An example of a non-associative Moufang loop of point classes on a cubic surface

D. Kanevsky

LOOP'S-23

July 1, 2023
Bedlevo, Poland

Introduction

First Scene:
An open place. Thunder and lightning. Enter three witches.
Shakespeare. Macbeth, Act I.

This epigraph was introducing the reader to the Chapter I of the book [Ma86] Yu. I. Manin. Cubic Forms. 2nd Edition, Amsterdam, North-Holland, 1986,
where a problem was stated (Problem 11.11), that was remaining unsolved for more than 50 years.
In this talk, I'll discuss how I recently solved this problem. The presentation is based on my recent paper. [Ka21] Dimitri Kanevsky. An example of a non-associative Moufang loop of point classes on a cubic surface. `https://arxiv.org/pdf/2104.05118.pdf`.

THREE WITCHES: COMMUTATIVE MOUFANG LOOPS

I will start with a brief presentation of basic definitions and problems.

- DEFINITION 1. A symmetric quasigroup is a set E with binary composition law $\circ : E \times E \to E$ satisfying the following condition:

The triple relation $L(x, y, z) : x \circ y = z$ is S_3-invariant.

- EXAMPLE 1. Consider an irreducible cubic curve in a projective plane over a field k, and let E be the set of its non-singular points.

Then the triple relation $L(x, y, z) : (x, y, z)$ are collinear (taking in account multiplicities of intersections) defines on E a structure of symmetric quasigroup.

- (NON-)EXAMPLE 2. Consider now an irreducible cubic hypersurface of dimension ≥ 2 in a projective space over k. One can try define the triple collinearity relation in the same way as above, but then we will have to consider some points in members of such a relation with infinite multiplicity.

Multidimensional case

The following trick will allow us to (partially) extend the statement of Example 1 in multidimension case.

- DEFINITION 2. A symmetric quasigroup E is called Abelian one, if for any element $u \in E$ the composition law $xy := u \circ (x \circ y)$ turns E into an Abelian group.
- PROPOSITION 1. In the setup of (non-) Example 2, the collinearity relation $L(x, y, z)$ induces the structure of abelian quasigroup on any subset of E, consisting of non-singular k-points of an irreducible intersection of the hypersurface with plane.

Generalising this remark, we will introduce our next Definition.

- DEFINITION 3. Let E be a symmetric quasigroup. It is called a CHquasigroup, if any three elements of E generate in it an Abelian subquasigroup.

(Of course, "CH" comes from "Cubic Hypersurface")

- THEOREM 0. Let $(E, \circ)$ be a symmetric quasigroup. For any $x \in E$, denote by $t_x : E \to E$ the map $E \to E$ sending each y to $x \circ y$. Then the following properties are equivalent:
(i) $(E, \circ)$ is an Abelian symmetric quasigroup.
(ii) The group $T^0(E)$ with its natural left action upon E, generated by products of even number of reflections t_x is abelian.
(iii) For any $x, y, z \in E$, we have $(t_x t_y t_z)^2 = 1$ (identical map $E \to E$).
(iv) For any $u \in E$, the composition law $xy := u \circ (x \circ y)$ defines on E the structure of abelian group with identity u.
(v) The same as (iv) for some element u.
In [Ma86], the proof of this Theorem takes pages 12-13. It is organised as a series of implications

$$(i) \Longrightarrow (ii) \Longrightarrow (iii) \Longrightarrow (i)$$

and

$$(ii) \Longrightarrow (iv) \Longrightarrow (v) \Longrightarrow (i).$$

- SKETCH OF PROOF. (i) $(E, \circ)$ is an Abelian symmetric quasigroup.
  (ii) The group $T^0(E)$ with its natural left action upon E, generated by products of even number of reflections t_x is abelian.

  (i) $\Longrightarrow$ (ii) : In this case $x \circ y = ux^{-1}y^{-1}$, and $t_x t_y(z) = \left(x^{-1}y\right) z$ in terms of an abelian group structure on E. Therefore a product of any even number of reflections is a group translation, and they commute.

(ii) The group $T^0(E)$ with its natural left action upon E, generated by products of even number of reflections t_x is abelian.
(iii) For any $x, y, z \in E$, we have $(t_x t_y t_z)^2 = 1$ (identical map $E \to E$).

(ii) $\Longrightarrow$ (iii) : Since $T^0(E)$ is abelian, pairwise products of reflections commute, hence

$$(t_x t_y t_z)^2 = t_x t_y (t_z t_x) t_y t_z = (t_z t_x) t_x t_y t_y t_z = 1$$

(i) $(E, \circ)$ is an Abelian symmetric quasigroup.
(iii) For any $x, y, z \in E$, we have $(t_x t_y t_z)^2 = 1$ (identical map $E \to E$).

(iii) $\Longrightarrow$ (i) : First of all, accepting (iii) one easily sees, that for any $x, y, z \in E$ we have

$$t_x t_y t_z = t_{y \circ (x \circ z)}.$$

Now, again accepting (iii), consider the map $E \to T^0(E) : x \mapsto \bar{x} := t_u t_x$. Obviously, it is an embedding. To check that it is surjective, one checks that

$$t_x t_y = \overline{x \circ (u \circ y)}$$

Finally, commutativity of $T^0(E)$ from a combination of these identities.

By that time, we established that (i), (ii), and (iii) are equivalent. We check next.

(ii) The group $T^0(E)$ with its natural left action upon E, generated by products of even number of reflections t_x is abelian.

(iv) For any $u \in E$, the composition law $xy := u \circ (x \circ y)$ defines on E the structure of abelian group with identity u.

(ii) $\Longrightarrow$ (iv)

$uy = u \circ (u \circ y) = y$,

$xy = u \circ (x \circ y) = u \circ (y \circ x) = yx$,

$x^{-1} = (u \circ u) \circ x$,

$xx^{-1} = u \circ (x \circ (x \circ (u \circ u))) = u$

Associativity follows from $T^0(E)$ being abelian.

Next:
(iv) For any $u \in E$, the composition law $xy := u \circ (x \circ y)$ defines on E the structure of abelian group with identity u.
(v) The same as (iv) for some element u.

(iv) $\Longrightarrow$ (v) : obvious.

Now we check the last:
(i) $(E, \circ)$ is an Abelian symmetric quasigroup.
(v) For some $u \in E$, the composition law $xy := u \circ (x \circ y)$ defines on E the structure of abelian group with identity u.

(v) $\Longrightarrow$ (i) : by assumption, $xy := u \circ (x \circ y)$ is the composition law of an Abelian group.
We have $(xy)(x \circ y) = u \circ [(u \circ (x \circ y)) \circ (x \circ y)] = u \circ u$. It follows that $(xy)(x \circ y) = u \circ u$, which in turn implies commutativity of the quasigroup E via intermediate step $x \circ y = (u \circ u)x^{-1}y^{-1}$.

Commutative Moufang Loop

- DEFINITION 4. (i) A Commutative Moufang Loop (CML for brevity) is a set E with commutative binary composition law $\star : E \times E \to E : (x, y) \mapsto x \star y$, having identity $u \in E$ and left inverse map $E \to E : x \mapsto x^{-1}$, satisfying the following additional identities (called "weak associativity" in "Cubic Forms", Def. 1.4):

$$x \star (x \star y) = (x \star x) \star y, \quad (x \star y) \star (x \star z) = (x \star x) \star (y \star z),$$
$$(x \star y) \star (x \star z) = ((x \star x) \star y) \star z.$$

(ii) A CML E is called non-associative one, if there exists a triple of its elements (x, y, z) such that $x \star (y \star z) \neq (x \star y) \star z$.
(iii) Associative centre $Z(E)$ of a CML $(E, \star)$ is the subset

$$Z(E) := \{x \in E \mid x \star (y \star z) = (x \star y) \star z \text{ for all } y, z \in E\}$$

The associative centre of a CML E is an associative subloop (and therefore an abelian group).

Theorems

- THEOREM 1. Let $(E, \circ, u)$ be a $CH - quasigroup$, endowed with some fixed element $u \in E$. Then E with composition law $(x, y) \mapsto x \star y := u \circ (x \circ y)$ is CML with identity u. For different choices of u, we get isomorphic CML's.
- THEOREM 2. Let $(E, \star, c)$ be a CML, endowed with some fixed element of its associative center $c \in Z(E)$. Then the composition law $x \circ y := cx^{-1} \star y^{-1}$ turns E into CH-quasigroup, denoted E_c.

How these constructions can be extended from basic structures to morphisms between them, is described in the following Theorem. We start with two triples $(E, \star, c)$ and $(F, \star, d)$, as in Theorem 2.

- THEOREM 3. Let $f : E_c \to F_d$ be a morphism of quasigroups, as above, and 1 denotes the identity in E_c. Then $d = f(c)f(1)^2$, and the map $g = f(1)^{-1}f : E \to F$ is a $CML-$ morphism.
Conversely, let $g : E \to F$ be a morphism of two CMLs, and $c \in E; d, b \in F$ are such three elements that $g(c) = db^3$. Then the map $f := b^{-1}g$ is a morphism of CH-quasigroups.

Moufang Loops from cubic hypersurfaces

- COLLINEARITY. Let k be a field, V a cubic hypersurface in P^{r+1}, $r \geq 2$, over k.

A family of three points $P_1, P_2, P_3 \in V(k)$ is called collinear one, if all points lie on a projective line $L \subset \mathrm{P}^{r+1}$ defined over k, and moreover, one of the following conditions holds:
(a) $P_1 + P_2 + P_3$ is the intersection cycle of V and L, with correct multiplicities;
or else
(b) $L \subset V$.

- ADMISSIBLE EQUIVALENCE RELATIONS. An equivalence relation $\mathcal{A}$ on the set $V(k)$ as above is called admissible one, if the following condition is satisfied:

Let P_i and P_i' be two collinear families of points in $V(k)$. If pairs (P_i, P_i') for $i = 1, 2$ belong to the same equivalence classes $\mathrm{mod}\,\mathcal{A}$, the same is true for (P_3, P_3').

One can check directly that if $\mathcal{A}$ is an admissible equivalence relation as above, then the partial composition law $P_3 := P_1 \circ P_2$ induced by collinearity defines on $E := V(k)/\mathcal{A}$ the structure of a commutative symmetric quasigroup, and therefore the composition law $X \star Y := U \circ (X \circ Y)$ induces the structure of CML .
The following result refers to admissible equivalence relations on $V(k)$ in the case, when geometry of V itself is "sufficiently general".
The latter restriction means that not all points in $V(k)$ are singular, and each line $\mathrm{L} \subset \mathrm{P}^{r+1}$ defined over k intersects V at 2 or 3 different geometric points.

- THEOREM 3. Let geometry of V be sufficiently general.Let $\mathcal{A}$ be admissible equivalence relation on the set $V(k)$.
  (i) Let $E := V(k)/\mathcal{A}$. Then E is CH-quasigroup.
  (ii) A CML E with a composition law $U \circ (X \circ Y)$ satisfies the identity $X^6 = 1$
  Spedifically, CML E has a finite number of generators only it is finite. In this case it has $2^a 3^b$ generators.

Non-associative CML from a cubic surface: presentation of an example

- GROUND RING. It will be $\mathrm{Z}_3[t]/\left(t^2+t+1\right)$: extension of the 3-adic completion of Z by a primitive cubic root of 1 . We will put $\theta := t \bmod \left(t^2+t+1\right)$.
- CUBIC SURFACE. Our cubic surface $V \subset P^3$ over $k := \mathrm{Q}_3(\theta)$ will be given by the equation in homogeneous coordinates $T_0^3 + T_1^3 + T_2^3 + \theta T_3^3 = 0$.

We will represent its $k-$ points by equivalence classes of quadruples $p = (t_0 : \cdots : t_3) \in \mathrm{Z}_3[\theta]^4$ defined up to a common multiplication by invertible elements of the ground ring.

- THEOREM 4. Define the equivalence relation $\mathcal{A}_3$ on the set $V(k)$ by

$$(t_0 : \cdots : t_3) \sim \left(t_0'\varepsilon : \cdots : \tau_3'\varepsilon\right),$$

where $\varepsilon \equiv 1 \bmod (1-\theta)^3$. This equivalence relation is admissible one, and the respective CML is non-associative.

Sketch of proof of Theorem 4

- ADMISSIBILITY OF $\mathcal{A}_3$. We must check that if $P_1, P_2, P_3 \in V(k)$ and $P_1', P_2', P_3' \in V(k)$ are two collinear families, such that $P_i \sim P_i'$ mod $\mathcal{A}_3$ for $i = 1, 2$, then also $P_3 \sim P_3'$ mod $\mathcal{A}_3$.

This was checked by direct computations in Sec. 6 of [Ka21]. The verification was subdivided there into three cases:

1. $P_1 = P_2$ and $P_1' = P_2'$.
2. P_1 and P_2 are different modulo $1 - \theta$.
3. $P_1 \equiv P_2$ mod $(1 - \theta)$.

Non-Associativity of composition mod $\mathcal{A}_3$

Consider the following family of three points in $V(k)$, given by their homogeneous coordinates:

$$Q_1 := (1 : 0 : -1 : 0), \quad Q_2 := (0 : 1 : -\theta : 0),$$

and

$$Q_0 := \text{ a lift of } (1 : -1-3\theta : 1-\theta : -1+\theta) \bmod (1-\theta)^3 \text{ to } V(k).$$

Finally, put $U_0 := (1 : -1 : 0 : 0)$. According to Theorem 1 above, we may define $P \star Q := U_0 \circ (P \circ Q)$, if $(U_0, P \circ Q, P \star Q)$ are collinear, and in this triple there are ≤ 2 coinciding points.
Then we have

$$(Q_0 \star Q_1) \star Q_2 \neq Q_0 \star (Q_1 \star Q_2) \bmod (1-\theta)^3.$$

This crucial statement was checked in Subsections 5.4.2 and 5.4.3 of [Ka21] by direct computation of both sides.

Universal equivalence

- Statement: ([Ka24] Moufang loops of point classes on cubic surfaces over local fields. In preparation).
  The admissible equivalence relation $\mathcal{A}_3$ is universal in the sense of [Ma86], pp. 43, 44, 54, 69 .

Roughly speaking, this means that it is the finest equivalence relation in the environment described above.

Conjecture on cubic surfaces over number fields

Let $V \subset \mathbb{P}^3_L$ be a smooth cubic surface defined over a number field L. Let ν_1 and ν_2 be two different places of L such that the following holds.

1. There exists a non-associative Moufang loop of point classes on $V(L_{\nu_1})$ (This can happen only if the residue field of L_{ν_1} has characteristic 3 [Ka24])
2. Let $\mathcal{O}$ be the ring of integers of L_{ν_2}, which has a maximal ideal generated by uniformizing element π. Let V_{ν_2} be the Zariski closure of V in $\mathbb{P}^3_{L_{\nu_2}}$. Let $\tilde{V}_{\nu_2}$ be the special fibre of V_{ν_2} (this is a reduction of V modulo π). Assume that $\tilde{V}_{\nu_2}$ is a cone over smooth cubic curve (over $\mathcal{O} \mod \pi$)

Under these conditions we have

Conjecture

There exists an admissible equivalence $\mathcal{A}$ on $V(L)$ such that CML $V(L)/\mathcal{A}$ is not associative.

This conjecture is motivated by the fact that if a cubic surface over $\mathfrak{p}$-adic field k has a "bad" reduction to a cone over a smooth cubic curve then generically the local evaluation map $V(k) \to \mathbb{Q}/\mathbb{Z}$ takes as many values as possible (Martin Bright, *Evaluating Azumaya Algebras on Cubic Surfaces. Journal Manuscripta Mathematica, vo. 134, no. 3 (2011): 405-421*). This can be used to show that for every point $\boldsymbol{P}_1 \in V(L_{\nu_1})$ we can find a point $\boldsymbol{P}_2 \in V(L_{\nu_2})$ such that the sum of local invariants over a certain adele (that includes $\boldsymbol{P}_1$ and $\boldsymbol{P}_2$) vanishes. Using this observation one can expect (for example, in the spirit of Collioth-Théléne's and Sansuc's conjecture H3 in the section 3.8 (J.L. Colliot-Théléne and J.-J. Sansuc, *La descente sur les variétés rationnelles II, Duke Math. J.54 (1987) 375-492. EUCLID*) that $V(L)$ is dense in $V(L_{\nu_1})$ and therefore a non-associative Moufang loop of point classes on $V(L_{\nu_1})$ induces a non-associative Moufang loop of point classes over $V(L)$.

What is next?

1. Construct non-associative CMLs for cubic surfaces over number fields
2. Classify all CMLs for cubic surfaces over p-adic fields
3. Does the asymptotic behavior of rational points on a cubic surface depend on whether this cubic surface has a non-associative CMLs of point classes?
4. Anything else?