The term $x^{1/2}yx^{1/2}$

Petr Vojtěchovský

Department of Mathematics
University of Denver

July 1, 2014 / Algebra and Clones Fest, Prague

1. Introduction: Basic properties of $x^{1/2}yx^{1/2}$
2. Sequential product in C^*-algebras
3. Bruck and Moufang loops of odd order
4. Automorphic loops
5. Commutative automorphic loops

Introduction

Motivation

The term

$$x^{1/2}yx^{1/2}$$

proved useful in several types of algebras.

The operation

$$x \circ y = x^{1/2}yx^{1/2}$$

either plays an important role, or the associated algebra $(A, \circ)$ is easier to investigate than the original algebra $(A, \cdot)$.

The term is interesting only if $(A, \cdot)$ is not commutative and/or not associative.

Taking square roots

We denote by $x^{1/2}$ the unique element in A (or a fixed subset of A) such that

$$(x^{1/2})^2 = x.$$

The square root $x^{1/2}$ is well-defined if the squaring map $a \mapsto a^2$ is a bijection of A, i.e., if A is *uniquely 2-divisible*.

A special case of this is when every element of $(A, \cdot)$ has odd order. Indeed, if $|x| = 2n + 1$, we have $x^{1/2} = x^{n+1}$.

An alternative: $(xy^2x)^{1/2}$

Suppose that the squaring map f is a bijection of A. Let

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

Then $f : (A, \bullet) \to (A, \circ)$ is an isomorphism:

$$\begin{aligned} f(x \bullet y) &= f((xy^2x)^{1/2}) = xy^2x \\ &= (x^2)^{1/2} y^2 (x^2)^{1/2} = x^2 \circ y^2 = f(x) \circ f(y). \end{aligned}$$

The Baer trick

When A is a uniquely 2-divisible group of nilpotence class at most two, the operation

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

coincides with the operation $x \circ y$.

The association of $(A, *)$ with $(A, \cdot)$ is known in group theory as the *Baer trick*.

Figure: The bear trick

Badly nonassociative situations

In badly nonassociative situations (when xy^2x is not well defined), we might have to resort to variations.

For instance, if $\backslash$ denotes the left division, that is,

$$x\backslash y = z \quad \Leftrightarrow \quad y = xz$$

we might use

$$(x^{-1}\backslash(y^2x))^{1/2}.$$

In all such situations, the more complicated term reduces to our friend $(xy^2x)^{1/2}$ in the presence of associativity.

Powers

If $(A, \cdot)$ is *power-associative*, that is, $\langle x \rangle$ is a group, then:

- powers in $(A, \cdot)$ and $(A, \circ)$ coincide:

$$x \circ x^n = x^{1/2} x^n x^{1/2} = x^{n+1}$$

- inverses in $(A, \cdot)$ and $(A, \bullet)$ coincide:

$$x \bullet x^{-1} = (x x^{-2} x)^{1/2} = 1 = x^{-1} \bullet x.$$

Inverses

Note that we have $(x^{1/2})^{-1} = (x^{-1})^{1/2} = x^{-1/2}$.

In all situations covered in this talk $(A, \circ)$ has the *automorphic inverse property*

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

Proof (in reasonable situations):

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

Bol identity

We will also always obtain the *(left) Bol identity*

$$x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z$$

Proof in associative case:

$$x \circ (y \circ (x \circ z)) = x^{1/2}y^{1/2}x^{1/2}zx^{1/2}y^{1/2}x^{1/2},$$
$$(x \circ (y \circ x)) \circ z = (x^{1/2}y^{1/2}xy^{1/2}x^{1/2})^{1/2}z(x^{1/2}y^{1/2}xy^{1/2}x^{1/2})^{1/2}.$$

So it is enough to check that

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

Loops

A *loop* is a groupoid $(Q, \cdot)$ in which all translations

$$L_x : Q \to Q,\ y \mapsto xy, \quad R_x : Q \to Q,\ y \mapsto yx$$

are bijections of Q, and there is an identity element 1 such that

$$1x = x1 = x.$$

The left and right divisions are then well defined as

$$x\backslash y = L_x^{-1}(y), \quad x/y = R_y^{-1}(x)$$

and we have

$$x(x\backslash y) = y,\ (x/y)y = x,\ x\backslash(xy) = y,\ (xy)/y = x.$$

Bruck loops

A loop $(Q, \cdot)$ is a *Bol loop* it if satisfies the Bol identity

$$x(y(xz)) = (x(yx))z.$$

A Bol loop satisfying the automorphic inverse property is known as *Bruck loop* (or *K-loop* or *gyrocommutative gyrogroup*).

In all situations covered here, $(A, \circ)$ is a Bruck loop.

Addition of vectors in special relativity

The addition of vectors in special relativity is given by

$$\mathbf{u} \oplus \mathbf{v} = \frac{1}{1 + \frac{\mathbf{u}\cdot\mathbf{v}}{c^2}} \left(\mathbf{u} + \mathbf{v}_{\parallel} + \sqrt{1 - \frac{|\mathbf{u}|^2}{c^2}} \mathbf{v}_{\perp} \right),$$

where

$$\mathbf{v}_{\parallel} = \frac{\mathbf{u} \cdot \mathbf{v}}{|\mathbf{u}|^2} \mathbf{u}$$

is the projection of $\mathbf{v}$ onto a vector parallel with $\mathbf{u}$, and

$$\mathbf{v}_{\perp} = \mathbf{v} - \mathbf{v}_{\parallel}.$$

Ungar noticed that $\oplus$ is a Bruck loop.

Sequential product

Order of measurements

In quantum physics, two measurements often cannot be performed at the same time, hence must be measured in a sequence $A \circ B$ (A is measured first).

There are experiments in which the order of measurements matters. Since

$$P(A)P(B|A) = P(A)P(A \cap B)/P(A) = P(A \cap B)$$

is symmetric in A, B, classical probability cannot be used.

The interpretation of $A \circ B \circ C$ is by convention $A \circ (B \circ C)$, which in the Gudder-Nagy approach below disagrees with $(A \circ B) \circ C$. Is there a physical meaning of $(A \circ B) \circ C$?

Related algebras

- *Banach space* is a vector space with a norm, complete w.r.t. the norm (limits of Cauchy sequences exist)
- *Hilbert space* is a Banach space with norm $\| x \| = \sqrt{x \cdot x}$,
- *Banach algebra* is an algebra $(A, +, \cdot)$ where $(A, \cdot)$ is associative, $(A, +)$ is a Banach space and $\| xy \| \leq \| x \| \| y \|$,
- *C^*-algebra* is a Banach algebra over $\mathbb{C}$ with $^* : A \to A$ such that $x^{**} = x$, $(x + y)^* = x^* + y^*$, $(xy)^* = y^* x^*$, $(\lambda x)^* = \overline{\lambda} x^*$ and $\| x^* x \| = \| x \| \| x^* \|$.

Example

Let H be a separable (countable dense subset) infinite-dimensional Hilbert space. Then its compact operators form a C^*-algebra.

Quantum effects

In 1955, John von Neumann introduced a model of quantum mechanics based on complex separable Hilbert spaces H. Observables are self-adjoint linear operators. Measurements act on observables. A measurement with only 0 or 1 outcome is called an *effect*.

Stan Gudder and Gabriel Nagy (2001) identify quantum effects $\mathcal{E}(H)$ as operators A on H such that $0 \leq A \leq I$. (Consequently, A is self-adjoint.) The cumulative effect of sequential measurements is modeled by

$$A \circ B = A^{1/2} B A^{1/2},$$

where $A^{1/2}$ is the unique square root of A in $\mathcal{E}(H)$. (It can be obtained as follows: If A has eigenvalues and eigenvectors λ_i, e_i, then $A^{1/2}$ has eigenvalues and eigenvectors $\sqrt{\lambda_i}$, e_i.)

Some results of Gudder and Nagy

The product $A \circ B$ indeed falls back in the interval $[0, I]$:

$$0 \leq \langle A^{1/2} B A^{1/2} x, x \rangle = \langle B A^{1/2} x, A^{1/2} x \rangle$$
$$\leq \langle A^{1/2} x, A^{1/2} x \rangle = \langle Ax, x \rangle \leq \langle x, x \rangle.$$

Theorem (Gudder, Nagy 2001)

If $A \circ B = B \circ A$ then $AB = BA$.
If $A \circ (B \circ C) = (A \circ B) \circ C$ for all $C \in \mathcal{E}(H)$ then $AB = BA$.

S. Gudder and G. Nagy, *Sequential quantum measurements*, Journal of Mathematical Physics **42**, 5212 (2001)

Uniqueness of the operation

(Left) Bruck loops have the *left alternative property*

$$a(ab) = (aa)b.$$

The following result states that under reasonable conditions on sequential products, the operation is uniquely determined:

Theorem (Gudder and Latrémolière 2008)

Suppose that $\odot$ is an operation on $\mathcal{E}(H)$ such that $A \odot I = A = I \odot A$, $(A \odot A) \odot B = A \odot (A \odot B)$ and such that certain properties on the trace and projections hold. Then $A \odot B = A^{1/2} B A^{1/2} = A \circ B$.

Gudder and Latrémolière, *Characterization of the sequential product on quantum effects*, J. Math. Physics **49** (2008).

Molnár's generalization to C^*-algebras

Lajos Molnár greatly generalized the above results in the setting of general C^*-algebras.

- L. Molnár and R. Beneduci, *On the standard K-loop structure of positive invertible elements in a C^*-algebra*, to appear in J. Math. Anal. Appl.
- L. Molnár, *A few conditions for a C^*-algebra to be commutative*, to appear in Abstr. Appl. Anal.

Let X be a unital C^*-algebra, X_+ the cone of positive elements of X, and X_+^{-1} the invertible elements in X_+. As always, define $\circ$ on X_+^{-1} by $A \circ B = A^{1/2}BA^{1/2}$.

Deep theorems of C^*-algebras are required.

Algebraic properties

A loop is *Moufang* it it satisfies the identity

$$a(b(ac)) = ((ab)a)c.$$

Theorem (Molnár 2011-2014)

The following conditions are equivalent:

- $(X, \cdot)$ *is commutative,*
- $(X_+^{-1}, \circ)$ *is commutative,*
- $(X_+^{-1}, \circ)$ *is associative,*
- $(X_+^{-1}, \circ, +)$ *is distributive,*
- $(X_+^{-1}, \circ)$ *is a Moufang loop.*

Uniqueness

A positive linear functional $\tau : X \to \mathbb{C}$ is called a *trace* if

$$\tau(AB) = \tau(BA).$$

It is *faithful* if $\tau(A^*A) = 0$ implies $A = 0$.

Theorem (Molnár 2014)

Let τ be a faithful trace on X. Let $\odot$ be defined on X_+^{-1} so that:

- *X_+^{-1} is a left quasigroup,*
- *$A \odot 1 = A$,*
- *$(A \odot A) \odot B = A \odot (A \odot B)$,*
- *$\tau((A \odot B) \odot C) = \tau(B \odot (A \odot C))$,*
- *$\tau(A \odot B) = \tau(AB)$.*

Then $A \odot B = A \circ B$.

Bruck and Moufang loops of odd order

Overview

In 1960s George Glauberman wrote a series of three papers where he proved important structural results about Bruck loops of odd order and Moufang loops of odd order.

1. G. Glauberman, *On loops of odd order*, J. Algebra **1**, 374–396 (1964)
2. G. Glauberman, *Central elements in core free groups*, J. Algebra **4**, 403–420 (1966)
3. G. Glauberman, *On loops of odd order II*, J. Algebra **8**, 393–414 (1968)

Papers 1 and 3 are a curious mixture of loop theory with advanced group theory. A few results follow rather easily in loop theory alone.

Z^*-theorem

A loop is *solvable* if it has a subnormal series where every factor is an abelian group.

In 1 Glauberman formulated a conjecture in group theory which is true if and only if every Bruck loop of odd order is solvable.

He established the conjecture in 2, and one of its reformulations is now known as *Glauberman's Z^*-theorem*. It is a key result in the classification of finite simple groups.

Z^*-theorem

For a finite group G, let $O(G)$ be the largest normal subgroup of odd order.

Let $Z^*(G)$ be a normal subgroup of G such that

$$Z^*(G)/O(G) = Z(G/O(G)).$$

Theorem (Glauberman's Z^*-theorem)

Let G be a finite group with a Sylow 2-subgroup S. If there is an involution $x \in S$ such that $x^G \cap S = \{x\}$ then $x \in Z^*(G)$.

Bruck loops of odd order

Let G be a group of odd order. Recall that $(G, \circ)$ is a Bruck loop.

Glauberman showed that any Bruck loop Q of odd order can be embedded in a certain group G_Q, and established properties of Q by studying the group G_Q and its automorphisms.

Theorem (Glauberman)

Let Q be a Bruck loop of odd order. Then:

- *Cauchy's Theorem: If a prime p divides $|Q|$ then there is $x \in Q$ such that $|x| = p$.*
- *Lagrange's Theorem: If $A \leq Q$ then $|A|$ divides $|Q|$.*
- *If $|Q| = p^k$, p prime, then Q is centrally nilpotent.*
- *Sylow's Theorem: Q contains Sylow p-subloops, and every p-subloop is contained in a Sylow p-subloop.*
- *Hall's Theorem: Q contains Hall π-subloops, and every π-subloop is contained in a Hall π-subloop.*

Left power alternative property

Here is an example of a result of Glauberman that can be obtained by elementary loop theory:

Lemma

Let Q be a left power alternative loop, that is, $x^i(x^j y) = x^{i+j}y$. If $x \in Q$ and Q is finite then $|x|$ divides $|Q|$.

Proof.

Let $A = \langle x \rangle$. If $Ay \cap Az \neq \emptyset$ then $x^i y = x^j z$,
$y = x^{-i} \cdot x^i y = x^{-i} \cdot x^j z = x^{j-i} z \in Az$, $x^k y = x^{k+j-i} z \in Az$, so
$Ay \subseteq Az$. By symmetry, $Ay = Az$. □

Since left Bol loops are left power alternative (proof by induction), we obtain:

Corollary

Let Q be a finite Bruck loop and $x \in Q$. Then $|x|$ divides $|Q|$.

Feit-Thompson Theorem for Bruck loops

Theorem (Glauberman)

Let x be an involution in a group G. Then $x \in Z^*(G)$ iff for every $g \in G$ the order of $g^{-1}g^x$ is odd.

Lemma (Brauer)

Let S be a Sylow 2-subgroup of G and x an involution in S. The following are equivalent:

- *for every $g \in G$ the order of $g^{-1}g^x$ is odd,*
- $x^G \cap S = \{x\}$.

The Z^*-theorem follows, and combined with previous work of Glauberman:

Theorem (Feit-Thompson Theorem for Bruck loops)

Every Bruck loop of odd order is solvable.

Moufang loops of odd order

Moufang loops are *diassociative*, that is, $\langle x, y \rangle$ is a group.

Glauberman noticed that $(G, \circ)$ is a Bruck loop even if G is just a Moufang loop of odd order. He then managed to translate properties from Bruck loops of odd order to Moufang loops of odd order. The translation is not straightforward.

Theorem (Glauberman)

Let Q be a Moufang loop of odd order. Then:

- *Cauchy's Theorem: If a prime p divides $|Q|$ then there is $x \in Q$ such that $|x| = p$.*
- *Lagrange's Theorem: If $A \leq Q$ then $|A|$ divides $|Q|$.*
- *If $|Q| = p^k$, p prime, then Q is centrally nilpotent.*
- *Sylow's Theorem: Q contains Sylow p-subloops, and every p-subloop is contained in a Sylow p-subloop.*
- *Hall's Theorem: Q contains Hall π-subloops, and every π-subloop is contained in a Hall π-subloop.*
- *Feit-Thompson Theorem: Q is solvable.*

More recent results

Theorem (Glauberman-Wright)

Every Moufang loop of order 2^k is centrally nilpotent.

Sylow theorem does not generalize to Moufang loops of even order easily. There is a simple Moufang loop of order 120 with no elements of order 5. Sylow theory can be saved for good primes (Gagola, Grishkov, Zavarnitsine).

Lagrange's Theorem also holds for Moufang loops:

Theorem (Grishkov-Zavarnitsine, Hall-Gagola)

Let Q be a finite Moufang loop and $A \leq Q$. Then $|A|$ divides $|Q|$.

This requires classification of finite simple Moufang loops (Liebeck) and a careful study of groups with triality associated with Moufang loops.

Recent development

Modern approach to Glauberman's theory is due to Aschbacher (for Moufang loops) and Foguel-Kinyon-Phillips (for Bol loops).

Here is the key concept: A subset S of G is a *twisted subgroup* if $1 \in S$, S is closed under inverses and under the operation xyx.

Theorem (Aschbacher, Kinyon, Phillips)

If S is a uniquely 2-divisible twisted subgroup then $(S, \bullet)$ is a Bruck loop.

Example

- It G is a group and $\tau \in \mathrm{Aut}(G)$ then $K(\tau) = \{g \in G;\ g^\tau = g^{-1}\}$ is a twisted subgroup.
- If Q is a Bol loop then $\{L_x;\ x \in Q\}$ is a twisted subgroup of $\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q \rangle$.

Automorphic loops

Inner mapping groups

For a loop Q define the *multiplication group*

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

and the *inner mapping group*

$$\mathrm{Inn}(Q) = \{\varphi \in \mathrm{Mlt}(Q);\ \varphi(1) = 1\rangle.$$

Bruck showed that

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

where $L_{x,y} = L_{xy}^{-1} L_x L_y$, $R_{x,y} = R_{yx}^{-1} R_x R_y$ and $T_x = L_x^{-1} R_x$.

Automorphic loops

A loop Q is *automorphic* if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$.

Automorphic loops form a variety because $L_{x,y}$, $R_{x,y}$, $T_x \in \mathrm{Aut}(Q)$ can be written as identities (with multiplication and divisions).

Theorem (Johnson, Kinyon, Nagy, V 2011)

A loop Q is automorphic iff T_x, $L_{x,y} \in \mathrm{Aut}(Q)$ for every x, $y \in Q$.

The most recent treatment is:

M. Kinyon, K. Kunen, J.D. Phillips and P.V., *The structure of automorphic loops*, to appear in Transactions of AMS

Basic properties

In

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

the authors wanted to prove that every diassociative automorphic loop is Moufang. This is now a theorem due to Osborn in commutative case and Kinyon, Kunen and Phillips in general.

Theorem (Bruck and Paige, 1956)

Automorphic loops are power associative. The middle nucleus $N_\mu(Q) = \{y \in Q;\ x(yz) = (xy)z \text{ for all } x, z \in Q\}$ *plays a special role.*

Automorphic loops in context

Theorem (Johnson, Kinyon, Nagy, V 2011)

Automorphic loops satisfy the anti-automorphic inverse property $(xy)^{-1} = y^{-1}x^{-1}$.

Note: Bruck loops $\cap$ automorphic loops $=$ commutative Moufang loops.

Proof: Commutative Moufang loops are Bruck loops, because they are both left and right Bol. Bruck proved that every commutative Moufang loop is automorphic. Conversely, a loop that is both Bruck and automorphic has AAIP and AIP, hence is commutative, hence Moufang.

Finite simple automorphic loops?

It is an open problem if there are nonassociative finite simple automorphic loops.

Theorem (Johnson, Kinyon, Nagy, V 2011)

There are no nonassociative finite simple automorphic loops of order less than 2500*.*

The proof uses classification of primitive groups of small degrees. A group acts *primitively* on X if no nontrivial partition of X is preserved by the action.

Theorem (Albert)

A loop Q is simple if and only if $\mathrm{Mlt}(Q)$ *acts primitively on Q.*

We have some information about the socle of $\mathrm{Mlt}(Q)$. (So O'Nan-Scott theorem narrows down the possibilities.)

Constructions

There are by now quite a few constructions of nonassocative automorphic loops.

Theorem (Grishov, Rasskazova, V 2014)

Let R be a commutative ring, V an R-module, $E = \mathrm{End}_R(V)$. Suppose that $(W, +) \leq (E, +)$ satisfies

- $I + W \subseteq E^*$,
- $(W, \cdot)$ *is commutative.*

Then $W \times V$ with multiplication

$$(a, x)(b, y) = (a + b, (I + b)x + (I - a)y)$$

is an automorphic loop.

Construction

Theorem (KKPV and Aboras 2013)

Let G be an abelian group, m an even integer and $\alpha \in \mathrm{Aut}(G)$. If $m > 2$, also assume $\alpha^2 = 1$. Then $\mathbb{Z}_m \times G$ with multiplication

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

is an automorphic loop.

Two ideas: 1) Associated Bruck loops

Let $(Q, \cdot)$ be a uniquely 2-divisible automorphic loop. Mimicking the situation in Moufang loops, define $(Q, \bullet)$ by

$$x \bullet y = (x^{-1} \backslash (y^2 x))^{1/2}.$$

You can also obtain it as follows:

- prove that $P_Q = \{P_x;\ x \in Q\}$ is a twisted subgroup of $\mathrm{Mlt}(Q)$, where $P_x = R_x L_{x^{-1}}^{-1}$,
- then $(P_Q, \bullet)$ is a Bruck loop, project down from $\mathrm{Mlt}(Q)$ onto Q, get $(Q, \bullet)$.

This gives Lagrange's and Cauchy's theorems, but not Sylow's and Hall's theorems for automorphic loops of odd order.

Two ideas: 2) Associated Lie rings

Generalize a construction due to Wright (1967).

A *Lie ring* $(L, +, [\cdot, \cdot])$ is an abelian group $(L, +)$ with a bracket satisfying

- $[x, y] = -[y, x]$,
- $[x + y, z] = [x, z] + [y, z]$,
- $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$.

Associated Lie rings

Theorem

On a Lie ring $(Q, +, [\cdot,\cdot])$ *define* $x \diamond y = x + y - [x, y]$. *Then* $(Q, \diamond)$ *is a uniquely 2-divisible automorphic loop whose associated Bruck loop is an abelian group iff*

- *the translations* $y \mapsto y \pm [y, x]$ *biject,*
- $[[Q, x], [Q, x]] = 1$.

Conversely, if $(Q, \cdot)$ *is a uniquely 2-divisible automorphic loop with associated Bruck loop* $(Q, \circ)$ *that is an abelian group, define* $[x, y] = x \circ y \circ (xy)^{-1}$ *and get a Lie ring satisfying the above two conditions.*
The constructions are inverse to one another.

Corollaries of the second idea

Theorem (Kinyon, Kunen, Phillips, V 2013)

Automorphic loops of odd order are solvable.

Theorem (KKPV 2013)

An automorphic loop of order p^2 is a group. There are automorphic loops of order p^3 that are not centrally nilpotent.

Moving toward the commutative case:

Theorem (Grishkov, Kinyon, Nagy 2013)

There are no finite simple nonassociative commutative automorphic loops.

Commutative automorphic loops

Early results on odd order

1. P. Jedlička, M. Kinyon and P. V., *Constructions of commutative automorphic loops*, Communications in Algebra **38** (2010), no. **9**, 3243–3267
2. _____, *The structure of commutative automorphic loops*, Transactions of AMS **363** (2011), 365–384
3. _____, *Nilpotency in automorphic loops of prime power order*, Journal of Algebra **350** (2012), no. **1**, 64–76

In 2 the twisted subgroup $\{P_x;\ x \in Q\}$ appears for the first time and the Feit-Thompson theorem is obtained, as well as Cauchy's and Lagrange's Theorems.

Even order

We actually obtain Cauchy's and Lagrange's Theorems for *all* finite commutative automorphic loops thanks to the following decomposition result analogous to the first step in the decomposition for finite abelian groups:

Theorem

Let Q be a finite commutative automorphic loop. Then Q is a direct product of a loop of odd order and a loop od order 2^k.

The odd order subloop does not further decompose into p-primary components. Drápal constructed counterexamples of order pq.

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

Nilpotence

Theorem (JKV 2013)

If Q is a commutative automorphic loop of order p^k, p an odd prime, then Q is centrally nilpotent.

Counterexamples for order $n = 2^k$, already at $n = 8$.

Automated deduction

Due to the many interconnected operations, automated deduction (particularly PROVER9 and MACE4 by W. McCune) is heavily used in papers on automorphic loops.

Automated deduction is becoming common in nonassociative algebra:

J.D. Phillips and D. Stanovský, *Automated theorem proving in quasigroup and loop theory*, Artificial Intelligence Communications **23/2–3** (2010), 267–283

Figure: Home appliance with built-in automated deduction

Figure: About to push the wrong button

Automated deduction

A key step in the decomposition result was the following lemma:

Lemma

In a commutative automorphic loop, x^2y^2 is the square of $z = ((xy)\backslash x \cdot (yx)\backslash y)^{-1}$.

First time the result was obtained (in a car while driving to Fort Collins), PROVER9 found a more complicated formula for C:

$$
\begin{aligned}
&((((((x \cdot x)\backslash x) \cdot (y \cdot (x \cdot x)))\backslash(y \cdot (x \cdot x)))\backslash 1) \\
&\cdot (((((((x \cdot x)\backslash x) \cdot (y \cdot (x \cdot x)))\backslash(y \cdot (x \cdot x)))\backslash 1) \\
&\backslash((((x \cdot x)\backslash x) \cdot ((x \cdot x)\backslash x)) \cdot (y \cdot (x \cdot x))))\backslash 1)) \\
&\backslash(((((((x \cdot x)\backslash x) \cdot (y \cdot (x \cdot x)))\backslash(y \cdot (x \cdot x)))\backslash 1) \\
&\cdot (((((((((x \cdot x)\backslash x) \cdot (y \cdot (x \cdot x)))\backslash(y \cdot (x \cdot x)))\backslash 1) \\
&\backslash((((x \cdot x)\backslash x) \cdot ((x \cdot x)\backslash x)) \cdot (y \cdot (x \cdot x))))\backslash 1) \\
&\cdot ((((((x \cdot x)\backslash x) \cdot (y \cdot (x \cdot x)))\backslash(y \cdot (x \cdot x)))\backslash 1) \\
&\cdot \backslash((((x \cdot x)\backslash x) \cdot ((x \cdot x)\backslash x)) \cdot (y \cdot (x \cdot x))))))
\end{aligned}
$$

Inverse functors

All of the above results for *odd order commutative* automorphic loops have been superseded by the the recent work of M. Greer.

M. Greer, *A class of loops categorically isomorphic to uniquely 2-divisible Bruck loops*, to appear in Comm. Algebra

He defined a certain class of power-associative loops, called Γ*-loops*, that properly contain commutative automorphic loops.

Greer's results

Theorem (Greer)

The following are inverse functors between the category B of uniquely 2-divisible Bruck loops, and the category C of uniquely 2-divisible Γ-loops:

$$B \to C, \quad (Q,\cdot) \mapsto (Q,\bullet), \qquad x \bullet y = (x^{-1}\backslash(y^2 x))^{1/2},$$
$$C \to B, \quad (Q,\cdot) \mapsto (Q,*), \qquad x * y = xy[y,x]^{1/2}.$$

You recognize our usual term on the one hand, and the Baer trick on the other hand.

Corollary (Greer)

Cauchy, Lagrange, Sylow, Hall and Feit-Thompson Theorems hold in commutative automorphic loops of odd order.

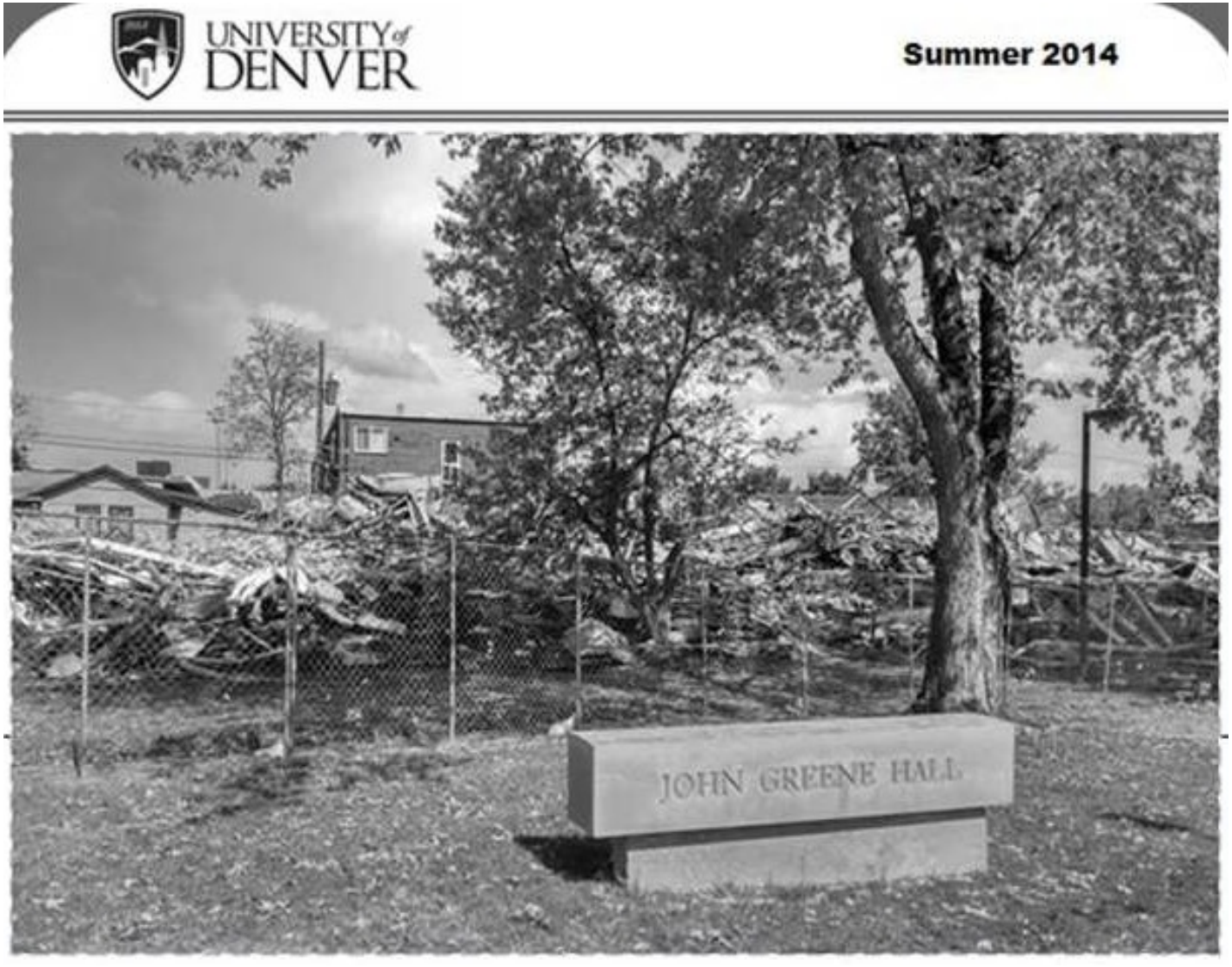

Figure: Thank you and visit us in Denver!