Conjugacy closedness and related matters

Aleš Drápal
Charles University, Prague, Czech Republic

July 2, 2005

This is a user-friendly version of the lecture slides.

—

Let Q be a loop.
$L_a : x \mapsto ax$ is called the *left translation.*
$R_a : x \mapsto xa$ is called the *right translation.*
Left and right translations are permutations and the group they generate is called the *multiplication group*, and will be denoted by $\mathrm{Mlt}\, Q$.
The *left multiplication group* $\mathcal{L} = \mathcal{L}(Q)$, and the *right multiplication group* $\mathcal{R} = \mathcal{R}(Q)$ generate together the full multiplication group $\mathrm{Mlt}\, Q$.
Some, while not all, properties of loops can be expressed by means of translations and multiplication groups.

—

Left translations can be *closed under composition:*

$$L_a L_b \text{ is a left translation for all } a, b \in Q.$$

or *closed under conjugation:*

$$L_a L_b L_a^{-1} \text{ is a left translation for all } a, b \in Q.$$

This corresponds to the *associative law*

$$(xy) \cdot z = x \cdot (yz)$$

and the *left conjugacy law* (LCC law)

$$((xy)/x) \cdot (xz) = x(yz)$$

Conjugacy closed loops are LCC and RCC, i.e. CC = LCC+RCC

—

CC loops have tight structure and seem to be much more accessible than general LCC loops. The connection of CC loops to groups looks to be rather direct, as illustrated by the famous theorem of Basarab [1991]:

If Q is a CC-loop, then Q/N is an abelian group.

Here $N = N(Q)$ stands for the *nucleus*, the set of elements $a \in Q$ which associate with every other two elements of Q.

$a \in N \ \Leftrightarrow \ ax \cdot y = a \cdot xy, \ xa \cdot y = x \cdot ay, \ xy \cdot a = x \cdot ay$

The most accessible CC-loops are those with $Z(Q) \leq A(Q)$. Here $Z(Q) = \{a \in N(Q);\ ax = xa \text{ for all } x \in Q\}$ and $A(Q)$ is the least normal subloop with $Q/A(Q)$ a group.

—

[Drápal 2005] **Every CC-loop $Q(*)$ with $A(Q) \leq Z(Q)$ possesses a normal subloop S such that Q/S is an abelian group of exponent two, and $S(*)$ can be obtained from a group $G = S(\cdot)$ and a symmetric quadri-additive mapping $b : G \times G \to G$ so that**

$$x * y = x \cdot y \cdot b(x, y).$$

What means quadri-additive? For abelian groups the definition can be expressed by:

$b(x, y) : G \times G \to H$ **is quadri-additive $\Leftrightarrow$**
quadratic in x, additive in y.

—

More formally:

Let G and H be Abelian groups. A mapping $b : G \times G \to H$ is said to be *quadri-additive* if

1. $b(\lambda x, \mu y) = \lambda^2 \mu b(x, y)$ for $\lambda, \mu \in \mathbb{Z}$;
2. $b(x, y + z) = b(x, y) + b(x, z)$; and
3. $(x, y) \mapsto b(x + y, z) - b(x, z) - b(y, z)$ is a biadditive mapping $G \times G \to H$ for every $z \in G$.

For nonabelian groups practically the same definition holds. We say that $b : G \times G \to H$ is quadri-additive if b induces a quadri-additive mapping $G/G' \times G/G' \to Z(H)$.

The fact that b can be factorized over the commutant can be expressed as $\mathrm{Rad}(b) \geq G'$, where $\mathrm{Rad}(b) = \{a \in G;\ b(x + a, y) = b(x, y) = b(x, y + a) \text{ for all } x, y \in G\}$. The other condition states $\mathrm{Im}(b) \leq Z(H)$.

If $b : G \times G \to G$ is symmetric quadri-additive, and $\mathrm{Rad}(b) \geq \mathrm{Im}(b)$, then $x * y = xyb(x, y)$ gives a CC loop, and all CC loops with $A(Q) \leq Z(Q)$ can be obtained in this way.

The loop will be denoted by $G[b]$.

—

Recall that nonassociativity in loops is measured by associators $[x, y, z]$, defined by

$$(x \cdot yz)[x, y, z] = xy \cdot z.$$

Note that $A(Q) \leq Z(Q)$ is equivalent to $[x, y, z] \in Z(Q)$, for all $x, y, z \in Q$.

If B and C are abelian groups, then a mapping $f : B \times B \times B \to C$ is said to be *triadditive*, if it is additive in each variable. Call it *symmetric*, if it is invariant under permutation of variables.

For a nonabelian group call $f : G \times G \times G \to G$ *triadditive* if it induces a triadditive mapping $G/G' \times G/G' \times G/G' \to Z(G)$.

—

If $b : G \times G \to G$ is quadri-additive, then
$f : G \times G \times G \to G$, defined by

$$f(x, y, z) = b(xy, z)b(x, z)^{-1}b(y, z)^{-1}$$

is **triadditive**. The corresponding additive formula, which is more natural, has the form

$$f(x, y, z) = b(x + y, z) - b(x, z) - b(y, z).$$

Call b *symmetric quadri-additive* if f is symmetric. (The notion is related to Aschbacher's 3-form.)

Let $Q = Q(\cdot) = G[b]$, where $b : G \times G \to G$ is quadri-additive. Then

$$f(x, y, z) = [x, y, z].$$

When $Z(G)$ is of odd order, one can extract b from f by setting

$$b(x, y) = \frac{1}{2} f(x, x, y).$$

—

Hence all odd order CC-loops Q with $A(Q) \leq Z(Q)$ can be obtained from groups and symmetric trilinear mappings in the form of operations $xyh(x, x, y)$, where h (the half of f) is trilinear symmetric.

Let p be a prime and put $F = \mathbb{Z}_p$. Up to isomorphism there are exactly three nonassociative CC-loops of order p^2 [Kunen, 2000]. Fix $\kappa \in F$ to be a nonsquare. Formulas for these CC-loops can be given as follows [Csörgő & Drápal, 2004]:
$(x, y)(u, v) = (x + y, u + v + x^2 y)$

$xy = x + y + px^2y$
$xy = x + y + \kappa px^2y.$
The trilinear mappings are just the products xyz (or $pxyz$).

These are the simplest nonassociative odd order CC-loops.

—

The simplest generic example of this class is obtained from an elementary abelian group V (which we regard as a vector space over F) and a trilinear symmetric mapping $h : V \times V \times V \to F$. Let $V(h)$ be the loop on $V \times F$ with

$$(x, i) \times (y, j) = (x + y, i + j + h(x, x, y)).$$

In this way one gets *odd code loops* defined by Richardson [1995]. Essentially he takes a linear $[n, k]$ code C of over F and defines on $C \times F$ operation
$(x_1, x_2, \ldots, x_n; i)(y_1, y_2, \ldots, y_n; j) =$
$(x_1 + y_1, \ldots, x_n + y_n; i + j + \sum x_i^2 y_i)$.
It is not difficult to show the equivalence of the two notions [Drápal & Vojtěchovský, 2005].

—

(In fact Richardson's definition is slightly more complicated—when translated to abstract settings he requires an existence of a pointed nontrivial element $u \in V$ with $h(u, u, u) = 0$. For $p = 3$ all elements must have this property.)

—

In $V(h)$ one easily observes that $x = (u, i)$ associates with itself (i.e. $x \cdot xx = xx \cdot x$) if and only $h(u, u, u) = 0$. By a result of [Kunen 2000] if an element associates with itself, then it is mono-associative and power-associative, in every CC-loop. Call h *diagonal*, when $h^{(3)}(u) = h(u, u, u) = 0$ for all $u \in V$. If h is nontrivial diagonal, then $p = 3$ since for $p > 3$ we get

$$\begin{aligned} h(x, y, z) = \frac{1}{6}[&h^{(3)}(x + y + z) \\ &- h^{(3)}(x + y) - h^{(3)}(y + z) - h^{(3)}(x + z) \\ &+ h^{(3)}(x) + h^{(3)}(y) + h^{(3)}(z)]. \end{aligned}$$

This is in accordance with general theory of power-associative CC loops as developed by K&K.

—

Diagonal symmetric trilinear forms over $\mathbb{Z}_3$ call for classification! Nearly all

of symmetric trilinear forms over $\mathbb{Z}_3$ are of this kind because of the following easy observation [Drápal, 2005] — make me aware of an earlier reference!

Let $h : V \times V \times V \to \mathbb{Z}_3$ be a symmetric trilinear form, which is not diagonal. Then $\{u \in V;\ h^{(3)}(u) = 0\}$ is a hyperplane of V.

—

There are several papers on (even) code loops (Griess, Chein & Goodaire, Aschbacher, Hsu). These loops are exactly those that can be expressed as $V(b)$, V a vector space over $\{0, 1\}$, $b : V \times V \to \{0, 1\}$ symmetric quadri-additive (or quadrilinear). Hence a code loop is always a CC-loop (more generally: Moufang CC loops are exactly extra loops, and that is the same as Moufang loops with squares in the nucleus).

Beware! Extraspecial groups are code loops in the even case, but not in the odd case.

—

Can the described construction of CC loops be extended beyond the case $A(Q) \leq Z(Q)$? I have reasons to believe so. One needs to start again from symmetric mappings $f : B \times B \times B \to A$, where B and A are abelian.

Assume that B acts upon A, $a \mapsto a^x$, and that the following equality

$$f(x + y, u, v) = f(x, u, v)^y + f(y, u, v) \\ = f(x, u, v) + f(y, u, v)^x$$

holds for all $x, y, u, v \in B$. One might speak about *skew triadditivity* or *semitri-additivity*. I think that eventually the structure of all CC-loops will be derived from such mappings.

—

To prove it we shall need also *skew quadri-additive* mappings $b : B \times B \to A$ that fulfill

$$b(u, v + w) = b(u, v)^w + b(u, w) \\ = b(u, v) + b(u, w)^v$$

for all u, v and w, and yield f by $f(u, v, w) = b(u + v, w) - b(u, v) - b(u, w)$. One then defines a new operation from a group $G(\cdot)$ by

$$(x, y) \mapsto xyb(x, y)$$

where $R = \mathrm{Rad}(b)$ contains G' and $\mathrm{Im}(b) \leq Z(R)$. The mapping b is thus induced by a mapping $B \times B \to A$, where $B = G/R$ and $A = Z(R)$.

—

To give an example, let $A = \mathbb{Z}_p(+)$ and $B = \mathbb{Z}_p^*(\cdot)$, with B acting on A multiplicatively. We are looking for f with

$$f(xy,u,v) = yf(x,u,v) + f(y,u,v)$$
$$= xf(y,u,v) + f(x,u,v).$$

The simplest way to prescribe f seems to be

$$f(x,y,z) = (x-1)(y-1)(z-1).$$

By setting

$$b(x,y) = (x-1)(y-1)$$

we fulfill the needed relation

$$f(x,y,z) = b(uv,w) - b(u,v) - b(u,w).$$

—

The holomorph of $A = \mathbb{Z}_p(+)$ is the group on $B \times A$,

$$(\alpha,i)\cdot(\beta,j) = (\alpha\beta, \beta i + j).$$

The modification by b yields the operation

$$(\alpha,i)\cdot(\beta,j) = (\alpha\beta, \beta i + j + (\alpha-1)(\beta-1)).$$

We have reconstructed the loop V. D. Belousov found when searching for an example of a G-loop that would not be a WIP-loop.