

Discrete and Algebraic n -Valued Groups*

Mikhail Kornev

Steklov Mathematical Institute

*Seminar on Discrete Geometry
and the Geometry of Numbers*

December 3, 2025

*The talk is based on the arXiv preprints [BK25a], [BK25b] and [Kor25].

n -Valued Monoids

An n -valued monoid is a set X equipped with an operation

$$* : X \times X \rightarrow \text{Sym}^n(X)$$

where $\text{Sym}^n(X) = X^{\times n}/S_n$ is the set of unordered n -tuples of elements of X :

- *Associativity.* The n^2 -multisets

$$\begin{aligned} &[x * w \mid w \in y * z], \\ &[w * z \mid w \in x * y] \end{aligned}$$

coincide.

- *Strong unit.* $e * x = x * e = \underbrace{[x, x, \dots, x]}_{n \text{ times}}$ for every $x \in X$.
- *Weak unit.* $e * x \ni x$ and $x * e \ni x$ for every $x \in X$.

n -Valued Groups

An *n -valued group* X is an n -valued monoid equipped with an inverse map

$$\text{inv} : X \rightarrow X.$$

For every $x \in X$, we have two options:

- *Weak inverse map.* $x * \text{inv}(x) \ni e, \quad \text{inv}(x) * x \ni e.$
- *Strong inverse map.* $x * \text{inv } x = \text{inv } x * x = \underbrace{[e, \dots, e]}_{n \text{ times}}.$

The notions of homomorphisms, commutativity, kernels, and related concepts admit natural generalizations from the context of 1-valued groups to that of n -valued groups.

Example. For $n = 1$, we get the usual definition of a group.

n -Diagonal Construction

n -diagonal construction of a single-valued monoid (group) G is the n -valued monoid (group) $\text{diag}(G)$ in which

$$g_1 * g_2 = \underbrace{[g_1 g_2, \dots, g_1 g_2]}_{n \text{ times}}$$

for any $g_1, g_2 \in G$.

Similarly, the n -diagonal is defined for any m -valued monoid (group), yielding an mn -valued monoid (group).

n - and n' -valued monoids X and X' are *isomorphic* if there exists a isomorphism $\varphi : X \rightarrow X'$ preserving the unit, $\varphi(e) = e'$:

$$\frac{m_{x,y}^z}{n} = \frac{m_{\varphi(x),\varphi(y)}^{\varphi(z)}}{n'},$$

where $m_{x,y}^z$ denotes the multiplicity of the element z in the product $x * y$.

Adding a Point

Let's consider the following construction [BR98]. If G is a 1-valued group and x is an indeterminate, let $\widehat{G} = G \cup \{x\}$. Define the multiplication:

$$x * x = e,$$

$$x * g = g * x \text{ for all } g \in G \setminus \{e\},$$

$$g_1 * g_2 = \begin{cases} g_1 g_2, & \text{if } g_1 g_2 \neq e, \\ [e, x] & \text{if } g_1 g_2 = e \text{ and } g_1 \neq e. \end{cases}$$

Coset (Étale) Construction

Given 1-valued group G with multiplication μ_0 , identity e_G , and inverse $\text{inv}_G(u) = u^{-1}$, and given $H < \text{Aut}(G)$, $|H| = n$.

Consider *the set of orbits* $X := G/H$ with projection $\pi : G \rightarrow X$ and an n -valued multiplication

$$\mu : X \times X \rightarrow \text{Sym}^n(X)$$

$$\mu(x, y) = [\pi(\mu_0(u, h(v))) \mid h \in H]$$

where $u \in \pi^{-1}(x)$ and $v \in \pi^{-1}(y)$.

Theorem (Buchstaber, [Buc06])

The multiplication μ defines an n -valued multiplication on X with identity $e_x = \pi(e_G)$ and inverse $\text{inv}_X(x) = \pi(\text{inv}_G(u))$, where $u \in \pi^{-1}(x)$.

Groups $\mathbb{G}_n$

Consider the operation $* : \mathbb{C} \times \mathbb{C} \rightarrow \text{Sym}^n(\mathbb{C})$ that assigns to each pair of complex numbers x and y the multiset

$$x * y = [(\sqrt[n]{x} + \varepsilon^r \sqrt[n]{y})^n \mid r = 1, \dots, n]$$

of n complex numbers, where ε is a primitive n th root of unity, and $\sqrt[n]{\cdot}$ denotes a fixed root branch.

The operation $*$, the identity element 0 , and the inverse $\text{inv}(x) = (-1)^n x$ endow the set of complex numbers $\mathbb{C}$ with the structure of a *commutative n -valued group* $\mathbb{G}_n$.

Groups $\mathbb{G}_n$

$\mathbb{G}_n$'s are examples of coset groups.

Let G be the additive subgroup of $\mathbb{C}$. Let $\varepsilon = e^{2\pi i/n}$. Consider an automorphism

$$\varphi : z \mapsto \varepsilon z$$

We have the projection

$$\begin{aligned}\pi : \mathbb{C} &\rightarrow \mathbb{C} / \langle \varphi \rangle \cong \mathbb{C} \\ z &\mapsto z^n\end{aligned}$$

So, in this case we get

$$x * y = [(\sqrt[n]{x} + \varepsilon^r \sqrt[n]{y})^n \mid r = 1 \dots n]$$

Polynomials $p_n(z; x, y)$

Introduce the following symmetric polynomials:

$$p_n(z; x, y) = \prod_{w \in \text{inv}(x) * \text{inv}(y)} (z - w)$$

$$p_1 = \sigma_1,$$

$$p_2 = \sigma_1^2 - 4\sigma_2,$$

$$p_3 = \sigma_1^3 - 27\sigma_3,$$

$$p_4 = \sigma_1^4 - 2^3 \sigma_1^2 \sigma_2 + 2^4 \sigma_2^2 - 2^7 \sigma_1 \sigma_3,$$

$$p_5 = \sigma_1^5 - 5^4 \sigma_1^2 \sigma_3 - 5^5 \sigma_2 \sigma_3,$$

$$p_6 = \sigma_1^6 - 2^2 \cdot 3 \sigma_1^4 \sigma_2 - 2 \cdot 3^4 \cdot 17 \sigma_1^3 \sigma_3 + 2^4 \cdot 3 \sigma_1^2 \sigma_2^2 \\ - 2^3 \cdot 3^4 \cdot 19 \sigma_1 \sigma_2 \sigma_3 - 2^6 \sigma_2^3 + 3^3 \cdot 19^3 \sigma_3^2$$

where σ_j 's are elementary symmetric polynomials in x, y, z .

Polynomials $p_n(z; x, y)$

For $p_{11}(z; x, y)$ we have:

$$\begin{aligned}\{19, 0, 0\} &\rightarrow 1^1 \\ \{16, 0, 1\} &\rightarrow -1^1 13^1 19^4 198197^1 \\ \{14, 1, 1\} &\rightarrow 2^1 19^6 47^1 199^1 4583^1 \\ \{13, 0, 2\} &\rightarrow 3^1 19^7 942163^1 9355873^1 \\ \{12, 2, 1\} &\rightarrow -1^1 5^1 19^8 2417^1 8753^1 \\ \{11, 1, 2\} &\rightarrow 11^1 19^9 11177^1 12538172357^1 \\ \{10, 3, 1\} &\rightarrow 7^1 19^{10} 3693331^1 \\ \{10, 0, 3\} &\rightarrow -1^1 3^2 19^{10} 3720688976716581473^1 \\ \{9, 2, 2\} &\rightarrow 11^1 19^{11} 2749147^1 165730231^1 \\ \{8, 4, 1\} &\rightarrow -1^1 7^1 19^{12} 23^1 109^1 127^1 \\ \{8, 1, 3\} &\rightarrow 13^1 19^{12} 62503755207269680897^1 \\ \{7, 3, 2\} &\rightarrow 2^2 19^{13} 118901^1 4560604513^1 \\ \{7, 0, 4\} &\rightarrow 2^3 5^1 19^{14} 733^1 39551^1 475379^1 145012169^1 \\ \{6, 5, 1\} &\rightarrow 2^1 3^1 11^1 19^{14} 1307^1\end{aligned}$$

where, e.g., $(10, 3, 1) \rightarrow 7^1 19^{10} 3693331^1$ means that the coefficient of $x^{10} y^3 z$ equals $7 \cdot 19^{10} \cdot 3693331$.

Polynomials $p_n(z; x, y)$

One can define the n -valued group $\mathbb{G}_n$ via the roots of polynomials:

$$p_n(z; x, y) = \prod_{r,s=1}^n \left(\sqrt[n]{z} + \varepsilon^r \sqrt[n]{x} + \varepsilon^s \sqrt[n]{y} \right), \quad \varepsilon = e^{2\pi i/n}$$

$$\tilde{p}_n = p_n(z; (-1)^n x, (-1)^n y)$$

$$x * y = [z \mid z \text{ is a root of } \tilde{p}_n(z; x, y)]$$

These polynomials were first introduced in [BN71] in the context of the theory of n -valued groups.

The problem of describing the structure of the coefficients of the polynomials p_n was posed in [Buc06], where also the explicit form of $p_n(z; x, y)$ was given for $1 \leq n \leq 7$.

Kronecker Sums

Recall the following definition:

Let A and B be arbitrary square matrices over the field $\mathbb{k}$ of orders m and n , respectively.

The *Kronecker sum* $A \boxplus B$ of the matrices $A \in \text{Mat}_{m \times m}(\mathbb{k})$ and $B \in \text{Mat}_{n \times n}(\mathbb{k})$ is the $mn \times mn$ matrix

$$A \boxplus B = A \otimes I_n + I_m \otimes B.$$

This notion has many applications in various fundamental and applied fields of science, including differential equations, quantum computing, machine learning, robotics, and others.

Kronecker Sums

Proposition (Stephanos, [Sté00])

Let $A \in \mathbb{C}^{m \times m}$, $B \in \mathbb{C}^{n \times n}$, and $p(x, y) = \sum_{j,k=0}^{\ell} c_{jk} x^j y^k \in \mathbb{C}[x, y]$.

Consider the matrix

$$p(A, B) = \sum_{j,k=0}^{\ell} c_{jk} A^j \otimes B^k$$

Let $\lambda_1, \dots, \lambda_m$ be the eigenvalues of the matrix A ,
 $\mu_1, \dots, \mu_n$ the eigenvalues of B .

Then the eigenvalues of the matrix $p(A, B)$ are the mn numbers $p(\lambda_r, \mu_s)$, where $r = 1, \dots, m$ and $s = 1, \dots, n$.

Frobenius Companion Matrices

Let $f(t)$ be $t^m + a_{m-1}t^{m-1} + \cdots + a_0 \in \mathbb{C}[t]$.

The *Frobenius companion matrix* $F(a_{m-1}, \dots, a_0)$ of the polynomial $f(t)$ is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & 0 & -a_2 \\ 0 & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & -a_{m-1} \end{pmatrix}.$$

$p_n(z; x, y)$ and Kronecker Sums

Proposition (Buchstaber, Kornev, 2025)

The following statements hold for each natural n :

❶ $p_n(z; x, y)$ is symmetric in the variables x , y , and z .

❷

$$p_n(z^n; x, y) = \chi(\underbrace{F(0, \dots, 0, (-1)^{n+1}x)}_n \boxplus \underbrace{F(0, \dots, 0, (-1)^{n+1}y)}_n; z)$$

❸ The polynomial $p_n(z; x, y)$ is a homogeneous polynomial in the variables x , y , and z of degree n with integer coefficients.

θ -Circulants

For any elements $a_0, \dots, a_{n-1} \in \mathbb{k}$, introduce a θ -circulant matrix:

$$\text{Circ}_{\theta}(a_0, \dots, a_{n-1}) = \begin{pmatrix} a_0 & \theta a_1 & \theta a_2 & \cdots & \theta a_{n-1} \\ a_{n-1} & a_0 & \theta a_1 & \ddots & \vdots \\ a_{n-2} & a_{n-1} & a_0 & \ddots & \theta a_2 \\ \vdots & \ddots & \ddots & \ddots & \theta a_1 \\ a_1 & \cdots & a_{n-2} & a_{n-1} & a_0 \end{pmatrix}$$

Wendt Matrices

This class contains *Wendt matrices* W_n of the form

$$\begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{n-1} \\ \binom{n}{n-1} & 1 & \binom{n}{n-2} & \cdots & \binom{n}{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \cdots & 1 \end{pmatrix}$$

Proposition (Wendt, [Wen94])

Let p be an odd prime and $q = 2kp + 1$ be prime for some $k \geq 1$. Then there exist integers x, y, z , not divisible by q , such that

$$x^p + y^p + z^p \equiv 0 \pmod{q}$$

if and only if q divides $\det W_{2k}$.

Wendt Matrices

Following tradition, we say that the *first case of Fermat's theorem is true for the odd prime exponent p* when:

if x, y, z are (non-zero) integers, not multiples of p , then $x^p + y^p \neq z^p$.

Theorem (Germain, Legendre, 1823, [Rib99])

Let p and q be distinct odd prime numbers, and suppose the following conditions hold:

- If a, b, c are integers and $a^p + b^p + c^p \equiv 0 \pmod{q}$, then $q \mid abc$.
- There is no integer m such that $m^p \equiv p \pmod{q}$.

Then the first case of Fermat's Last Theorem holds for the exponent p .

Wendt Matrices

In 1991, Fee and Granville computed the factors of (the modified) $\det W_n$ for every even $n \leq 200$ (including when 6 divides n). From these calculations, it followed:

If $k \leq 100$, if p and $2kp + 1$ are primes, then the first case of Fermat's last theorem is true for the exponent p .

The result follows from the explicit determination of the factors of W_{2k} (for $2k \leq 200$) and the verification that the conditions of theorem above are satisfied.

$p_n(z; x, y)$ and Wendt Matrices

Theorem (Buchstaber, Kornev, 2025)

The polynomial $p_n(z; x, y)$ defining the n -valued multiplication is the determinant of a y -circulant $n \times n$ matrix:

$$\text{Circ}_y \left(w^n + (-1)^{n+1}x + y, \binom{n}{1}w, \dots, \binom{n}{n-1}w^{n-1} \right)$$

where $w^n = z$.

These matrices generalize the Wendt matrices (the substitution $x = (-1)^n$, $y = z = 1$).

$p_n(z; x, y)$ and Wendt Matrices

$$p_2 = \begin{vmatrix} w^2 - x + y & 2wy \\ 2w & w^2 - x + y \end{vmatrix}$$

$$p_3 = \begin{vmatrix} w^3 + x + y & 3yw & 3yw^2 \\ 3w^2 & w^3 + x + y & 3yw \\ 3w & 3w^2 & w^3 + x + y \end{vmatrix}$$

$$p_4 = \begin{vmatrix} w^4 - x + y & 4yw & 6yw^2 & 4yw^3 \\ 4w^3 & w^4 - x + y & 4yw & 6yw^2 \\ 6w^2 & 4w^3 & w^4 - x + y & 4yw \\ 4w & 6w^2 & 4w^3 & w^4 - x + y \end{vmatrix}$$

The Coefficients of $p_n(z; x, y)$

Theorem (Buchstaber, Kornev, 2025)

For prime $n \geq 5$, the polynomial

$$p_n(z; x, y) - (x + y + z)^n$$

is divisible by n^4xyz .

This result follows from the above observations and from the following:

Theorem (Wolstenholme, [Wol62])

$$\binom{2n-1}{n-1} - 1$$

is divisible by n^3 for primes $n \geq 5$.

Finite Discrete Groups: First Examples

It is easy to see that every n -valued group $\mathbb{G}$ on the singleton set $\{0\}$ is a diagonal construction [Buc06, Lemma 1] of the trivial group.

Each n -valued group $\mathbb{G}$ on the two-element set $\{0, 1\}$ with unit 0 is determined by a pair of non-negative integers (a, b) with $a + b = n$, $a > 0$, since there is only one nontrivial relation:

$$1 * 1 = a \cdot 0 + b \cdot 1.$$

Discrete Groups $\mathbb{X}_n$

For each $n \geq 3$, there exists a commutative n -valued group $\mathbb{X}_n$ on the set $\{0, 1, 2\}$ with unit 0 [Kor25, Example 3]:

$$1 * 1 = [0, \underbrace{2, \dots, 2}_{n-1}]$$

$$1 * 2 = [0, 1, \underbrace{2, \dots, 2}_{n-2}]$$

$$2 * 2 = [0, 1, 1, \underbrace{2, \dots, 2}_{n-3}]$$

Non-coset Groups

For every n -valued group on a set X , in addition to the inverse map $\text{inv} : X \rightarrow X$, we define a multivalued inverse map $\text{Inv} : X \rightarrow \mathbb{P}(X)$ taking values in the set of all finite subsets of X :

$$\text{Inv}(x) = \{y \in X \mid x * y \ni e, \quad y * x \ni e\}.$$

An n -valued group has a uniquely defined inverse map if and only if $\text{inv} = \text{Inv}$. We call such groups *reversible*; otherwise, we call them *non-reversible*.

Every coset group is reversible. So, $\mathbb{X}_n$ is not a coset group.

For $\mathbb{X}_n$, the inverse map inv may be defined in four different ways: $\text{Inv}(1) = \text{Inv}(2) = \{1, 2\}$.

Combinatorial Algebras

An n -valued group $(X, *, \text{inv})$ is called *★-involutive* if the inverse map $x \mapsto \text{inv}(x)$ is an involution satisfying the following conditions:

- 1 For any $x \in X$, one has $x * y \ni e$ if and only if $y = \text{inv}(x)$.
- 2 $m(x) = m(\text{inv}(x))$, where $m(x) = m_{x, \text{inv}(x)}^e$ is the multiplicity of e in the product $x * \text{inv}(x)$.
- 3 $\text{inv}(x * y) = \text{inv}(y) * \text{inv}(x)$ for all $x, y \in X$.

The category of combinatorial algebras and the category of multivalued involutive groups are equivalent [BVEP96].

The Classification of n -Valued Monoids

The complete classification of all $\star$ -involutive n -valued groups of order 3 was achieved in [Pon24, GPV25], based on the classification of all single-valued finite groups of rank 3.

A full classification of n -valued monoids and groups of order 3 has been recently obtained by Kornev in [arXiv:2508.04454](https://arxiv.org/abs/2508.04454) [Kor25].

As a corollary, *there are non- $\star$ -involutive non-coset n -valued groups*.

Classification of n -Valued Monoids of Order 3

Proposition (Kornev, 2025)

Let $\mathfrak{X} = (e, x_1, x_2)^\top$ and

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}^{\circledast 2} = \begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ d_0 & d_1 & d_2 \\ c_0 & c_1 & c_2 \end{pmatrix} \mathfrak{X} = B \mathfrak{X}.$$

Then every n -valued monoid on the set X is represented by one of the following matrices $B = B_j$, provided that all fractional expressions yield non-negative integers:

$$B_1 = \begin{pmatrix} a_0 & n - a_0 & 0 \\ 0 & 0 & n \\ 0 & 0 & n \\ c_0 & \frac{c_0 n}{a_0} & n - c_0 - \frac{c_0 n}{a_0} \end{pmatrix},$$

$$B_2 = \begin{pmatrix} a_0 & a_1 & n - a_0 - a_1 \\ b_0 & b_1 & n - b_0 - b_1 \\ b_0 & b_1 & n - b_0 - b_1 \\ \frac{b_0(n - b_0 - b_1) + a_0 b_1 - a_1 b_0}{n - a_0 - a_1} & \frac{(b_0 + b_1)(n - b_1)}{n - a_0 - a_1} & \frac{(n - b_0 - b_1)^2 + n(b_1 - a_0 - a_1) + a_1 b_0 - a_0 b_1}{n - a_0 - a_1} \end{pmatrix}$$

$$B_3 = \begin{pmatrix} 0 & n & 0 \\ 0 & n & 0 \\ 0 & n & 0 \\ c_0 & c_1 & n - c_0 - c_1 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 0 & n & 0 \\ 0 & 0 & n \\ 0 & 0 & n \\ 0 & c_1 & n - c_1 \end{pmatrix},$$

$$B_5 = \begin{pmatrix} 0 & n & 0 \\ 0 & n & 0 \\ 0 & 0 & n \\ 0 & 0 & n \end{pmatrix}, \quad B_6 = \begin{pmatrix} 0 & n & 0 \\ 0 & 0 & n \\ 0 & n & 0 \\ 0 & 0 & n \end{pmatrix}.$$

Corollaries from the Classification

Corollary (Kornev, 2025)

Every commutative n -valued monoid of order 3 belongs to one of the first four series.

Every noncommutative monoid is a diagonal of one of the two noncommutative single-valued monoids.

In particular, all n -valued groups of order 3 are commutative, and there exist only two noncommutative multivalued monoids up to isomorphism.

Corollary (Kornev, 2025)

Every ★-involutive n -valued group has as its matrix B above one of the following:

$$\tilde{B}_1 = \begin{pmatrix} m(x_1) & a(x_1) & n - m(x_1) - a(x_1) \\ 0 & a(x_1, x_2) & n - a(x_1, x_2) \\ 0 & a(x_1, x_2) & n - a(x_1, x_2) \\ m(x_2) & a(x_2) & n - m(x_2) - a(x_2) \end{pmatrix},$$

$$\tilde{B}_2 = \begin{pmatrix} 0 & a(x_1) & n - a(x_1) \\ n - 2a(x_1) & a(x_1) & a(x_1) \\ n - 2a(x_1) & a(x_1) & a(x_1) \\ 0 & n - a(x_1) & a(x_1) \end{pmatrix},$$

$$a(x_1, x_2) = r(n - m(x_1) - a(x_1)), a(x_2) = r(n - a(x_1, x_2)), r = \frac{m(x_2)}{m(x_1)},$$

and $m(x_1)$, $m(x_2)$, $a(x_1)$ are free parameters.

As shown in [GPV25, Theorem 1.1], an n -valued group from the series $\tilde{B}_2$ with $n = 2k + 1$ is a coset group if and only if

$$\tilde{B}_2 = \begin{pmatrix} 0 & k & k+1 \\ 1 & k & k \\ 1 & k & k \\ 0 & k+1 & k \end{pmatrix},$$

and $4k + 3$ is a power of a prime number.

The classification of coset groups from the series $\tilde{B}_1$ is related to the classification of finite single-valued permutation groups of rank 3 and the theory of strongly regular graphs [GPV25].

Involutive Groups

In the paper [BVG22], in connection with Conway's topograph, the notion of an involutive 2-valued group was introduced.

Definition

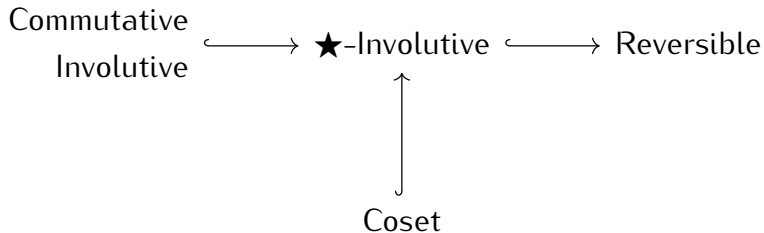
A reversible n -valued group on a set X is called *involutive* if $\text{inv}(x) = x$ for every $x \in X$.

Every commutative involutive group is $\star$ -involutive.

The article [BVG22] gives a complete classification of involutive 2-valued groups.

In the work [Gai24], it is shown that every involutive 2-valued group is commutative.

The Diagram of Embeddings



Corollary (Kornev, 2025)

Groups from the series B_1 are involutive. A group from the series B_2 is involutive if and only if $b_0 = 0$.

Algebraic n -Valued Monoids and Groups

An *algebraic n -valued monoid* is an algebraic variety X equipped with an associative n -valued multiplication given by a *rational morphism* $X \times X \rightarrow \text{Sym}^n(X)$ with a neutral element $e \in X$ such that

$$x * e = e * x = [x, x, \dots, x] \quad \text{for every } x \in X.$$

An *algebraic n -valued group* is an algebraic n -valued monoid on X together with a *regular morphism* $\text{inv} : X \rightarrow X$ such that for any $x \in X$ the following two conditions hold:

$$e \in x * \text{inv}(x), \quad e \in \text{inv}(x) * x.$$

Hadamard monoid on $\mathbb{CP}^1$

Consider $\mathbb{CP}^1 = \mathbb{C} \cup \{\infty\}$.

There is a structure of a 1-valued commutative algebraic monoid $M_{\text{mult}}(\mathbb{CP}^1)$ with identity element $1 = [1 : 1]$ and multiplication

$$(z_1 : z_0) \cdot (w_1 : w_0) = (z_1 w_1 : z_0 w_0),$$

defined on $(\text{Sym}^2 \mathbb{CP}^1) \setminus \{[0, \infty]\}$.

The element $\infty = (1 : 0)$ is absorbing in this monoid, i.e. $z * \infty = \infty$ for each $z \in \mathbb{CP}^1 \setminus \{0\}$.

The elements of $\mathbb{CP}^1 \setminus \{0, \infty\}$, and only they, have inverse $\text{inv}(z_1 : z_0) = (z_0 : z_1)$.

Monoid $M_{\text{cusp}}(\mathbb{CP}^1)$

On $\mathbb{CP}^1 = \mathbb{C} \cup \{\infty\}$ there is also a structure $M_{\text{cusp}}(\mathbb{CP}^1)$ of a 1-valued commutative algebraic monoid with neutral element 0 and addition

$$(z_1 : z_0) \cdot (w_1 : w_0) = (z_1 w_0 + z_0 w_1 : z_0 w_0),$$

defined on $(\text{Sym}^2 \mathbb{CP}^1) \setminus \{[\infty, \infty]\}$.

The elements of $\mathbb{CP}^1 \setminus \{\infty\}$, and only they, have inverse $\text{inv}(z_1 : z_0) = (-z_1 : z_0)$.

Theorem (Buchstaber, Kornev, 2025)

The structure of the group $\mathbb{G}_n(\mathbb{C})$ extends (only) to the structure of an algebraic n -valued coset monoid $\mathbb{M}_n(\mathbb{C}P^1)$ on $\mathbb{C}P^1$. Here the point ∞ is absorbing, i.e. $\infty * x = x * \infty = [\infty, \infty, \dots, \infty]$ for any $x \in \mathbb{C}P^1 \setminus \{\infty\}$, and the value $\infty * \infty$ is undefined.

$$* : \mathbb{C}P^1 \times \mathbb{C}P^1 \longrightarrow \mathbb{C}P^n$$

$$(x_1 : x_0) * (y_1 : y_0) = (b_n : b_1 : \dots : b_0),$$

where $b_j = b_j(x, y)$ is the coefficient of $z_1^{n-j} z_0^j$ in the homogeneous polynomial

$$(x_0 y_0 z_0)^n p_n \left(\frac{z_1}{z_0}; (-1)^n \frac{x_1}{x_0}, (-1)^n \frac{y_1}{y_0} \right)$$

whenever $(x_1 : x_0)$ and $(y_1 : y_0)$ are not both equal to $(1 : 0) =: \infty$.

The Chebyshev Coset Monoid

On $M_{\text{mult}}(\mathbb{CP}^1)$ consider the involution $\tau : z \mapsto 1/z$ for each $z \in \mathbb{CP}^1$.

Points of the orbit space of the involution τ are represented by fibers of the branched double covering

$$\begin{aligned}\pi : \mathbb{CP}^1 &\rightarrow \mathbb{CP}^1 \\ z &\mapsto \frac{1}{2}(z + 1/z)\end{aligned}$$

with branch points ± 1 .

The corresponding coset monoid $\mathbb{M}_{\text{mult}}(\mathbb{CP}^1) := M_{\text{mult}}(\mathbb{CP}^1)_{\langle \tau \rangle}$ has identity 1 and multiplication

$$x * y = \left[xy \pm \sqrt{(x^2 - 1)(y^2 - 1)} \right],$$

defined on $(\text{Sym}^2 \mathbb{CP}^1) \setminus [\infty, \infty]$.

The Chebyshev Coset Monoid

This structure of a 2-valued algebraic monoid does not extend to a structure of a 2-valued algebraic group.

The addition law is given by the roots in z of the polynomial

$$P_{\text{mult}}(z; x, y) = z^2 - 2xy z + x^2 + y^2 - 1.$$

With the multiplication in homogeneous coordinates:

$$\mathbb{C}P^1 \times \mathbb{C}P^1 \rightarrow \text{Sym}^2(\mathbb{C}P^1) \cong \mathbb{C}P^2$$

$$(x_1 : x_0) * (y_1 : y_0) = (x_1^2 y_0^2 + y_1^2 x_0^2 - x_0^2 y_0^2 : -2x_1 y_1 x_0 y_0 : x_0^2 y_0^2).$$

The Chebyshev Coset Monoid

For $x = \cos \alpha$, $y = \cos \beta$, the addition becomes the cosine addition formulas. Let

$$T_j = T_j(\cos \alpha) = \cos j\alpha$$

be the classical Chebyshev polynomials of the first kind ($j \geq 0$). Then

$$T_j * T_k = [T_{j+k}, T_{|j-k|}].$$

Consider the 2-valued submonoid $\mathbb{T} = \mathbb{T}(\mathbb{C})$ of $\mathbb{M}_{\text{mult}}(\mathbb{C}P^1)$ generated by taking integral nonnegative powers of the element $\cos \alpha$.

Regular and n -Algebraic n -Valued Monoids

We say that an algebraic n -valued monoid (or group) on X is *regular* if the n -valued multiplication $X \times X \rightarrow \text{Sym}^n(X)$ is defined on all of $X \times X$.

A *symmetric n -algebraic n -valued monoid (group)* on $\mathbb{C}$ is an algebraic n -valued monoid (group) $\mathbb{G}_{\mathbb{C}}(f(z; x, y))$ whose (partially defined) multiplication

$$x * y = [z \mid f(z; x, y) = 0]$$

is given by a symmetric polynomial $f(z; x, y)$ in which each variable appears with degree at most n .

Buchstaber Polynomials

Consider a 3-parametrized family of polynomials:

$$B_a(z; x, y) = (x + y + z - a_2xyz)^2 - 4(1 + a_3xyz)(xy + yz + xz + a_1xyz)$$

In elementary symmetric functions:

$$B_a(z; x, y) = (e_1^2 - 4e_2) - 4a_1e_3 - 2a_2e_1e_3 - 4a_3e_2e_3 + (a_2^2 - 4a_1a_3)e_3^2.$$

The polynomials $B_a(z; x, y)$ endow $\mathbb{C}$ with the structure of the universal regular algebraic 2-valued group $\mathbb{G}_{\mathbb{C}}(B_a)$ for any $\mathbf{a} \in \mathbb{C}^3$, with addition

$$x * y = [z \mid B_a(z; x, y) = 0],$$

neutral element 0, and inversion map $\text{inv}(x) = x$ [BV19, Theorem 6.3], [BK25b, Theorem 1].

Let's Draw an Elliptic Curve:

Weierstrass Form of a Cubic

Let $\delta_a = \Delta_t(t^3 + a_1 t^2 + a_2 t + a_3)$ be the discriminant. Then

$$\delta_a = -4a_3a_1^3 + a_2^2a_1^2 + 18a_2a_3a_1 - 4a_2^3 - 27a_3^2.$$

Let $\mathcal{E}$ be an irreducible cubic over the field $\mathbb{C}$. As is well known (see, e.g., [FW69, Exercise 5–24]), $\mathcal{E}$ is isomorphic to a cubic given in $\mathbb{C}P^2$ with coordinates $(x : y : z)$, in the chart $\{z = 1\}$, by

$$\mathcal{E} = \{y^2 = x^3 + a_1x^2 + a_2x + a_3\}.$$

As an abelian variety over $\mathbb{C}$, a cubic admits only automorphisms of orders 2, 3, 4, and 6 [Har77, Corollary 4.7].

Let complex parameters α, g_2, g_3 be such that

$$y^2 = (x + \alpha)^3 - \frac{g_2}{4}(x + \alpha) - \frac{g_3}{4}, \quad \begin{cases} a_1 = 3\alpha, \\ a_2 = 3\alpha^2 - \frac{g_2}{4}, \\ a_3 = \alpha^3 - \frac{g_2\alpha}{4} - \frac{g_3}{4}. \end{cases}$$

Recall that the group law

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$$

on $\mathcal{E}$ is given (for distinct points of $\mathcal{E}$) by

$$\begin{cases} x_3 = -x_1 - x_2 - 3\alpha + \left(\frac{y_1 - y_2}{x_1 - x_2} \right)^2, \\ y_3 = (x_1 - x_3) \cdot \frac{y_1 - y_2}{x_1 - x_2} - y_1. \end{cases} \quad (1)$$

In the coincident case, (1) is understood via the limit as $x_2 \rightarrow x_1$.

2-Valued Structures on $\mathbb{CP}^1$

There is a branched double covering

$$\begin{aligned}\pi : \mathcal{E} &\rightarrow \mathbb{CP}^1, \\ (x, y) &\mapsto x, \\ \infty &\mapsto \infty.\end{aligned}$$

with branch points at $\{x^3 + a_1x^2 + a_2x + a_3 = 0\}$ and at ∞ . The fibers of π are in bijection with the points of the orbit space $\mathcal{E}/\langle\sigma\rangle$ for the involution

$$\begin{aligned}\sigma : (x, y) &\mapsto (x, -y), \\ \infty &\mapsto \infty\end{aligned}$$

Applying the coset construction, we obtain a structure $\mathcal{E}_{\langle\sigma\rangle}$ of a coset algebraic 2-valued group on $\mathbb{CP}^1$ with neutral element ∞ :

$$x_1 * x_2 = \left[-x_1 - x_2 - 3\alpha + \left(\frac{y_1 \pm y_2}{x_1 - x_2} \right)^2 \right].$$

2-Valued Structures on $\mathbb{CP}^1$

Proposition

The values of $x_1 * x_2$ are the roots of a quadratic polynomial $D(z; x_1, x_2)$ in z :

$$D(z; x_1, x_2) = \Theta_0(x_1, x_2) z^2 + \Theta_1(x_1, x_2) z + \Theta_2(x_1, x_2),$$

$$\left\{ \begin{array}{l} \Theta_0 = 16(x_1 - x_2)^2, \\ \Theta_1 = 8(2g_3 + g_2(x_1 + x_2 + 2\alpha) - \\ \quad - 4(x_1 x_2(x_1 + x_2) + 6x_1 x_2 \alpha + 3(x_1 + x_2)\alpha^2 + 2\alpha^3)), \\ \Theta_2 = (g_2 + 4x_1 x_2)^2 + 16g_2(x_1 + x_2)\alpha + 24(g_2 - 4x_1 x_2)\alpha^2 \\ \quad - 64(x_1 + x_2)\alpha^3 - 48\alpha^4 + 16g_3(x_1 + x_2 + 3\alpha). \end{array} \right.$$

Generalized Kontsevich Polynomial

In [BGR24], $D(z; x_1, x_2)$ was called the *generalized Kontsevich polynomial*. The first appearance of these polynomials, is due to the explicit computations in Geometric Langlands Correspondence.

As noted in [BGR24], one has

$$D_a(z; x, y) = (xyz)^2 B_a \left(-\frac{1}{z}; -\frac{1}{x}, -\frac{1}{y} \right),$$

where $D_a(z; x, y)$ is the generalized Kontsevich polynomial.

2-Valued Structures on $\mathbb{CP}^1$

Theorem (Buchstaber, Gaiur, Rubtsov) [BGR24]

(I) If $\delta_a \neq 0$, the algebraic 2-valued group $\mathbb{G}_{\mathbb{CP}^1}(D_a) \cong \mathbb{G}_{\mathbb{CP}^1}(B_a)$ with identity ∞ is the regular coset group $\mathcal{E}_{\langle\sigma\rangle}$ for the group of points of the elliptic curve $\mathcal{E}$ with respect to the involution $\sigma : (x, y) \mapsto (x, -y)$. The group $\mathbb{G}_{\mathbb{CP}^1}(B_a)$ on $\mathbb{CP}^1$ has zero $(0 : 1)$ and addition

$$\mu_a : \mathbb{CP}^1 \times \mathbb{CP}^1 \rightarrow \mathbb{CP}^2$$

$$(x_1 : x_0) * (y_1 : y_0) = (u_2 : u_1 : u_0)$$

$$\begin{cases} u_2 = (x_1 y_0 - x_0 y_1)^2, \\ -\frac{1}{2} u_1 = x_1 x_0 (2a_1 y_1 y_0 + a_2 y_1^2 + y_0^2) + x_1^2 y_1 (a_2 y_0 + 2a_3 y_1) + x_0^2 y_0 y_1, \\ u_0 = x_1^2 y_1 (a_2^2 y_1 - 4a_3(a_1 y_1 + y_0)) - 2x_0 x_1 y_1 (a_2 y_0 + 2a_3 y_1) + x_0^2 y_0^2. \end{cases}$$

Theorem (Buchstaber, Kornev, 2025)

(II) The isomorphism class of the coset algebraic 2-valued group $\mathbb{G}_{\mathbb{CP}^1}(B_a)$ is completely determined by the j -invariant of the elliptic curve $\mathcal{E}$:

$$j(a) = 6912 \frac{(3a_2 - a_1^2)^3}{4(3a_2 - a_1^2)^3 + (27a_3 - 9a_1a_2 + 2a_1^3)^2}.$$

3-Valued Structures on $\mathbb{CP}^1$

There is a unique projective equivalence class of nonsingular cubic curves whose groups of points contain elements of order 3 (in this case the j -invariant equals 0).

For each complex number $c \neq 0$, the *equiharmonic cubic*

$$\mathcal{E} = \{ y^2 = x^3 + c \}$$

belongs to this class [Dol12, Theorem 3.1.3].

3-Valued Structures on $\mathbb{C}P^1$

Introduce the slope

$$m = m((x_1, y_1), (x_2, y_2)) = \frac{y_1 - y_2}{x_1 - x_2}.$$

Then we have for the addition law:

$$\begin{cases} x_3 = -x_1 - x_2 + m^2, \\ y_3 = m(x_1 - x_3) - y_1. \end{cases}$$

The curve $\mathcal{E}$ admits an automorphism

$$\varphi_3 : (x, y) \mapsto (\varepsilon x, y)$$

of order 3 as an abelian variety, where $\varepsilon = e^{2\pi i/3}$. Indeed,

$$\begin{aligned} \varphi_3(x_1, y_1) \oplus \varphi_3(x_2, y_2) &= \left(-\varepsilon x_1 - \varepsilon x_2 + \left(\frac{y_1 - y_2}{\varepsilon x_1 - \varepsilon x_2} \right)^2, \right. \\ &\quad \left. \frac{y_1 - y_2}{\varepsilon x_1 - \varepsilon x_2} (\varepsilon x_1 - \varepsilon x_3) - y_1 \right) = \varphi_3(x_3, y_3). \end{aligned}$$

3-Valued Structures on $\mathbb{CP}^1$

The orbit $\{(x, y), (\varepsilon x, y), (\varepsilon^2 x, y)\}$ of the automorphism φ_3 corresponds bijectively to the value of y . There is a branched triple covering

$$\pi : \mathcal{E} \rightarrow \mathbb{CP}^1$$

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

$$\infty \mapsto \infty.$$

whose base is identified with the orbit space $\mathcal{E} / \langle \varphi_3 \rangle$. The branch points are $\pm\sqrt{c}$ and ∞ .

$$\begin{aligned} y_1 * y_2 &= [\pi((x_1, y_1) \oplus (\varepsilon^k x_2, y_2)) \mid k = 0, 1, 2] \\ &= \left[m_k \left(2\sqrt[3]{y_1^2 - c} + \varepsilon^k \sqrt[3]{y_2^2 - c} - m_k^2 \right) - y_1 \right], \end{aligned}$$

$$\text{where } m_k = \frac{y_1 - y_2}{\sqrt[3]{y_1^2 - c} - \varepsilon^k \sqrt[3]{y_2^2 - c}}, \quad k = 0, 1, 2.$$

3-Valued Structures on $\mathbb{CP}^1$

Theorem (Buchstaber, Kornev, 2025)

On $\mathbb{CP}^1$, for each nonzero $c \in \mathbb{C}$ there exists a structure (which we call *equiharmonic*) of an algebraic 3-valued coset group $\mathbb{G}_{3,\text{eqh}}(\mathbb{CP}^1)$ with neutral element 0, the map $\text{inv}(x) = -x$, and addition given by the polynomial $p_{3,\text{eqh}}(z; x, y)$, where

$$\begin{aligned} p_{3,\text{eqh}}(-z; x, y) = & e_1^3 - 27e_3 \\ & + 18c e_1^2 e_3 - 54c e_2 e_3 - 27c^2 e_2^2 e_3 + 81c^2 e_1 e_3^2, \end{aligned}$$

and e_k denotes the k -th elementary symmetric function in x, y, z . All such 3-valued groups are isomorphic.

Symmetric 3-Algebraic 3-Valued Groups

Let us now describe all symmetric 3-algebraic 3-valued groups.

The general form of the polynomials P_3 is as follows:

$$\begin{aligned} &\sigma_1^3 + k_0\sigma_3 + k_6\sigma_3^2 + k_{12}\sigma_3^3 + k_2\sigma_1\sigma_3 + k_4\sigma_2\sigma_3 + \ell_6\sigma_1\sigma_2\sigma_3 \\ &+ \ell_4\sigma_1^2\sigma_3 + k_8\sigma_2^2\sigma_3 + \ell_8\sigma_3^2\sigma_1 + k_{10}\sigma_3^2\sigma_2, \end{aligned}$$

where σ_i 's are elementary symmetric polynomials and k_i 's are parameters.

Theorem (Buchstaber, Kornev, 2025)

There are two classes of symmetric 3-algebraic 3-valued groups:

(I) If $k_0 = -27$, we have

$$P_3(z; -x, -y) = (\sigma_1^3 - 27\sigma_3) + 18c\sigma_1^2\sigma_3 - 54c\sigma_2\sigma_3 - 27c^2\sigma_2^2\sigma_3 + 81c^2\sigma_1\sigma_3^2.$$

(II) If $k_0 = 0$, we have

$$P_3(z; -x, -y) = (\sigma_1 + \alpha\sigma_3)^3,$$

In this case, the 3-valued group is obtained by the diagonal construction $G \times G \xrightarrow{\mu} G \xrightarrow{\text{Sym}^3 \circ \text{diag}} \text{Sym}^3(G)$ from the 1-algebraic 1-valued group G , constructed by the polynomial $P_1(z; -x, -y) = \sigma_1 + \alpha\sigma_3$.

4-Valued Structures on $\mathbb{CP}^1$

There is a unique projective equivalence class of nonsingular cubic curves whose automorphism group is isomorphic to $\mathbb{Z}/4$ (in this case the j -invariant equals 1728).

This class consists of the *harmonic cubics* [Dol12, Theorem 3.1.3]

$$\mathcal{E} = \{ y^2 = x^3 + bx \}.$$

Consider the map

$$\begin{aligned}\varphi_4 : \mathcal{E} &\rightarrow \mathcal{E} \\ (x, y) &\mapsto (-x, iy)\end{aligned}$$

which is clearly an automorphism of the abelian variety $\mathcal{E}$. The orbit space $\mathcal{E} / \langle \varphi_4 \rangle$ is identified with the fibers of

$$\begin{aligned}\pi_4 : \mathcal{E} &\rightarrow \mathbb{C}P^1 \\ (x, y) &\mapsto x^2, \\ \infty &\mapsto \infty\end{aligned}$$

Write the 4-valued addition law:

$$\begin{aligned}x_1 * x_2 &= \left[\pi_4 \left((x_1, y_1), \varphi_4^r(x_2, y_2) \right) \mid r = 0, \dots, 3 \right] \\ &= \left[\left(-\sqrt{x_1} - (-1)^\ell \sqrt{x_2} + m_{\ell,k}^2 \right)^2 \mid k, \ell = 0, 1 \right],\end{aligned}\tag{2}$$

where

$$m_{\ell,k} = \frac{\sqrt{\sqrt{x_1^3} + b\sqrt{x_1}} - (-1)^k \cdot \sqrt{(-1)^\ell (\sqrt{x_2^3} + b\sqrt{x_2})}}{\sqrt{x_1} - (-1)^\ell \sqrt{x_2}}.$$

4-Valued Structures on $\mathbb{C}P^1$

Theorem (Buchstaber, Kornev, 2025)

On $\mathbb{C}P^1$, for each nonzero $b \in \mathbb{C}$ there exists a structure (which we call harmonic) of an involutive algebraic 4-valued coset group $\mathbb{G}_{4,\text{har}}(\mathbb{C}P^1)$ with neutral element 0, whose addition is given by the polynomial

$$\begin{aligned} p_{4,\text{har}}(z; x, y) = & e_1^4 - 8 e_1^2 e_2 + 16 e_2^2 - 128 e_1 e_3 \\ & - 112 b e_1^2 e_3 - 4 b^2 e_1^3 e_3 - 64 b e_2 e_3 \\ & - 112 b^2 e_1 e_2 e_3 - 64 b^2 e_3^2 \\ & - 288 b^3 e_1 e_3^2 + 6 b^4 e_1^2 e_3^2 - 136 b^4 e_2 e_3^2 \\ & - 112 b^5 e_3^3 - 4 b^6 e_1 e_3^3 + b^8 e_3^4 \end{aligned}$$

where e_k denotes the k -th elementary symmetric function in x, y, z . All such 4-valued groups are isomorphic.

6-Valued Structures on $\mathbb{CP}^1$

There is a unique projective equivalence class of nonsingular cubics (with j -invariant equal to 0) whose group of points is isomorphic to $\mathbb{Z}/6$.

For each complex number $c \neq 0$, the *equiharmonic cubic*

$$\mathcal{E} = \{y^2 = x^3 + c\}$$

belongs to this class [Dol12, Theorem 3.1.3].

Consider the map ($\varepsilon = e^{2\pi i/3}$)

$$\varphi_6 : \mathcal{E} \rightarrow \mathcal{E}$$

$$(x, y) \mapsto (\varepsilon x, -y),$$

$$\infty \mapsto \infty.$$

φ_6 is an automorphism of the abelian variety $\mathcal{E}$. The points of the orbit space $\mathcal{E} / \langle \varphi \rangle$ are identified with the fibers of the map:

$$\pi_6 : \mathcal{E} \rightarrow \mathbb{CP}^1$$

$$(x, y) \mapsto y^2,$$

$$\infty \mapsto \infty.$$

$$y_1 * y_2 = [\pi_6((x_1, y_1), \varphi_6^r(x_2, y_2)) \mid r = 0, \dots, 5]$$

$$= \left[\left(m_{\ell,k} \left(2\sqrt[3]{y_1 - c} + \varepsilon^k \sqrt[3]{y_2 - c} - m_{\ell,k}^2 \right) - \sqrt{y_1} \right)^2 \mid \begin{array}{l} k = 0, 1, 2; \\ \ell = 0, 1 \end{array} \right],$$

$$\text{where } m_{\ell,k} = \frac{\sqrt{y_1} - (-1)^\ell \sqrt{y_2}}{\sqrt[3]{y_1 - c} - \varepsilon^k \cdot \sqrt[3]{y_2 - c}}.$$

Theorem (Buchstaber, Kornev, 2025)

For each nonzero $c \in \mathbb{C}$, there exists a unique structure (*equiharmonic*) of an involutive 6-valued algebraic coset group $\mathbb{G}_{6,\text{eqh}}(\mathbb{C}P^1)$ with neutral element 0 and addition given by

$$\begin{aligned} p_{6,\text{eqh}}(z; -x, -y) = & e_1^6 - 2^2 \cdot 3 e_1^4 e_2 + 2^4 \cdot 3 e_1^2 e_2^2 - 2^6 e_2^3 - 2 \cdot 3^4 \cdot 17 e_1^3 e_3 \\ & - 2^3 \cdot 3^4 \cdot 19 e_1 e_2 e_3 + 3^3 \cdot 19^3 e_3^2 \\ & - 2^5 \cdot 3^2 \cdot 11 c e_1^4 e_3 - 2^2 \cdot 3^3 \cdot 5 c^2 e_1^5 e_3 - 2^4 \cdot 3^2 \cdot 211 c e_1^2 e_2 e_3 \\ & - 2^2 \cdot 3^3 \cdot 197 c^2 e_1^3 e_2 e_3 - 2^3 \cdot 3^5 c^3 e_1^4 e_2 e_3 - 2^6 \cdot 3^2 \cdot 5^2 c e_2^2 e_3 \\ & - 2^4 \cdot 3^3 \cdot 107 c^2 e_1 e_2^2 e_3 - 2^4 \cdot 3^7 c^3 e_1^2 e_2^2 e_3 - 2 \cdot 3^6 c^4 e_1^3 e_2^2 e_3 \\ & - 2^6 \cdot 3^5 c^3 e_2^3 e_3 - 2^3 \cdot 3^7 c^4 e_1 e_2^3 e_3 + 2^4 \cdot 3^3 \cdot 7^2 \cdot 19 c e_1 e_3^2 \\ & + 2^2 \cdot 3^3 \cdot 47 \cdot 53 c^2 e_1^2 e_3^2 + 2^3 \cdot 3^5 \cdot 61 c^3 e_1^3 e_3^2 + 2 \cdot 3^7 \cdot 17 c^4 e_1^4 e_3^2 \\ & + 2^2 \cdot 3^4 \cdot 701 c^2 e_2 e_3^2 + 2^3 \cdot 3^6 \cdot 7 \cdot 13 c^3 e_1 e_2 e_3^2 + 2^{10} \cdot 3^6 c^4 e_1^2 e_2 e_3^2 \\ & + 2^4 \cdot 3^8 \cdot 5 c^5 e_1^3 e_2 e_3^2 + 2 \cdot 3^7 \cdot 5 \cdot 17 c^4 e_2^2 e_3^2 + 2^5 \cdot 3^8 \cdot 7 c^5 e_1 e_2^2 e_3^2 \\ & + 2^2 \cdot 3^9 \cdot 17 c^6 e_1^2 e_2^2 e_3^2 + 2^2 \cdot 3^9 \cdot 11 c^6 e_2^3 e_3^2 + 2^3 \cdot 3^{11} c^7 e_1 e_2^3 e_3^2 \\ & + 3^{12} c^8 e_2^4 e_3^2 - 2^3 \cdot 3^{12} c^3 e_3^3 - 2 \cdot 3^9 \cdot 5 \cdot 47 c^4 e_1 e_3^3 \\ & - 2^4 \cdot 3^9 \cdot 17 c^5 e_1^2 e_3^3 - 2^2 \cdot 3^9 \cdot 5 c^6 e_1^3 e_3^3 - 2^6 \cdot 3^{11} c^5 e_2 e_3^3 \\ & - 2^2 \cdot 3^{10} \cdot 5 \cdot 11 c^6 e_1 e_2 e_3^3 - 2^3 \cdot 3^{11} c^7 e_1^2 e_2 e_3^3 - 2^3 \cdot 3^{11} \cdot 5 c^7 e_2^2 e_3^3 \\ & - 2 \cdot 3^{12} c^8 e_1 e_2^2 e_3^3 - 2^3 \cdot 3^{12} c^6 e_3^4 - 2^3 \cdot 3^{12} c^7 e_1 e_3^4 \\ & + 3^{12} c^8 e_1^2 e_3^4 - 2^2 \cdot 3^{13} c^8 e_2 e_3^4. \end{aligned}$$

Nodal Case

We now turn to singular cubics.

The change of variables

$$x \mapsto x + 1, \quad y \mapsto y + 1, \quad z \mapsto z + 1$$

shows that the Chebyshev $\mathbb{M}_{\text{mult}}(\mathbb{C}P^1)$ is isomorphic to the monoid $\mathbb{G}_{\mathbb{C}P^1}(B_a)$ with $a_1 = 1, a_2 = a_3 = 0$. This monoid corresponds to the cubic

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

Nodal Case

Theorem (Buchstaber, Kornev, 2025)

Let $\alpha \neq \beta \in \mathbb{C}$, and let $\mathcal{E} = \{y^2 = (x - \alpha)^2(x - \beta)\}$. Then the addition of points on $\mathcal{E}$ and the involution σ define on $\mathbb{CP}^1$ a unique structure of a 2-valued coset algebraic monoid $\mathbb{M}_{\text{node}}(\mathbb{CP}^1)$ with neutral element ∞ and operation

$$x_1 * x_2 = \left[\left(\frac{\sqrt{x_1 - \beta} \sqrt{x_2 - \beta} \pm (\alpha - \beta)}{\sqrt{x_1 - \beta} \pm \sqrt{x_2 - \beta}} \right)^2 + \beta \right],$$

given by the Kontsevich polynomial $D_{\alpha, \beta}(-z; -x_1, -x_2)$. The element α is absorbing, i.e., $x * \alpha = \alpha * x = \alpha$ for any $x \in \mathbb{CP}^1 \setminus \{\alpha\}$. The product $\alpha * \alpha$ is not defined. Moreover, the element 0 has an inverse ($\text{inv}(0) = 0, 0 * 0 = [\alpha(1 - \alpha/(4\beta)), \infty]$) if and only if $\alpha \neq 0$.

Cuspidal Case

Theorem (Buchstaber, Kornev, 2025)

Let $\alpha \in \mathbb{C}$ and let $\mathcal{E} = \{y^2 = (x - \alpha)^3\}$.

- (I) The addition of points on $\mathcal{E}$ and the involution define on $\mathbb{C}P^1$ a unique structure of a 2-valued coset algebraic monoid $\mathbb{M}_2(\mathbb{C}P^1)$.
- (II) The group $\mathbb{G}_{3,\text{eqh}}(\mathbb{C}P^1)$ tends, as $c \rightarrow 0$, to the monoid $\mathbb{M}_3(\mathbb{C}P^1)$.
- (III) The group $\mathbb{G}_{4,\text{har}}(\mathbb{C}P^1)$ tends, as $b \rightarrow 0$, to the monoid $\mathbb{M}_4(\mathbb{C}P^1)$.
- (IV) The group $\mathbb{G}_{6,\text{eqh}}(\mathbb{C}P^1)$ tends, as $c \rightarrow 0$, to the monoid $\mathbb{M}_6(\mathbb{C}P^1)$.

Basics of Projective Duality

Consider a projective space $\mathbb{P} = \mathbb{P}(V_{\mathbb{C}})$. Hyperplanes in $\mathbb{P}$ form the dual projective space $\mathbb{P}^* = \mathbb{P}(V^*)$.

Let $X \subset \mathbb{P}$ be a closed *irreducible* algebraic subvariety.

A hyperplane $H \subset \mathbb{P}$ is said to be tangent to X if there exists a smooth point $x \in X$ such that $x \in H$ and the tangent space to H at x contains the tangent space to X at x , i.e. $\mathcal{T}_x X \subset \mathcal{T}_x H$.

Denote by $X^\vee \subset \mathbb{P}^*$ the closure of the set of all hyperplanes tangent to X . The variety $X^\vee$ is called *projectively dual* to X .

Basics of Projective Duality



The Coffee Cup Caustic.

Grace Weir, 2005

Reproduced from graceweir.com/page31/page31.html

Basics of Projective Duality

- Let $H = \{\ell = 0\}$. Then

x is a singular point of $X \cap H \Leftrightarrow d\ell|_{\mathcal{T}_x X} = 0 \Leftrightarrow \mathcal{T}_x X \subset \mathcal{T}_x H$.

If X is smooth and does not lie in any hyperplane, then

$H \in X^\vee \Leftrightarrow \exists x \in X$ with $\mathcal{T}_x X \subset \mathcal{T}_x H \Leftrightarrow H \cap X$ is singular.

- For any projective variety $X \subset \mathbb{P}$ we have $(X^\vee)^\vee = X$.
- If $z \in X$ and $H \in X^\vee$ are smooth points, then

H is tangent to X at $z \Leftrightarrow z \subset \mathbb{P}^*$ is tangent to $X^\vee$ at H .

- If X is irreducible then $X^\vee$ is irreducible.

Basics of Projective Duality

For any smooth curve $X \subset \mathbb{P}^2$ of degree d , according to Plücker formulas [GKZ94, Proposition 2.4], we have $\deg X^\vee = d(d-1)$.

Hence, $X^\vee$ cannot be smooth for $\deg X > 3$ because $(X^\vee)^\vee = X$.

Basics of Projective Duality

Suppose that X is a hypersurface (not a hyperplane) in $\mathbb{P}(V)$. Then $X^\vee = \{\Delta_X = 0\}$ is a hypersurface in $\mathbb{P}(V^*)$. We shall call the *X -discriminant* the defining polynomial Δ_X of $X^\vee$.

Example. For $M_2^1 = \{x^2 + y^2 = z^2\}$, we have

$$(M_2^1)^\vee = \{u^2 + v^2 + w^2 = 0\}.$$

Example [GKZ94]. For the curve $M_3^1 = \{x^3 + y^3 = z^3\}$ we have

$$(M_3^1)^\vee = \{u^6 + v^6 + w^6 - 2u^3v^3 - 2u^3w^3 - 2v^3w^3 = 0\}.$$

The curve $(M_3^1)^\vee$ is not smooth since M_3^1 is smooth and $\deg M_3^1 = 3 > 2$.

Fermat Curves and $\mathbb{G}_d(\mathbb{C})$

Theorem (Buchstaber, Kornev, 2025)

Consider the Fermat curve ($d \geq 2$)

$$M_d^1 = \{x^d + y^d = z^d\}.$$

Then the dual curve $(M_d^1)^\vee \subset (\mathbb{P}^2)^*$ is given by the equation

$$p_{d-1}(w^d; u^d, v^d) = 0.$$

Projective Duality is a Shift on $\mathbb{M}_d$'s

For each $d \geq 2$ consider a curve

$$X_d = \{p_d(z; x, y) = 0\}.$$

Theorem (Buchstaber, Kornev, 2025)

Under projective duality the curve X_d ($d \geq 2$) goes to

$$X_d^\vee = \{ (uvw)^{d-1} p_{d-1}(1/w; 1/u, 1/v) = 0 \} \subset (\mathbb{CP}^2)^*.$$

The composition of the duality $X_d \mapsto X_d^\vee$ with the subsequent Möbius transformation $(u, v, w) \mapsto (1/u, 1/v, 1/w)$ defines a shift operation

$$\mathbb{M}_d(\mathbb{CP}^1) \mapsto \mathbb{M}_{d-1}(\mathbb{CP}^1)$$

in the family of algebraic d -valued monoids.

Fermat Hypersurfaces and $p_{d,n}$'s

Theorem (Buchstaber, Kornev, 2025)

Let M_d^{n-1} be a Fermat hypersurface

$$M_d^{n-1} = \{x_1^d + x_2^d + \dots + x_n^d = z^d\}$$

in $\mathbb{C}P^n$ with coordinates $x_1, \dots, x_n, z$. The dual hypersurface is defined by the equation

$$(M_d^{n-1})^\vee = \{p_{d-1,n}(w^d; u_1^d, \dots, u_n^d) = 0\}$$

in $(\mathbb{C}P^n)^*$ with the dual coordinates $u_1, \dots, u_n, w$.

References I

- [BGR24] Buchstaber V., Gaiur I., Rubtsov V.
Algebraic 2-Valued Group Structures on $\mathbb{P}^1$, Kontsevich-type Polynomials, and Multiplication Formulas, I.
arXiv:2412.07330.
<https://arxiv.org/abs/2412.07330>
- [BK25a] Buchstaber V., Kornev M.
Algebraic n -Valued Monoids on $\mathbb{CP}^1$, Discriminants and Projective Duality.
arXiv:2510.14010.
<https://doi.org/10.48550/arXiv.2510.14010>
- [BK25b] Buchstaber V., Kornev M.
 n -Valued Groups, Kronecker Sums, and Wendt's Matrices.
arXiv:2505.04296.
<https://doi.org/10.48550/arXiv.2505.04296>
- [BN71] Buhštaber V.M., Novikov S.P.
Formal groups, power systems and Adams operators.
Math. USSR-Sb., 13(1) (1971) 80–116.
<https://doi.org/10.1070/SM1971v013n01ABEH001030>
- [BR98] Buchstaber V.M., Rees E.G.
Multivalued Groups, n-Hopf Algebras and n-Ring Homomorphisms.
Springer Netherlands, Dordrecht (1998)
- [Buc06] Buchstaber V.M.
 n -Valued Groups: Theory and Applications.
Mosc. Math. J., 6(1) (2006) 57–84.
<https://doi.org/10.17323/1609-4514-2006-6-1-57-84>
- [BV19] Buchstaber V.M., Veselov A.P.
Conway Topograph, $\mathrm{PGL}_2(\mathbb{Z})$ -Dynamics and Two-Valued Groups.
Russian Mathematical Surveys, 74(3) (2019) 387—430.
<https://doi.org/10.1070/RM9886>

References II

- [BVEP96] Buchstaber V.M., Vershik A.M., Evdokimov S.A., Ponomarenko I.N.
Combinatorial algebras and multivalued involutive groups.
Funct. Anal. Appl., 30(3) (1996) 158–162.
<https://doi.org/10.1007/BF02509502>
- [BVG22] Buchstaber V.M., Veselov A.P., Gaifullin A.A.
Classification of involutive commutative two-valued groups.
Russian Mathematical Surveys, 77(4) (2022) 651–727.
<https://doi.org/10.4213/rm10064e>
- [Dol12] Dolgachev I.V.
Classical Algebraic Geometry: A Modern View.
Cambridge University Press (2012).
<https://doi.org/10.1017/CB09781139084437>
- [FW69] Fulton W., Weiss R.
Algebraic Curves: An Introduction to Algebraic Geometry.
Addison-Wesley Publishing Company, Inc. The Advanced Book Program (1969).
<https://api.semanticscholar.org/CorpusID:116886820>
- [Gai24] Gaifullin A.A.
Commutativity of involutive two-valued groups.
Russian Mathematical Surveys, 79(2) (2024) 363–365.
<https://doi.org/10.4213/rm10170e>
- [GKZ94] Gelfand I.M., Kapranov M.M., Zelevinsky A.V.
Discriminants, resultants, and multidimensional determinants.
Modern Birkhäuser Classics. Birkhäuser Boston, MA (1994).
<https://doi.org/10.1007/978-0-8176-4771-1>

References III

- [GPV25] Guo J., Ponomarenko I., Vasil'ev A.V.
On multivalued groups of order 3.
Science China Mathematics, 68 (2025) 1969–1978.
<https://doi.org/10.1007/s11425-024-2388-0>
- [Har77] Hartshorne R.
Algebraic Geometry.
Graduate Texts in Mathematics. Springer New York, NY (1977).
<https://doi.org/10.1007/978-1-4757-3849-0>
- [Kor25] Kornev M.
On the Classification of n -Valued Monoids and Groups of Order 3.
arXiv.2508.04454.
<https://doi.org/10.48550/arXiv.2508.04454>
- [Pon24] Ponomarenko I.N.
On a family of multivalued groups.
Proceedings of the Steklov Institute of Mathematics, 326 (2024) 286–288.
<https://doi.org/10.1134/S0081543824040138>
- [Rib99] Ribenboim P.
Fermat's Last Theorem for Amateurs.
Springer New York, NY, 1st edition (1999).
<https://doi.org/10.1007/b97437>
- [Sté00] Stéphanos C.
Sur une extension du calcul des substitutions linéaires.
Journal de Mathématiques Pures et Appliquées, 6(5) (1900) 73–128.
https://www.numdam.org/item/JMPA_1900_5_6__73_0/

References IV

- [Wen94] Wendt E.
Arithmetische Studien über den 'letzten' Fermatschen Satz, welcher aussagt, dass die Gleichung $a^n = b^n + c^n$ für $n > 2$; in ganzen Zahlen nicht auflösbar ist.
Journal für die reine und angewandte Mathematik, 113(335-347).
<https://doi.org/10.18452/175>
- [Wol62] Wolstenholme J.
On certain properties of prime numbers.
The Quarterly Journal of Pure and Applied Mathematics, 5 (1862) 35-39

Thank you for attention!