell_x \text{ is fixed-point free, and } \ell_x \in C_G(H_x)\}.$$

If $\mathcal{L}_x = \emptyset$, stop with failure. (This is a set of candidates for ℓ_x. The first two conditions are necessary by Lemma 3.1. The last condition is necessary by Lemma 3.2(ii). Note that if $\mathcal{L}_x$ is nonempty, it suffices to find one $\ell \in \mathcal{L}_x$ and set $\mathcal{L}_x = \ell(C_G(H_x)_1)$.)

Step 3: For all $x \in X$, let

$$\begin{aligned}\mathbb{L}_x = \{\ell_x^H\ &: \ell_x \in \mathcal{L}_x,\ |\ell_x^H| = |H(x)|,\\ &\ell_x^{-1}\ell \text{ is fixed-point free for every } \ell \in \ell_x^H \text{ with } \ell \ne \ell_x\}.\end{aligned}$$

If $\mathbb{L}_x = \emptyset$, stop with failure. (By Lemma 3.2, the desired $L = \{\ell_x : x \in Q\}$ is a union of H-conjugacy classes in G. The set $\mathbb{L}_x$ is a set of candidates for the H-conjugacy class containing ℓ_x. The condition $|\ell_x^H| = |H(x)|$ is forced by Lemma 3.2(i). The second condition is forced by Lemma 3.1(iii).)

Step 4: Construct a graph Γ on $V = \bigcup_{x \in X} \mathbb{L}_x$ by letting $(\ell_x^H, \ell_y^H) \in \mathbb{L}_x \times \mathbb{L}_y$ to be an edge if and only if $(\ell_x^H)^{-1}(\ell_y^H)$ consists of fixed-point free permutations. (Note that it suffices to check that $\ell_x^{-1}\ell_y^H$ consists of fixed-point free permutations. Indeed, if $\psi\ell_x\psi^{-1}(z) = \varphi\ell_y\varphi^{-1}(z)$ for some $z \in Q$, then $\ell_x(\psi^{-1}(z)) = (\psi^{-1}\varphi)\ell_y(\psi^{-1}\varphi)^{-1}(\psi^{-1}(z))$.)

Step 5: Find all subsets C of V such that C is a clique in Γ and $\sum_{v \in C} |v| = |Q| - 1$. If there are no such C, stop with failure. Else return all loops $Q(L) = (Q, *)$, where $L = L(C) = \{\ell_1\} \cup \bigcup_{v \in C} v = \{\ell_x : x \in Q\}$ and $x * y = \ell_x(y)$. (The clique property accounting for $|Q| - 1$ left translations is at this stage necessary and sufficient by Lemmas 3.1 and 3.2.)

Denote by $\mathcal{A}_\ell^{\le}(Q, G)$ all left automorphic loops $(Q, *)$ defined on Q with identity element 1 and satisfying $\mathrm{Mlt}_\ell(Q, *) \le G$, by $\mathcal{A}_\ell^{=}(Q, G)$ all loops $(Q, *) \in \mathcal{A}_\ell^{\le}(Q, G)$ with $\mathrm{Mlt}_\ell(Q, *) = G$, and by $\mathcal{A}^{=}(Q, G)$ all loops $(Q, *) \in \mathcal{A}_\ell^{\le}(Q, G)$ that are automorphic and satisfy $\mathrm{Mlt}(Q, *) = G$. Let also $\mathcal{C}(Q, G, H)$ be the set of all loops $(Q, *)$ obtained by Algorithm 3.3 with input Q, G and H.

Lemma 3.4. *Let G be a transitive permutation group on $Q = \{1, \dots, d\}$. Then $\mathcal{A}^{=}_{\ell}(Q, G) \subseteq \mathcal{C}(Q, G, G_1) \subseteq \mathcal{A}^{\leq}_{\ell}(Q, G)$. Moreover, $\mathcal{A}^{=}(Q, G) \subseteq C(Q, G, G_1)$.*

Proof. First let $(Q, *) \in \mathcal{A}^{=}_{\ell}(Q, G)$. Then $\mathrm{Inn}_{\ell}(Q, *) = \mathrm{Mlt}_{\ell}(Q, *)_1 = G_1$, and therefore $(Q, *) \in \mathcal{C}(Q, G, G_1)$. Now let $(Q, *) \in C(Q, G, G_1)$. Then $\mathrm{Mlt}_{\ell}(Q, *) \leq G$ because every left translation of $(Q, *)$ is in G. Since $\mathrm{Inn}_{\ell}(Q, *) = \mathrm{Mlt}_{\ell}(Q, *)_1 \leq G_1 \leq \mathrm{Aut}(Q, *)$, the loop $(Q, *)$ is left automorphic. Finally, let $(Q, *) \in \mathcal{A}^{=}(Q, G)$. Then $\mathrm{Mlt}_{\ell}(Q, *) \leq G$ and $G_1 = \mathrm{Mlt}(Q, *)_1 = \mathrm{Inn}(Q, *) \leq \mathrm{Aut}(Q, *)$. Thus $(Q, *) \in \mathcal{C}(Q, G, G_1)$. □

Lemma 3.4 can be used to find all left automorphic loops on the set $Q = \{1, \dots, d\}$ with identity element 1. It suffices to apply the lemma to all transitive groups G in Q and discard duplicate loops.

3.2. Searching for finite simple automorphic loops

Recall that a loop Q is said to be *simple* if it has no normal subloops except for Q and 1.

In principle, Algorithm 3.3 returns all finite left automorphic loops, and hence also all finite simple automorphic loops. In practice, the algorithm is too slow to get to even moderately large orders. In this section we will describe improvements to the algorithm so that it can check for simple automorphic loops of order up to several thousands.

The key results are due to Albert and Vesanen. Albert's result is easy to prove, Vesanen's not so much.

Theorem 3.5 ([3, Theorem 8]). *A loop Q is simple if and only if its multiplication group $\mathrm{Mlt}(Q)$ acts primitively on Q.*

Theorem 3.6 ([45]). *Let Q be a finite loop. If $\mathrm{Mlt}(Q)$ is solvable then Q is solvable.*

Recall that a partition of Q is said to be *trivial* if it is of the form $\{Q\}$ or of the form $\{\{x\} : x \in Q\}$. A group $G \leq \mathrm{Sym}(Q)$ *preserves* a partition $\{B_1, \dots, B_n\}$ of Q if for every $\varphi \in G$ and every $1 \leq i \leq n$ there is $1 \leq j \leq n$ such that $\varphi(B_i) = B_j$. A transitive permutation group $G \leq \mathrm{Sym}(Q)$ is *primitive* if it does not preserve any nontrivial partition of Q. The *degree* of G is the cardinality of Q.

It is easy to see that every 2-transitive group $G \leq \mathrm{Sym}(Q)$ is primitive. (Consider a nontrivial partition $\{B_1, \dots, B_n\}$ with $n \geq 1$, B_1 containing distinct elements x, y, and let $z \in B_2$. Let $\varphi \in G$ be such that $\varphi(x) = x$ and $\varphi(y) = z$. Then $\varphi(B_1) \neq B_j$ for every $1 \leq j \leq n$.) Unlike finite 2-transitive groups, finite primitive groups are not classified [13]. `GAP` contains a library of all primite groups of degree < 2500. `MAGMA` [12] contains a library of all primitive groups of degree < 4096.

Lemma 3.7. *If Q is a loop of order bigger than 4 and $H \leq \mathrm{Aut}(Q)$ then H is not 3-transitive on $Q \setminus \{1\}$.*

Proof. Suppose that H is 3-transitive on $Q \setminus \{1\}$. Let x, $y \in Q$ be such that $|\{1, x, y\}| = 3$ and $z = xy \neq 1$. Then $\{x, y, z\}$ is a subset of $Q \setminus \{1\}$ of cardinality 3. Let $\varphi \in H$ be such that $\varphi(x) = x$, $\varphi(y) = y$ and $\varphi(z) \neq z$. (Here we use $|Q| > 4$.) We reach a contradiction with $\varphi(z) = \varphi(xy) = \varphi(x)\varphi(y) = xy = z$. □

Proposition 3.8. *All finite simple nonassociative automorphic loops are found in the set* $\bigcup \mathcal{C}(Q, G, G_1)$, *where the union is taken over sets* Q *of even order and over primitive groups* $G \leq \mathrm{Sym}(Q)$ *that are not solvable and not* 4*-transitive.*

Proof. Let $(Q, *)$ be a finite simple nonassociative automorphic loop of order $d > 1$ with the identity element 1. Let $G = \mathrm{Mlt}(Q, *)$. If $(Q, *)$ is solvable then it is an abelian group, a contradiction. By Theorem 2.21, we can assume that d is even. By Theorem 3.6, G is not solvable. If G is 4-transitive, then $G_1 \leq \mathrm{Aut}(Q, *)$ is 3-transitive on $Q \setminus \{1\}$, a contradiction with Lemma 3.7. It remains to show that $(Q, *) \in \mathcal{C}(Q, G, G_1)$. This follows from Lemma 3.4. □

Let $(Q, *) \in \bigcup \mathcal{C}(Q, G, G_1)$, where the union is as in Proposition 3.8. Suppose that we run the algorithm by incrementally increasing the cardinality of Q, and, for a fixed $d = |Q|$, by incrementally increasing the order of G. When should we catalog $(Q, *)$ as a newly found finite simple nonassociative automorphic loop? We first calculate the order of $M = \mathrm{Mlt}(Q, *) \leq G$. If $|M| < |G|$ then $(Q, *)$ is guaranteed to be automorphic (since $\mathrm{Inn}(Q, *) = M_1 \leq G_1 \leq \mathrm{Aut}(Q, *)$) but either M is not as in Proposition 3.8 or we have already seen $(Q, *)$ in $\mathcal{C}(Q, M, M_1)$, so we do not store $(Q, *)$. If $|M| > |G|$ then $(Q, *)$ is either not automorphic (checking this is expensive), or we will see the same loop later in $\mathcal{C}(Q, M, M_1)$, so we again do not store it. If $|M| = |G|$ then $(Q, *)$ is a finite simple nonassociative automorphic loop and we store it (upon checking for isomorphism against all already stored loops with the same multiplication group).

This search has been carried out in [29] for $d < 2500$ and recently by Cameron and Leemans [7] for $d < 4096$. The result is somewhat surprising:

Proposition 3.9. *There are no finite simple nonassociative automorphic loops of order less than* 4096*.*

We remark that Algorithm 3.3 finds numerous finite simple nonassociative left automorphic loops.

Are there any finite simple nonassociative commutative automorphic loops? The search for finite simple commutative automorphic loops can be reduced to orders 2^k by the following result (whose proof, incidentally, required another associated operation to show that a product of two squares is a square):

Theorem 3.10 ([25])**.** *Let* Q *be a finite commutative automorphic loop. Then* Q *is a direct product* $A \times B$, *where* $A = \{x \in Q : |x| = 2^n$ *for some* $n\}$ *and* $B = \{x \in Q : |x|$ *is odd*$\}$. *Morever,* $|A| = 2^m$ *for some* m *and* $|B|$ *is odd.*

With this decomposition at hand, we easily get:

Theorem 3.11 ([25]). *Let Q be a finite commutative automorphic loop. Then the Cauchy and Lagrange theorems hold for Q.*

It is much harder to deduce solvability in the even case. Grishkov, Kinyon and Nagy used advanced results on Lie algebras to prove:

Theorem 3.12 ([23]). *Every finite commutative automorphic loop is solvable.*

Thus there are no finite simple nonassociative commutative automorphic loops.

3.3. Commutative automorphic loops of order pq

Recall that a power-associative loop Q is a p-loop if every element of Q has order that is a power of p. From Theorem 3.11 we easily deduce that, for an odd prime p, a finite automorphic loop is a p-loop if and only if $|Q|$ is a power of p.

Let us now consider finite commutative automorphic loops. Unlike in abelian groups, the direct factor B from Theorem 3.10 does not necessarily decompose as a direct product of p-loops. In fact, for certain odd primes $p > q$, Drápal constructed a nonassociative commutative automorphic loop Q of order pq, which therefore does not factor as a direct product of an automorphic loop of order p and an automorphic loop of order q. We will discuss his construction at the end of this subsection. First we have a look at commutative automorphic loops of order pq in general.

Lemma 3.13. *Let Q be a power-associative loop. Then $Q/Z(Q)$ is never a nontrivial cyclic group.*

Proof. Suppose that $Q/Z(Q)$ is cyclic of order $m > 1$. Then there is $x \in Q \setminus Z(Q)$ such that $xZ(Q)$ has order m in $Q/Z(Q)$ and $Q = \bigcup_{0 \le i < m} x^i Z(Q)$. Therefore any element of Q can be written as $x^i a$ for some $0 \le i < m$ and $a \in Z(Q)$. With three elements of Q written in this form, we calculate

$$(x^i a \cdot x^j b) \cdot x^k c = (x^i x^j) x^k \cdot abc = x^i (x^j x^k) \cdot abc = x^i a \cdot (x^j b \cdot x^k c),$$

where we have used a, b, $c \in Z(Q)$ and power-associativity for $\langle x \rangle$. Hence Q is a group, and the result follows from the well-known fact that, in groups, $Q/Z(Q)$ is never a nontrivial cyclic group. □

Niederreiter and Robinson proved the following result while studying Bol loops of order pq:

Proposition 3.14 ([40]). *Let Q be a left Bol loop of order pq with odd primes $p > q$. Then Q contains a unique subloop of order p.*

Lemma 3.15. *Let Q be a nonassociative commutative automorphic loop of order pq with odd primes $p > q$. Then $Z(Q) = 1$, Q contains a normal subgroup S of order p, and all elements of $Q \setminus S$ have order q.*

Proof. We have $Z(Q) < Q$ by assumption. If $1 < Z(Q)$ then $Q/Z(Q)$ is isomorphic to $\mathbb{Z}_p$ or to $\mathbb{Z}_q$ by Corollary 2.8, a contradiction with Lemma 3.13. Hence $Z(Q) = 1$.

By Theorem 2.14, Q is solvable. Let $S = Q' < Q$. We have $1 < S$, else Q is an abelian group. Let $|S| = s$ and $\{s,t\} = \{p,q\}$. Then $|Q/S| = t$, and both S and Q/S are cyclic groups of prime order. Let $x \in Q \setminus S$. Then $|\langle xS\rangle| = |Q/S| = t$, so t divides $|x|$. By Theorem 2.7, either $|x| = st = pq$ or $|x| = t$. If $|x| = pq$ then $Q = \langle x\rangle$ is a group, a contradiction. Hence $|x| = t$.

Let $(Q,\circ)$ be the associated left Bruck loop. By Proposition 3.14, $(Q,\circ)$ contains a unique subloop of order p. Since powers in $(Q,\circ)$ and $(Q,\cdot)$ coincide, it follows that Q contains precisely $p-1$ elements of order p. Hence $s = p$. □

We will need the following two results:

Theorem 3.16 ([30]). *Let Q be a loop such that* $\mathrm{Inn}(Q)$ *is a cyclic group. Then Q is an abelian group.*

Theorem 3.17 (Albert). *Let S be a normal subgroup of Q, and let $L_S = \{L_x : x \in S\}$. For a permutation group G on Q, let $G_S = \{\varphi \in G : \varphi|_S = \mathrm{id}_S\}$ and $G_{Q/S} = \{\varphi \in G : \varphi(xS) = xS$ for every $x \in Q\}$. Then* $\mathrm{Mlt}(Q)_S = L_S \cdot \mathrm{Inn}(Q)$, $\mathrm{Mlt}(Q)_{Q/S} = L_S \cdot \mathrm{Inn}(Q)_{Q/S}$ *and* $\mathrm{Inn}(Q/S) \cong (\mathrm{Mlt}(Q)_S)/(\mathrm{Mlt}(Q)_{Q/S})$.

Proposition 3.18. *Let Q be a nonassociative commutative automorphic loop of order pq with odd primes $p > q$. Then there is a normal subgroup $C \cong \mathbb{Z}_p$ of* $\mathrm{Inn}(Q)$ *such that* $\mathrm{Inn}(Q)/C$ *is a cyclic group of order dividing* $p-1$.

Proof. Let S be the unique normal subgroup of order p in Q, whose existence is guaranteed by Lemma 3.15. Consider the mapping $f : \mathrm{Inn}(Q) \to \mathrm{Aut}(S)$, $f(\varphi) = \varphi|_S$. Since $\varphi|_S\psi|_S(x) = \varphi|_S(\psi(x)) = \varphi(\psi(x)) = (\varphi\psi)|_S(x)$ for every $x \in S$, the mapping f is a homomorphism. Its kernel is equal to $C = \{\varphi \in \mathrm{Inn}(Q) : \varphi|_S = \mathrm{id}_S\}$. Now, $\mathrm{Aut}(S) \cong \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ is cyclic, so $\mathrm{Inn}(Q)/C \le \mathrm{Aut}(S)$ is a cyclic group of order dividing $p-1$. If C is trivial, we deduce that $\mathrm{Inn}(Q)$ is cyclic and Theorem 3.16 then implies that Q is an abelian group, a contradiction. Thus C is nontrivial.

Let $S = \langle s\rangle$ and fix $t \in Q\setminus S$. Since $L_s(St) = s(St) = (sS)t = St$, the mapping $\psi = L_s|_{St}$ is a bijection on St. We claim that ψ is a p-cycle. Suppose this is not the case. Since ψ has no fixed points and p is a prime, ψ must contain nontrivial cycles of distinct lengths. Then a suitable power of ψ, say ψ^i, has more than 1 but less than p fixed points. Without loss of generality, let t be a fixed point of ψ^i. Then $\alpha = L_t^{-1}L_s^iL_t \in \mathrm{Mlt}(Q)$ fixes 1. Thus $\alpha \in \mathrm{Inn}(Q) \le \mathrm{Aut}(Q)$, and $\alpha|_S \in \mathrm{Aut}(S)$. Moreover, since $\alpha|_S$ is conjugate to ψ^i, they have the same cycle structure. The fixed points of $\alpha|_S$ then determine a nontrivial proper subgroup of $S \cong \mathbb{Z}_p$, a contradiction.

Since Q/S is of prime order q, it is an abelian group and $\mathrm{Inn}(Q/S) = 1$. Then Theorem 3.17 gives $1 = \mathrm{Inn}(Q/S) \cong (L_S \cdot \mathrm{Inn}(Q))/(L_S \cdot \mathrm{Inn}(Q)_{Q/S})$, so $\mathrm{Inn}(Q) = \mathrm{Inn}(Q)_{Q/S}$. In other words, every $\varphi \in \mathrm{Inn}(Q)$ satisfies $\varphi(xS) = xS$ for every $x \in Q$.

Consider $1 \neq \varphi \in C$. Then φ is determined by the value on t, and $t \neq \varphi(t) \in St$. Because $\psi = L_s|_{St}$ is a p-cycle, there exists some $0 < j < p$ such that $\psi^j(t) = \varphi(t)$. Furthermore, $\varphi(s^k t) = s^k\varphi(t) = L_{s^k}\psi^j(t) = \psi^j L_{s^k}(t) = \psi^j(s^k t)$ by Proposition 1.3, so $\varphi|_{St} = \psi^j$. Because ψ^j is a p-cycle and $\varphi^k|_{St} = \psi^{jk}$ for every k, the elements φ, φ^2, …, $\varphi^p = 1$ are distinct and account for all elements of C. Hence $C \cong \mathbb{Z}_p$. □

Construction 3.19 ([16, Propositions 3.1 and 3.6])**.** *Let p be an odd prime and $t \in \mathbb{Z}_p$. Define a partial map $f_t : \mathbb{Z}_p \to \mathbb{Z}_p$ by $f_t(x) = (x+1)(tx+1)^{-1}$. Suppose that for every $i \geq 1$ the value $f_t^i(0)$ is defined and there is a unique $x \in \mathbb{Z}_p$ such that $f_t^i(x) = 0$. Let $d = |\{f_t^i(0) : i \geq 1\}|$. Then $\mathbb{Z}_p \times \mathbb{Z}_d$ with multiplication*

$$(i,a)(j,b) = (i+j, (a+b)(1+tf_t^i(0)f_t^j(0))^{-1})$$

is a commutative automorphic loop.

Proposition 3.20 ([28])**.** *Construction 3.19 yields a nonassociative commutative automorphic loop of order pq for odd primes $p > q$ if and only if q divides $p^2 - 1$, in which case it yields only one such loop up to isomorphism.*

Thanks to Proposition 3.18, all commutative automorphic loops of order pq could be classified by the *tour de force* of classifying all loops with trivial center and metacyclic inner mapping group, a program of Drápal that is nearing completion (see, for instance, [15]). Another, perhaps easier approach, is to classify all left Bruck loops of order pq, and then use Theorem 2.13. In particular, if there is a unique nonassociative left Bruck loop of order pq and q divides p^2-1, then it must correspond to a unique nonassociative commutative automorphic loop of order pq, constructed by Construction 3.19.

3.4. Commutative automorphic loops of order p^3

Proposition 3.21 ([26])**.** *Let p be an odd prime and Q a commutative automorphic loop. If $|Q| \in \{p, 2p, 4p, p^2, 2p^2, 4p^2\}$ then Q is an abelian group.*

Proof. By Theorem 3.10, it suffices to prove that all commutative automorphic loops Q of odd order p and p^2 are groups. For $|Q| = p$ this is a special case of Corollary 2.8, for instance. When $|Q| = p^2$ then $Z(Q)$ is nontrivial by Theorem 2.14, and the case $|Z(Q)| = p$ is excluded by Lemma 3.13. □

In view of Proposition 3.21, commutative automorphic loops of order p^3 (for any prime p) are of interest. As above, we can easily show that if such a loop is nonassociative of odd order p^3 then $Z(Q) \cong \mathbb{Z}_p$ and $Q/Z(Q) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. There are commutative automorphic loops of order 8 with trivial center [26].

Consider the following construction of [26]. Let $n \geq 2$ be an integer. The *overflow indicator* $(.,.)_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \{0,1\}$ is defined by

$$(x,y)_n = \begin{cases} 1, & \text{if } x+y \geq n, \\ 0, & \text{otherwise.} \end{cases}$$

For a, $b \in \mathbb{Z}_n$, define $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ on $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ by

$$\begin{aligned}&(x_1, x_2, x_3)(y_1, y_2, y_3)\\ &\quad = (x_1 + y_1 + (x_2 + y_2)x_3y_3 + a(x_2, y_2)_n + b(x_3, y_3)_n,\ x_2 + y_2,\ x_3 + y_3).\end{aligned}$$

Then $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ is a commutative automorphic loop of order n^3, $Z(Q) = N_\ell(Q) = \mathbb{Z}_n \times 0 \times 0$, and $N_m(Q) = \mathbb{Z}_n \times \mathbb{Z}_n \times 0$.

It turns out that all nonassociative commutative automorphic loops of odd order p^3 are of the form $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$. This was shown by De Barros, Grishkov and the author, who studied quotients of free 2-generated nilpotent class 2 commutative automorphic loops and also proved:

Theorem 3.22 ([10])**.** *For every prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism, including the three abelian groups $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.*

The structure of the free 2-generated commutative automorphic loop of nilpotency class 2 can be found in [10, Theorem 2.3], which is proved by careful associator calculus. Lemma 3.23 below gives some insight, and once again shows that the middle nucleus is of key importance in automorphic loops.

Recall that the *associator* (x, y, z) is defined by $(xy)z = x(yz) \cdot (x, y, z)$.

Lemma 3.23 ([10, Lemmas 2.1 and 2.2])**.** *Let Q be a commutative loop of nilpotency class 2 (that is, $Q/Z(Q)$ is an abelian group). Then $(x, y, x) = 1$, $(x, y, z) = (z, y, x)^{-1}$ and $(x, y, z)(y, z, x)(z, x, y) = 1$ for every x, y, $z \in Q$. Moreover, Q is automorphic if and only if $(xy, u, v) = (x, u, v)(y, u, v)$ for every x, y, u, $v \in Q$.*

In the automorphic case, we have $(xy, u, v) = (x, u, v)(y, u, v)$, $(x, y, uv) = (x, y, u)(x, y, v)$, and $(x, yu, v) = (x, v, y)(x, v, u)(y, x, v)(u, x, v)$.

The structure of the free 2-generated commutative automorphic loop of nilpotency class 3 is also known, cf. [11, Theorem 5.4].

3.5. Two constructions of automorphic loops

We conclude the lecture notes with two constructions of automorphic loops.

Construction 3.24 ([24])**.** *Let R be a commutative ring, V an R-module and $E = \mathrm{End}_R(V)$ the ring of R-endomorphisms of V. Let $(W, +) \leq (E, +)$ be such that*

(i) $ab = ba$ for every a, $b \in W$, and

(ii) $1 + a$ is invertible for every $a \in W$.

Define multiplication on $W \times V$ by

$$(a, u)(b, v) = (a + b,\ (1 + b)(u) + (1 - a)(v)).$$

Then $(W \times V, \cdot)$ is an automorphic loop.

A special case of this construction was first given in [27] in an effort to shed some light on automorphic loops of order p^3. (Automorphic loops of order p^2 are known to be groups by [8] or by [34, Theorem 6.1].) A slight variation on Construction 3.24 was also given in [37] in characteristic 2.

An important special case of Construction 3.24 can be given as follows: Let $R = k < K = V$, where $k < K$ is a field extension. Let W be a k-subspace of K such that $k1 \cap W = 0$. We can identify $a \in W$ with the k-endomorphism of K given by $b \mapsto ba$ (the right translation by a in $(K, \cdot)$). Then it is easy to see (cf. [24]) that the conditions (i) and (ii) of Construction 3.24 are satisfied, and we obtain an automorphic loop $Q_{k<K}(W) = Q_{R,V}(W)$ on $W \times K$.

Let us come back to automorphic loops of order p^3. In order to obtain them as loops $Q_{k<K}(W)$, we choose $k = \mathbb{F}_p$ to be the field of order p and $K = \mathbb{F}_{p^2}$ a quadratic field extension of k. If p is odd, we can find all suitable k-subspaces W as follows: The field K can be identified with $\{x + y\sqrt{d} : x, y \in k\}$, where $d \in k$ is not a square. Let

$$W_0 = k\sqrt{d} \text{ and } W_a = k(1 + a\sqrt{d}) \text{ for } 0 \neq a \in k.$$

Then every W_a is a 1-dimensional k-subspace of K such that $k1 \cap W_a = 0$. Conversely, if W is a 1-dimensional k-subspace of K such that $k1 \cap W = 0$, there is $a + b\sqrt{d}$ in W with $a, b \in k$, $b \neq 0$. If $a = 0$ then $W = W_0$. Otherwise $a^{-1}(a + b\sqrt{d}) = 1 + a^{-1}b\sqrt{d} \in W$, and $W = W_{a^{-1}b}$. Hence there is a one-to-one correspondence between the elements of k and 1-dimensional k-subspaces W of K satisfying $k1 \cap W = 0$, given by $a \mapsto W_a$.

Proposition 3.25 ([24]). *Let p be a prime and $\mathbb{F}_p = k < K = \mathbb{F}_{p^2}$.*

(*i*) *Suppose that p is odd. If $a, b \in k$, then the automorphic loops $Q_{k<K}(W_a)$, $Q_{k<K}(W_b)$ of order p^3 are isomorphic if and only if $a = \pm b$. In particular, there are $(p+1)/2$ pairwise nonisomorphic automorphic loops of order p^3 of the form $Q_{k<K}(W)$, where we can take $W \in \{W_a : 0 \leq a \leq (p-1)/2\}$.*

(*ii*) *Suppose that $p = 2$. Then there are 2 pairwise nonisomorphic automorphic loops of order p^3 of the form $Q_{k<K}(W)$.*

We do not claim that Proposition 3.25 accounts for all automorphic loops of order p^3.

Finally, we present a construction reminiscent of generalized dihedral groups.

Construction 3.26 ([1]). *Let $(G, +)$ be an abelian group and $m > 1$ an even integer. Let $\alpha \in \mathrm{Aut}(G)$. Define multiplication on $\mathbb{Z}_m \times G$ by*

$$(i, u)(j, v) = (i + j, \alpha^{ij}((-1)^j u + v)).$$

Then the resulting loop $\mathrm{Dih}(m, G, \alpha)$ *is automorphic if and only if $m = 2$ or $\alpha^2 = 1$.*

Aboras [2] obtained many structural properties of the dihedral-like automorphic loops $\mathrm{Dih}(m, G, \alpha)$, which are of interest because they account for many small automorphic loops.

The special case of Construction 3.26 with $m = 2$ was originally introduced in [34], and the following result was obtained there:

Theorem 3.27 ([34, Corollary 9.9]). *Let p be an odd prime, and let Q be a loop of order $2p$. Then Q is automorphic if and only if it is isomorphic to the cyclic group $\mathbb{Z}_{2p}$ or to a dihedral-like loop $\mathrm{Dih}(2, \mathbb{Z}_p, \alpha)$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_p)$. There are precisely p pairwise nonisomorphic automorphic loops of order $2p$.*

Coming back full circle, the automorphic loop Q_6 from the introduction is isomorphic to the loop $\mathrm{Dih}(2, \mathbb{Z}_3, \alpha)$, where α is the unique nontrivial automorphism of $\mathbb{Z}_3$.

4. Open problems

Problem 4.1. *Is there a finite simple nonassociative automorphic loop?*

Problem 4.2. *Is there an automorphic loop of odd order with trivial middle nucleus?*

Problem 4.3. *If Q is a finite automorphic loop and $H \le Q$, does $|H|$ divide $|Q|$?*

Let p be a prime.

Problem 4.4. *Find an elementary proof of the fact that automorphic loops of order p^2 are groups.*

Problem 4.5. *Classify automorphic loops of order p^3.*

Problem 4.6. *Classify commutative automorphic loops of order p^4.*

Problem 4.7. *Classify left Bruck loops of order pq and p^2q, where p, q are distinct odd primes.*

Problem 4.8. *Classify (commutative) automorphic loops of order pq and p^2q, where p, q are distinct odd primes.*

Problem 4.9. *Study free commutative automorphic loops with k free generators and of nilpotency class n. Already the cases $(k, n) = (2, 4)$ and $k \ge 3$ are open.*

Problem 4.10. *Study in detail the mapping $\Phi : (Q, \cdot) \mapsto (Q, \circ)$ that associates a uniquely 2-divisible left Bruck loop $(Q, \circ)$ to a uniquely 2-divisible automorphic loop $(Q, \cdot)$ via $x \circ y = (x^{-1}\backslash y^2x)^{1/2}$. In particular, what is the image of Φ? If $(Q, \circ) \in \mathrm{im}(\Phi)$, is there also a commutative automorphic loop $(Q, \cdot)$ such that $(Q, \circ) = \Phi(Q, \cdot)$?*

Problem 4.11. *Can Proposition* 2.12 *be extended from left Bruck loops of odd order to uniquely* 2*-divisible left Bruck loops, perhaps under different correspondence?*

Problem 4.12. *Let* $(Q,+,[.,.])$ *be an algebra in which the condition* (2.10) *holds, and let* $(Q,\cdot)$ *be the associated linear loop with multiplication* $x\cdot y = x+y-[x,y]$. *Characterize when* $(Q,\cdot)$ *is an automorphic loop* (*beyond the obvious equational characterization*). *Are there interesting classes of algebras for which* $(Q,\cdot)$ *is always automorphic?*

Problem 4.13. *Let* $(Q,+,[.,.])$ *be a Lie ring satisfying* (2.10). *Characterize when the associated linear loop* $(Q,\cdot)$ *is automorphic* (*beyond the obvious equational characterization*).

An alternative theory of solvability in loop theory has been developed in [44], based on concepts from universal algebra (congruence modular varieties). Let us call this solvability *congruence solvability.* Congruence solvability is in general a stronger concept than solvability. To see whether congruence solvability is the right concept for loops, theorems previously proved for (classical) solvability in loops should be revisited. In particular:

Problem 4.14. *Are left Bruck* (*Moufang, commutative automorphic, automorphic*) *loops of odd order congruence solvable?*

Acknowledgment. I thank Michael Kinyon for useful conversations on the Greer correspondence, Přemysl Jedlička for comments on Construction 3.19, Aleš Drápal for the key idea in the proof of Proposition 3.18, and an anonymous referee for a few improvements to the presentation.

References

[1] **M. Aboras**, *Dihedral-like constructions of automorphic loops*, Comment. Math. Univ. Carolin. **55** (2014), 269–284.

[2] **M. Aboras**, *Dihedral-like constructions of automorphic loops*, PhD thesis, University of Denver, May 2015, preprint.

[3] **A.A. Albert**, *Quasigroups I*, Trans. Amer. Math. Soc. **54** (1943), 507–519.

[4] **M. Aschbacher**, *Near subgroups of finite groups*, J. Group Theory **1** (1998), 113–129.

[5] **R.H. Bruck**, *A survey of binary systems*, third printing, corrected, Ergebnisse der Mathematik und ihrer Grenzgebiete **20**, Springer Verlag, 1971.

[6] **R.H. Bruck and L.J. Paige**, *Loops whose inner mappings are automorphisms*, Ann. of Math. (**2**) **63** (1956), 308–323.

[7] **P. Cameron and D. Leemans**, e-mail correspondence, August 2014.

[8] **P. Csörgő**, *All automorphic loops of order p^2 for some prime p are associative*, J. Algebra Appl. **12** (2013), no. **6**, 1350013, 8 pp.

[9] **P. Csörgő**, *Multiplication groups of commutative automorphic p-loops of odd order are p-groups*, J. Algebra **350** (2012), 77–83.

[10] **D.A.S. De Barros, A. Grishkov and P. Vojtěchovský**, *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11** (2012), no. **5**, 1250100, 15 pages.

[11] **D.A.S. De Barros, A. Grishkov and P. Vojtěchovský**, *The free commutative automorphic* 2*-generated loop of nilpotency class* 3, Comment. Math. Univ. Carolin. **53** (2012), 321–336.

[12] **W. Bosma, J. Cannon and C. Playoust**, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[13] **J.D. Dixon and B. Mortimer**, *Permutation groups*, Graduate Texts in Mathematics, Springer, New York, 1996.

[14] **A. Drápal**, *A-loops close to code loops are groups*, Comment. Math. Univ. Carolin. **41** (2000), 245–249.

[15] **A. Drápal**, *Orbits of inner mapping groups*, Monatsh. Math. **134** (2002), 191–206.

[16] **A. Drápal**, *A class of commutative loops with metacyclic inner mapping groups*, Comment. Math. Univ. Carolin. **49** (2008), 357–382.

[17] **A. Figula**, *Affine reductive spaces of small dimension and left A-loops*, Results Math. **49** (2006), no. **1**–**2**, 45–79.

[18] **T. Foguel, M.K. Kinyon and J.D. Phillips**, *On twisted subgroups and Bol loops of odd order*, Rocky Mountain J. Math. **36** (2006), no. **1**, 183–212.

[19] **The GAP Group**, GAP – Groups, Algorithms, and Programming, Version 4.4.10; 2007. `http://www.gap-system.org`

[20] **G. Glauberman**, *On loops of odd order I*, J. Algebra **1** (1964), 374–396.

[21] **G. Glauberman**, *On loops of odd order II*, J. Algebra **2** (1968), 393–414.

[22] **M. Greer**, *A class of loops categorically isomorphic to Bruck loops of odd order*, Commun. Algebra **42** (2014), 3682–3697.

[23] **A. Grishkov, M. Kinyon and G.P. Nagy**, *Solvability of commutative automorphic loops*, Proc. Amer. Math. Soc. **142** (2014), 3029–3037.

[24] **A. Grishkov, M. Rasskazova and P. Vojtěchovský**, *Automorphic loops arising from module endomorphisms*, preprint.

[25] **P. Jedlička, M. Kinyon and P. Vojtěchovský**, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), 365–384.

[26] **P. Jedlička, M. Kinyon and P. Vojtěchovský**, *Constructions of commutative automorphic loops*, Commun. Algebra **38** (2010), 3243–3267.

[27] **P. Jedlička, M. Kinyon and P. Vojtěchovský**, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64–76.

[28] **P. Jedlička and D. Simon**, *On commutative A-loops of order pq*, J. Algebra Appl. **14** (2015), no. **3**, 1550041, 20 pp.

[29] **K.W. Johnson, M.K. Kinyon, G.P. Nagy and P. Vojtěchovský**, *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200–213.

[30] **T. Kepka and M. Niemenmaa**, *On loops with cyclic inner mapping groups*, Arch. Math. (Basel) **60** (1993), no. **3**, 233–236.

[31] **H. Kiechle**, *Theory of K-loops*, Lecture Notes in Math. **1778**, Springer-Verlag, Berlin, 2002.

[32] **M. Kikkawa**, *Geometry of homogeneous Lie loops*, Hiroshima Math. J. **5** (1975), 141–179.

[33] **M.K. Kinyon, K. Kunen and J.D. Phillips**, *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc. **130** (2002), 619–624.

[34] **M.K. Kinyon, K. Kunen, J.D. Phillips and P. Vojtěchovský**, *The structure of automorphic loops*, Trans. Amer. Math. Soc., in press.

[35] **W.W. McCune**, *Prover9 and Mace4*, version 2009-11A. `http://www.cs.unm.edu/~mccune/prover9/`

[36] **R. Moufang**, *Zur Struktur von Alternativkörpern* (German), Math. Ann. **110** (1935), 416–430.

[37] **G.P. Nagy**, *On centerless commutative automorphic loops*, Comment. Math. Univ. Carolin. **55** (2014), 485–491.

[38] **G.P. Nagy and P. Vojtěchovský**, *LOOPS: Computing with quasigroups and loops in GAP*, version 2.0.0, computational package for GAP, `http://www.math.du.edu/loops`

[39] **P.T. Nagy and K. Strambach**, *Loops as invariant sections in groups, and their geometry*, Canad. J. Math **46** (1994), 1027–1056.

[40] **H. Niederreiter and K.H. Robinson**, *Bol loops of order pq*, Math. Proc. Cambridge Philos. Soc. **89** (March 1981), 241–256.

[41] **J.M. Osborn**, *A theorem on A-loops*, Proc. Amer. Math. Soc. **9** (1958), 347–349.

[42] **J.D. Phillips and P. Vojtěchovský**, *A scoop from groups: equational foundations for loops*, Comment. Math. Univ. Carolin. **49** (2008), 279–290.

[43] **K.K. Shchukin**, *Nilpotency of the multiplication group of an A-loop* (Russian), Mat. Issled. **102** (1988), 116–117.

[44] **D. Stanovský and P. Vojtěchovský**, *Commutator theory for loops*, J. Algebra **399** (2014), 290–322.

[45] **A. Vesanen**, *Solvable groups and loops*, J. Algebra **180** (1996), 862–876.

[46] **C.R.B. Wright**, *On the multiplication group of a loop*, Illinois J. Math. **13** (1969), 660–673.

Received May 4, 2015

Department of Mathematics, University of Denver 2280 S Vine St., Denver, Colorado 80208, U.S.A.
E-mail: petr@math.du.edu