Algebraic n-Valued Monoids on $\mathbb{C}P^1$, Discriminants and Projective Duality

Victor Buchstaber and Mikhail Kornev

Abstract

In this work, we establish connections between the theory of algebraic n-valued monoids and groups and the theories of discriminants and projective duality. We show that the composition of projective duality followed by the Möbius transformation $z \mapsto 1/z$ defines a shift operation $\mathbb{M}_n(\mathbb{C}P^1) \mapsto \mathbb{M}_{n-1}(\mathbb{C}P^1)$ in the family of algebraic n-valued coset monoids $\{\mathbb{M}_n(\mathbb{C}P^1)\}_{n\in\mathbb{N}}$. We also show that projective duality sends each Fermat curve $x^n + y^n = z^n$ $(n \geq 2)$ to the curve $p_{n-1}(z^n; x^n, y^n) = 0$, where the polynomial $p_n(z; x, y)$ defines the addition law in the monoid $\mathbb{M}_n(\mathbb{C}P^1)$. We solve the problem of describing coset n-valued addition laws constructed from cubic curves. As a corollary, we obtain that all such addition laws are given by polynomials, whereas the addition laws of formal groups on general cubic curves are given by series.

Contents

1 Introduction **2**

2 Algebraic n-Valued Monoids and Groups **5**

3 Projective Duality and the Family of Monoids $\mathbb{M}_n(\mathbb{C}P^1)$ **11**

4 The Laws $p_n(z; x, y)$ and Discriminants of Field Extensions **17**

5 Cubics and n-Valued Coset Addition Laws **18**

5.1 The Case of a Nonsingular Cubic 19

5.1.1 2-Valued Structures on $\mathbb{C}P^1$ 19

5.1.2 3-Valued Structures on $\mathbb{C}P^1$ 22

5.1.3 4-Valued Structures on $\mathbb{C}P^1$ 24

5.1.4 6-Valued Structures on $\mathbb{C}P^1$ 25

5.2 Nodal Case 27

5.3 Cuspidal Case 30

1 Introduction

In [BGR24, GRS24], the addition laws of algebraic n-valued groups on $\mathbb{C}P^1$ [Buc06] were expressed in terms of discriminants. In the present work, we develop the connection between the theory of algebraic n-valued monoids and n-valued groups on $\mathbb{C}P^1$ and the theories of discriminants and projective duality [GKZ94]. We use algebro-geometric methods without invoking the theory of elliptic functions.

An algebraic n-valued monoid is an algebraic variety X with an associative n-valued multiplication (addition) given by a rational morphism

$$X \times X \to \mathrm{Sym}^n(X)$$

with a neutral element (zero) $e \in X$, i.e.

$$x * e = e * x = [x, x, \dots, x]$$

for every $x \in X$. An algebraic n-valued group is an algebraic n-valued monoid on X together with a morphism $\mathrm{inv} : X \to X$ such that for each $x \in X$ one has $e \in x * \mathrm{inv}(x)$ and

$$x * \mathrm{inv}(x) = \mathrm{inv}(x) * x.$$

Let

$$\delta_{\boldsymbol{a}} = \Delta_t\big(t^3 + a_1 t^2 + a_2 t + a_3\big)$$

be the discriminant. It is shown in [BV19, Theorem 6.3], [BK25, Theorem 1] that for any choice of complex parameters $\boldsymbol{a} = (a_1, a_2, a_3)$ the Buchstaber polynomial

$$B_{\boldsymbol{a}}(z; x, y) = (x + y + z - a_2 xyz)^2 - 4(1 + a_3 xyz)(xy + yz + xz + a_1 xyz) \tag{1}$$

defines the structure of the universal symmetric 2-algebraic 2-valued group $\mathbb{G}_{\mathbb{C}}(B_{\boldsymbol{a}})$ on $\mathbb{C}$ with addition

$$x * y = \{\, z \mid B_{\boldsymbol{a}}(z; x, y) = 0 \,\},$$

zero 0, and inverse $\mathrm{inv}(x) = x$. According to the recent work [BGR24, Theorem 4.7], when $\delta_{\boldsymbol{a}} \neq 0$ the law (1) induces a 2-valued group structure on $\mathbb{C}P^1$.

As noted in [BGR24], one has

$$D_{\boldsymbol{a}}(z; x, y) = (xyz)^2\, B_{\boldsymbol{a}}\left(-\frac{1}{z}; -\frac{1}{x}, -\frac{1}{y}\right),$$

where $D_{\boldsymbol{a}}(z; x, y)$ is the generalized Kontsevich polynomial.

Following [BK25, Example 2], denote by $\mathbb{G}_n(\mathbb{C})$ the coset [Buc06, Theorem 1] n-valued algebraic group on $\mathbb{C}$ with zero 0, inverse $\mathrm{inv}(x) = (-1)^n x$, and addition

$$x * y = \big[\, z \mid p_n\big(z; (-1)^n x, (-1)^n y\big) = 0 \,\big],$$

where

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

is a symmetric polynomial with integer coefficients, and $\varepsilon = e^{2\pi i/n}$ for a fixed branch of $\sqrt[n]{-}$.

The first result of our paper (Theorem 1) states that under projective duality the Fermat curve $\{x^n + y^n = z^n\}$ maps to the curve $\{p_{n-1}(z^n; x^n, y^n) = 0\}$.

Theorem 2 shows that the structure of the algebraic n-valued coset group $\mathbb{G}_n(\mathbb{C})$ extends (only) to the structure of an algebraic n-valued monoid $\mathbb{M}_n(\mathbb{C}P^1)$ on $\mathbb{C}P^1$. Here the point ∞ is absorbing, i.e.

$$\infty * x = x * \infty = [\infty, \infty, \dots, \infty] \quad \text{for every } x \in \mathbb{C}P^1 \setminus \{\infty\}.$$

For each natural n, the polynomial p_n defines a curve

$$X_n = \{p_n(z;x,y) = 0\}$$

in $\mathbb{C}P^2$. By Theorem 3, under projective duality the curve X_n ($n \geq 2$) goes to

$$X_n^\vee = \{(uvw)^{n-1} p_{n-1}(1/w; 1/u, 1/v) = 0\} \subset (\mathbb{C}P^2)^*,$$

and the composition of the duality $X_n \mapsto X_n^\vee$ with the subsequent Möbius transformation $(u,v,w) \mapsto (1/u, 1/v, 1/w)$ defines a shift operation $\mathbb{M}_n(\mathbb{C}P^1) \mapsto \mathbb{M}_{n-1}(\mathbb{C}P^1)$ in the family of algebraic n-valued monoids. From the Plücker formulas [GKZ94, Proposition 2.4] it follows that if X is smooth curve of degree n then the curve $X^\vee$ has degree $n(n-1)$. In our case X_n and $X_n^\vee$ are singular for $n \geq 3$, we have $\deg X_n = n$ and $\deg X_n^\vee = (n-1)^2$. The curves X_2 and $X_2^\vee$ are nonsingular (see Example 11).

Recall that by [GRS24, Theorem 2.3] the polynomial $p_n(z;x,y)$ and the discriminant $\Delta_t(P_{x,y,z}(t))$ of

$$P_{x,y,z}(t) = (-1)^n x\, t^{n-1}(1+t)^{n-1} + (-1)^n y(1+t)^{n-1} - t^{n-1} z$$

in the variable t satisfy

$$(-1)^n (n-1)^{2(n-1)} (xyz)^{n-2} p_n(z;x,y) = \Delta_t\big(P_{x,y,z}(t)\big). \tag{2}$$

For an explicit proof see [BK25, Theorem 8]. Theorems 1, 2, and 3 explain (2) via the theory of [GKZ94] relating discriminants and projective duality.

Iterations of the n-valued addition in $\mathbb{G}_n(\mathbb{C})$ are given by the symmetric polynomials

$$p_{n,m}(z;\boldsymbol{x}) = \prod_{k_1,\dots,k_m=1}^{n} \left(\sqrt[n]{z} + \varepsilon^{k_1} \sqrt[n]{x_1} + \cdots + \varepsilon^{k_m} \sqrt[n]{x_m}\right),$$

which arise, for example, in connection with Picard–Fuchs differential equations [GRS24, Section 3]. We denote by $\mathcal{O}_{n,m}(\mathbb{C}P^1)$ the variety $\mathbb{C}P^1$ equipped with this operation. Let $X_{n,m} = \{p_{n,m} = 0\}$ be the hypersurface in $\mathbb{C}P^m$, and set

$$P_{n,m}(w;\boldsymbol{u}) = (u_1 \cdots u_m w)^{n-1} p_{n-1}(w^{-1}; u_1^{-1}, \ldots, u_m^{-1}).$$

Then Theorem 4 asserts that the composition of the duality ($m \geq 2$, $n \geq 2$)

$$X_{n,m} \mapsto X_{n,m}^{\vee} = \{P_{n,m} = 0\} \subset (\mathbb{C}P^m)^*$$

with the subsequent Möbius transformation

$$(u_1, \ldots, u_m, w) \mapsto (1/u_1, \ldots, 1/u_m, 1/w)$$

defines a shift operation

$$\mathcal{O}_{n,m}(\mathbb{C}P^1) \mapsto \mathcal{O}_{n-1,m}(\mathbb{C}P^1)$$

in the family of m-ary n^{m-1}-valued algebraic structures $\mathcal{O}_{n,m}(\mathbb{C}P^1)$.

Theorem 5 is an iterated analog for Theorem 1. It gives the concrete realization

$$F_n^{\vee} = \{\, p_{n-1,m}(w^n; u_1^n, ..., u_m^n) = 0\}$$

of the polynomial equation for a Fermat hypersurface

$$F_{n,m} = \{\, x_1^n + ... + x_m^n = z^n \,\}.$$

An algebraic n-valued monoid (or group) on X is called regular if the n-valued multiplication $X \times X \longrightarrow \mathrm{Sym}^n(X)$ is defined on all of $X \times X$. An n-valued group X is called involutive if $\mathrm{inv}(x) = x$ for every $x \in X$. The coset construction for groups [Buc06, Theorem 1] carries over without difficulty to monoids. We call the n-valued monoid M_H built from a 1-valued monoid M and a subgroup H of order n in $\mathrm{Aut}(M)$ a coset monoid.

Theorem 6 gives a classification of all 2-valued coset groups and monoids obtained on elliptic curves by an involution. According to item **(i)** of Theorem 6, when $\delta_{\boldsymbol{a}} \neq 0$ the universal 2-valued group law $\mathbb{G}_{\mathbb{C}}(B_{\boldsymbol{a}})$ extends to a 2-valued coset algebraic regular involutive group $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ on $\mathbb{C}P^1$ with zero 0 and addition $\mu_{\boldsymbol{a}}$. The Möbius transformation $x \mapsto -1/x$, $y \mapsto -1/y$, $z \mapsto -1/z$ sends $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ to an isomorphic group $\mathbb{G}_{\mathbb{C}P^1}(D_{\boldsymbol{a}})$ with zero ∞ and addition given by the Kontsevich polynomial $D_{\boldsymbol{a}}(z; x, y)$. The group $\mathbb{G}_{\mathbb{C}P^1}(D_{\boldsymbol{a}})$ coincides with the coset group $\mathcal{E}_{\langle\sigma\rangle}$, where

$$\mathcal{E} = \{y^2 = x^3 + a_1 x^2 + a_2 x + a_3\} \tag{3}$$

is an elliptic curve and $\sigma : (x, y) \mapsto (x, -y)$, $\infty \mapsto \infty$ is the involution. This result was first obtained in [GRS24, Theorem 4.7] relying on the theory of elliptic functions. Our approach uses purely algebro-geometric methods. Item **(ii)** of Theorem 6 states that the groups $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ are classified by the j-invariant of the elliptic curve $\mathcal{E}$.

Call an element w of an n-valued monoid (group) $\mathbb{M}$ iterating (for $n = 2$, doubling) if for each $m \in \mathbb{M}$ the multisets $m * w$ and $w * m$ contain points of multiplicity at least 2. For $n = 2$ the set of doubling points forms a 2-valued diagonal submonoid (subgroup). If an n-valued algebraic group is given in some chart U by the roots in z of a polynomial $P(z; x, y)$, then an element y is iterating if and only if y is a root of the discriminant $\Delta_z(P(z; x, y))$ for every $x \in U$. Thus, the discriminant $\Delta_z(P(z; x, y))$ of the law $P(z; x, y)$ carries important information about the structure of an n-valued algebraic monoid. Theorem 7 shows that when $\delta_{\boldsymbol{a}} \neq 0$ the group of doubling points of the 2-valued group $\mathbb{G}(B_{\boldsymbol{a}})$ is isomorphic to the Klein four-group $\mathbb{Z}/2 \times \mathbb{Z}/2$.

In Theorems 8, 9, and 10, we explicitly describe the polynomials defining the addition in all possible (up to isomorphism) coset 3-, 4-, and 6-valued groups $\mathbb{G}_{3,\mathrm{eqh}}(\mathbb{C}P^1)$, $\mathbb{G}_{4,\mathrm{har}}(\mathbb{C}P^1)$, and $\mathbb{G}_{6,\mathrm{eqh}}(\mathbb{C}P^1)$ on $\mathbb{C}P^1$ modeled by elliptic curves and automorphisms. They correspond to the equiharmonic ($j = 0$, $\mathrm{Aut}\,\mathcal{E}(\mathbb{C}) \cong \mathbb{Z}/6$) and harmonic ($j = 1728$, $\mathrm{Aut}\,\mathcal{E}(\mathbb{C}) \cong \mathbb{Z}/4$) elliptic curves $\mathcal{E}$.

In the nodal case for the cubic $\mathcal{E}$, by Theorem 11 the coset group $\mathbb{G}_{\mathbb{C}P^1}(D_{\boldsymbol{a}})$ becomes (up to isomorphism) the coset monoid $\mathbb{M}_{\mathrm{node}}(\mathbb{C}P^1)$.

In the cuspidal case for the cubic $\mathcal{E}$, by Theorem 12 the coset groups $\mathbb{G}_{\mathbb{C}P^1}(D_{\boldsymbol{a}})$, $\mathbb{G}_{3,\mathrm{eqh}}(\mathbb{C}P^1)$, $\mathbb{G}_{4,\mathrm{har}}(\mathbb{C}P^1)$, and $\mathbb{G}_{6,\mathrm{eqh}}(\mathbb{C}P^1)$ become (up to isomorphism) the coset monoids $\mathbb{M}_2(\mathbb{C}P^1)$, $\mathbb{M}_3(\mathbb{C}P^1)$, $\mathbb{M}_4(\mathbb{C}P^1)$, and $\mathbb{M}_6(\mathbb{C}P^1)$, respectively.

The authors are grateful to Vladimir Rubtsov for helpful discussions during the preparation of this work.

2 Algebraic n-Valued Monoids and Groups

To state the results of this work, we recall and introduce several definitions and constructions.

Definition 1. An *algebraic n-valued monoid* is an algebraic variety X equipped with an associative n-valued multiplication given by a rational morphism $X \times X \to \mathrm{Sym}^n(X)$, i.e. specified on some Zariski open subset $Y \subset X \times X$ by a morphism $* : Y \to \mathrm{Sym}^n(X)$ of algebraic varieties, with a neutral element $e \in X$ such that

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

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

$$e \in x * \mathrm{inv}(x), \qquad x * \mathrm{inv}(x) = \mathrm{inv}(x) * x.$$

Example 1. On $\mathbb{C}P^1 = \mathbb{C} \cup \{\infty\}$ there is a structure of a 1-valued commutative algebraic Hadamard monoid $M_{\text{mult}}(\mathbb{C}P^1)$ 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 $(\operatorname{Sym}^2 \mathbb{C}P^1) \backslash [0, \infty]$. The element $\infty = (1 : 0)$ is absorbing in this monoid, i.e. $z * \infty = \infty$ for each $z \in \mathbb{C}P^1 \backslash \{0\}$. The elements of $\mathbb{C}P^1 \backslash \{0, \infty\}$, and only they, have inverse $\operatorname{inv}(z_1 : z_0) = (z_0 : z_1)$.

Example 2. On $\mathbb{C}P^1 = \mathbb{C} \cup \{\infty\}$ there is also a structure $M_{\text{cusp}}(\mathbb{C}P^1)$ 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 $(\operatorname{Sym}^2 \mathbb{C}P^1) \backslash [\infty, \infty]$. The elements of $\mathbb{C}P^1 \backslash \{\infty\}$, and only they, have inverse $\operatorname{inv}(z_1 : z_0) = (-z_1 : z_0)$.

Definition 2. Two algebraic (analytic, topological) n-valued monoids (groups) X and Y are called isomorphic if there exists an isomorphism (homeomorphism) $\varphi : X \to Y$ inducing the commutative diagram

$$\begin{tikzcd} X \times X \arrow[r] \arrow[d, "\cong"'] & \operatorname{Sym}^2(X) \arrow[d, "\cong"'] \\ Y \times Y \arrow[r] & \operatorname{Sym}^2(Y) \end{tikzcd} \tag{4}$$

Example 3. The algebraic 1-valued monoids $M_{\text{mult}}(\mathbb{C}P^1)$ and $M_{\text{cusp}}(\mathbb{C}P^1)$ are not isomorphic, since $M_{\text{mult}}(\mathbb{C}P^1)$ has elements of finite order.

Example 4. Consider the discrete coset group from [Buc06, Section 4] on the set $\mathbb{Z}_+$ of nonnegative integers with zero 0 and addition

$$x_1 * x_2 = [x_1 + x_2, |x_1 - x_2|].$$

Compare it with the coset subgroup $\mathbb{G}_2(\mathbb{Z}_+) \subset \mathbb{G}_2(\mathbb{C})$, which has zero 0 and addition

$$y_1 * y_2 = \left[(\sqrt{y_1} + \sqrt{y_2})^2, (\sqrt{y_1} - \sqrt{y_2})^2\right]$$

for all nonnegative integers y_1 and y_2. The squaring map $x \mapsto x^2$ is a bijection between the respective orbit spaces and makes the square (4) commute. Therefore these two 2-valued groups are isomorphic.

Definition 3. We say that an algebraic n-valued monoid (or group) on X is *regular* if the n-valued multiplication $X \times X \to \mathrm{Sym}^n(X)$ is defined on all of $X \times X$.

Definition 4. 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.

Example 5. Let

$$B_{\boldsymbol{a}}(z; x, y) = (x + y + z - a_2 xyz)^2 - 4(1 + a_3 xyz)(xy + yz + xz + a_1 xyz) \tag{5}$$

be the Buchstaber polynomial. In elementary symmetric functions:

$$B_{\boldsymbol{a}}(z; x, y) = e_1^2 - 4e_2 - 4a_1e_3 - 2a_2e_1e_3 - 4a_3e_2e_3 + (a_2^2 - 4a_1a_3)e_3^2.$$

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

$$x * y = [\, z \mid B_{\boldsymbol{a}}(z; x, y) = 0 \,],$$

neutral element 0, and inversion map $\mathrm{inv}(x) = x$ [BV19, Theorem 6.3], [BK25, Theorem 1].

Definition 5. Let M be a single-valued monoid on a set X, and let H be a subgroup of order n of its automorphism group $\mathrm{Aut}(M)$. We call the *coset n-valued monoid* M_H the result of applying the construction of [Buc06, Theorem 1] to M and H.

Proposition 1. The notion of a coset monoid is well-defined.

Proof. Let $\pi : G \to X = G/H$ be the projection to the orbit space. Suppose $\pi(g_1) = x_1$ and $\pi(g_2) = x_2$. Then the multiplication is arranged as follows:

$$\begin{aligned} x_1 * x_2 &= [\, \pi(\varphi(g_1) \cdot \psi(g_2)) \mid \varphi, \psi \in H \,] \\ &= [\, \pi\varphi(g_1 \cdot \varphi^{-1}\psi(g_2)) \mid \varphi, \psi \in H \,] \\ &= [\, \pi(g_1 \cdot \zeta(g_2)) \mid \zeta \in H \,]. \end{aligned}$$

For associativity we have, on the one hand,

$$\begin{aligned} (x_1 * x_2) * x_3 &= [\, \pi(g_1 \cdot \varphi(g_2)) * x_3 \mid \varphi \in H \,] \\ &= [\, \pi(g_1 \cdot \varphi(g_2) \cdot \psi(g_3)) \mid \varphi, \psi \in H \,]. \end{aligned}$$

And on the other hand,

$$\begin{aligned} x_1 * (x_2 * x_3) &= [\, x_1 * \pi(g_2 \cdot \varphi(g_3)) \mid \varphi \in H \,] \\ &= [\, \pi(g_1 \cdot \psi(g_2 \cdot \varphi(g_3))) \mid \varphi, \psi \in H \,] \\ &= [\, \pi(g_1 \cdot \psi(g_2) \cdot \psi(\varphi(g_3))) \mid \varphi, \psi \in H \,]. \end{aligned}$$

The identity is the class eH:

$$x * eH = eH * x = [\, g \cdot \varphi(e) \mid \varphi \in H \,] = [g, \dots, g].$$

□

Example 6 (The Chebyshev coset monoid)**.** On $M_{\mathrm{mult}}(\mathbb{C}P^1)$ (see Example 1) consider the involution $\tau : z \mapsto 1/z$ for each $z \in \mathbb{C}P^1$. Points of the orbit space of the involution τ are represented by fibers of the branched double covering

$$\begin{aligned} \pi : \mathbb{C}P^1 &\longrightarrow \mathbb{C}P^1 \\ z &\mapsto \tfrac{1}{2}\big(z + 1/z\big) \end{aligned}$$

with branch points ± 1. The corresponding coset monoid $\mathbb{M}_{\mathrm{mult}}(\mathbb{C}P^1) := M_{\mathrm{mult}}(\mathbb{C}P^1)_{\langle\tau\rangle}$ has identity 1 and multiplication

$$x * y = \left[xy \pm \sqrt{(x^2 - 1)(y^2 - 1)} \right], \tag{6}$$

defined on $(\mathrm{Sym}^2 \, \mathbb{C}P^1) \backslash [\infty, \infty]$. This structure of a 2-valued algebraic monoid does not extend to a structure of a 2-valued algebraic group. This example illustrates the use of the module square construction for monoids. The case of the multiplicative torus and the automorphism $z \mapsto 1/z$ was considered in [Buc06, Section 7, Example 3]. The addition law is given by the roots in z of the polynomial

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

In homogeneous coordinates the multiplication $\mathbb{C}P^1 \times \mathbb{C}P^1 \longrightarrow \mathrm{Sym}^2(\mathbb{C}P^1) \cong \mathbb{C}P^2$ is written as

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

For $x = \cos\alpha$, $y = \cos\beta$, the addition (6) becomes the cosine addition formulas. Consider the 2-valued submonoid $\mathbb{T} = \mathbb{T}(\mathbb{C})$ of $\mathbb{M}_{\mathrm{mult}}(\mathbb{C}P^1)$ generated by taking integral nonnegative powers of the element $\cos\alpha$. Let

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

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

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

This motivates the name of the monoid $\mathbb{T}$. The group $\mathbb{T}$ is isomorphic to $\mathbb{G}_2(\mathbb{C})$ (see Example 4).

Example 7. Let

$$p_n(z; x, y) = \prod_{r,s=1}^{n} \left(\sqrt[n]{z} + \varepsilon^r \sqrt[n]{x} + \varepsilon^s \sqrt[n]{y}\right), \tag{7}$$

where ε is a primitive nth root of unity, and $\sqrt[n]{-}$ denotes some fixed complex branch of the root. Then the polynomial $p_n(z; (-1)^n x, (-1)^n y)$ defines a commutative algebraic n-valued group $\mathbb{G}_n(\mathbb{C})$ on $\mathbb{C}$ with neutral element 0 and inverse $\mathrm{inv}(x) = (-1)^n x$. The group $\mathbb{G}_n(\mathbb{C})$ is obtained as a coset construction $\mathbb{G}_n(\mathbb{C}) = \mathbb{C}_{\langle\varphi\rangle}$ from the additive group $\mathbb{C}$ and its automorphism $\varphi : z \mapsto \varepsilon z$ of order n.

We introduce the notion of isomorphisms in the category of coset algebraic (topological) n-valued monoids.

Definition 6. Let M and N be single-valued algebraic (topological) monoids, and let $A \subset \mathrm{Aut}(M)$ and $B \subset \mathrm{Aut}(N)$ be finite subgroups of order n. We say that two coset monoids M_A and N_B are isomorphic if there exist isomorphisms $\widetilde{\varphi} : M \to N$ and $\varphi : M/A \to N/B$ making the following diagram commute:

$$\begin{tikzcd}
 & M \times M \arrow[rr] \arrow[dl, "\widetilde{\varphi}\times\widetilde{\varphi}"', "\cong"] \arrow[dd] & & \mathrm{Sym}^n(M) \arrow[dl, "\cong"] \arrow[dd] \\
N \times N \arrow[rr] \arrow[dd] & & \mathrm{Sym}^n(N) \arrow[dd] & \\
 & M/A \times M/A \arrow[rr] \arrow[dl, "\varphi\times\varphi"', "\cong"] & & \mathrm{Sym}^n(M/A) \arrow[dl, "\cong"] \\
N/B \times N/B \arrow[rr] & & \mathrm{Sym}^n(N/B) &
\end{tikzcd} \tag{8}$$

Moreover, all arrows connecting the front and back faces of the parallelepiped must be isomorphisms.

Example 8. The Möbius transformation $x \mapsto -1/x, y \mapsto -1/y, z \mapsto -1/z$ establishes an isomorphism of the groups $\mathbb{G}_{\mathbb{C}}(B_{\boldsymbol{a}}(z;x,y))$ and $\mathbb{G}_{\mathbb{C}P^1\setminus\{0\}}(D_{\boldsymbol{a}}(z;x,y))$.

We also recall the following.

Definition 7. An n-valued group G is called *involutive* if $\operatorname{inv}(x) = x$ for every $x \in G$.

Example 9. The group $\mathbb{G}_{\mathbb{C}}(B_{\boldsymbol{a}})$ from Example 5 is involutive.

Definition 8. An element w of an n-valued monoid M is called *iterating* if for any $m \in M$ each of the multisets $w * m$ and $m * w$ contains an element u (generally depending on m) with multiplicity at least 2. For $n = 2$ we call an iterating element w a *doubling* element.

Recall (see [Buc06, Lemma 1]) that the n-diagonal construction (or simply, the n-diagonal) of a single-valued monoid (group) G is the n-valued monoid (group) $\operatorname{diag}(G)$ in which $g_1 * g_2 = [g_1g_2, \dots, g_1g_2]$ 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).

Proposition 2. The set $\mathbb{W}$ of doubling elements of a 2-valued monoid (respectively, an involutive group) $\mathbb{M}$ forms a diagonal 2-valued submonoid (respectively, subgroup).

Proof. Let $\mathbb{W}$ denote the subset of $\mathbb{M}$ consisting of doubling elements. Suppose $w_1, w_2 \in \mathbb{W}$ and $w_1 * w_2 = [w_3, w_3]$ for some $w_3 \in \mathbb{M}$. Let $m \in \mathbb{M}$ be arbitrary. Then

$$\begin{aligned} [\, m * w_3,\ m * w_3 \,] &= m * (w_1 * w_2) \\ &= (m * w_1) * w_2. \end{aligned}$$

Hence $w_3 \in \mathbb{W}$, since the multiset $(m * w_1) * w_2$ is a certain 4-fold point. Define on the set $\mathbb{W}$ the operation

$$\begin{gathered} \mathbb{W} \times \mathbb{W} \to \mathbb{W} \\ w_1 \cdot w_2 = w_3. \end{gathered} \tag{9}$$

It is easy to see that the 2-valued submonoid $\mathbb{W} \subset \mathbb{M}$ is the 2-diagonal of the 1-valued monoid $\mathbb{W}$ with operation (9).

If $\mathbb{M}$ is an involutive group, then the monoid $\mathbb{W}$ is a group. Indeed, in this case the inverse element equals itself. □

Definition 9. We call the 1-valued monoid (group) from the proof of Proposition 2 the *monoid* (*group*) *of doubling points*.

Example 10. The Chebyshev coset 2-valued algebraic monoid from Example 6 has exactly two doubling elements, at the branch points (1 and −1) of the branched double covering in Example 6. Indeed, let y be an iterating element. Then the polynomial

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

has a multiple root in z for any x, i.e.

$$\Delta_z\big(P_{\mathrm{mult}}(z;x,y)\big) = 4(x^2-1)(y^2-1) = 0. \tag{10}$$

Hence $y \in \{\pm 1\}$. The resulting single-valued group of doubling points is isomorphic to $\mathbb{Z}/2$.

It is clear that under isomorphisms of 2-valued monoids, the single-valued monoids of doubling points are preserved.

Proposition 3. Let

$$\varphi : \mathbb{G}_1(f_1, U) \to \mathbb{G}_2(f_2, U)$$

be an isomorphism of algebraic n-valued groups given (over $\mathbb{C}$) in some neighborhood U by the roots in z of the polynomials $f_1(z;x,y)$ and $f_2(z;x,y)$. Then for any x there is a bijection between the roots in y of the discriminants $\Delta_{1,z}(f_1(z;x,y))$ and $\Delta_{2,z}(f_2(z;x,y))$ preserving multiplicities. Here $\Delta_{j,z} f_j(z;x,y)$ denotes the discriminant in the variable z of the polynomial $f_j(z;x,y)$.

Proof. The roots in y of the equation $\Delta_{j,z} f_j(z;x,y) = 0$ are precisely the iterating elements. Any isomorphism φ preserves iterating elements and their multiplicities (by continuity). □

3 Projective Duality and the Family of Monoids $\mathbb{M}_n(\mathbb{C}P^1)$

Consider the curve

$$X_n = \{\, p_n(z;x,y) = 0 \,\} \subset \mathbb{C}P^2,$$

where $p_n(z;x,y)$ is the polynomial (7) from Example 7.

Proposition 4. The projective dual of the curve X_n is the curve

$$X_n^\vee = \{\, P_{n-1}(w;u,v) = 0 \,\} \subset (\mathbb{C}P^2)^*,$$

where

$$P_{n-1}(w;u,v) = (uvw)^2\, p_{n-1}(w^{-1};u^{-1},v^{-1}).$$

Proof. It is easy to check that the curve $X_n \subset \mathbb{C}P^2$ admits the following rational parametrization:

$$(x,y,z) = \big((-s-t)^n,\ (-t)^n,\ s^n\big). \tag{11}$$

The chart $w = 1$ dual to $z = 1$ in $(\mathbb{C}P^2)^*$ consists of lines $ux + vy + 1 = 0$, each encoded by a pair (u, v). By the definition of projective duality (see, e.g., [GKZ94, Chapter 1, Section 1, Subsection B]), for any curve $X = (x(t), y(t))$ in the chart $z = 1$ its caustic $X^\vee$ in the chart $w = 1$ has a parametric representation $(u(t), v(t))$ such that the equation of the tangent to X at $(x(t), y(t))$ is

$$u(t)x + v(t)y + 1 = 0. \tag{12}$$

Hence

$$(u(t), v(t)) = \left(\frac{y'(t)}{R(t)}, \frac{-x'(t)}{R(t)}\right), \tag{13}$$
$$R(t) = x'(t)\,y(t) - x(t)\,y'(t).$$

Substituting (11) into (13), we obtain in the chart $w = 1$ the parametric equation for $X_n^\vee$:

$$(u, v) = \left((-1-t)^{1-n},\ t^{1-n}\right). \tag{14}$$

Since for odd n the value sets of the multivalued functions $u^{\frac{1}{1-n}}$ and $-u^{\frac{1}{1-n}}$ coincide, and for even n we have $(-u)^{\frac{1}{1-n}} = -u^{\frac{1}{1-n}}$ (for a suitable branch of the root), eliminating t from (14) yields

$$u^{\frac{1}{1-n}} + v^{\frac{1}{1-n}} = (-1)^{n-1}. \tag{15}$$

Let $m = n - 1$. Consider the algebraic element

$$\theta_1 = \left(u^{-\frac{1}{m}} + v^{-\frac{1}{m}}\right)^{-m}$$

of the extension

$$\mathbb{Q}(u, v) \subset \mathbb{Q}(\sqrt[m]{u},\ \sqrt[m]{v}).$$

Then the minimal polynomial of $\theta_1(u, v)$ is $(uvw)^m\, p_m(w^{-1}; u^{-1}, v^{-1})$, since the minimal polynomial of

$$\theta_2 = \left(u^{\frac{1}{m}} + v^{\frac{1}{m}}\right)^m$$

is $p_m(w; u, v)$ [BK25, Section 7]. Recalling that (15) defines the curve $X^\vee$ in the chart $w = 1$, we obtain the desired X_n-discriminant

$$\Delta_{X_n} = (uvw)^m\, p_m(w^{-1}; u^{-1}, v^{-1}).$$

□

Example 11. For X_2 we have

$$(u, v) = \left(-\frac{1}{1+t}, \frac{1}{t}\right) \quad \text{or} \quad \frac{1}{u} + \frac{1}{v} = -1.$$

Taking the projective closure (homogenization), we find that $X^\vee$ is given by

$$P_1 = uvw\, p_1(w^{-1}; u^{-1}, v^{-1}) = (u + v)w + uv = 0.$$

Example 12. For X_3:

$$(u, v) = \left(\frac{1}{(1+t)^2}, \frac{1}{t^2}\right) \quad \text{or} \quad \frac{1}{\sqrt{u}} + \frac{1}{\sqrt{v}} = 1.$$

The curve $X_3^\vee$ is given by

$$P_2 = (uvw)^2 p_2(w^{-1}; u^{-1}, v^{-1}) = (uv - w(u+v))^2 - 4uvw^2 = 0,$$

i.e.

$$P_2 = (uv)^2 + (vw)^2 + (uw)^2 - 2u^2vw - 2uv^2w - 2uvw^2.$$

In [GKZ94, Chapter 1, Example 2.3], for the family of Fermat curves (for integers $n \geq 2$)

$$F_n = \{x^n + y^n = z^n\} \tag{16}$$

it is shown that for a given n the dual curve (in the chart $\{w = 1\}$) is given by

$$F_n^\vee = \left\{ u^{\frac{n}{n-1}} + v^{\frac{n}{n-1}} = 1 \right\}.$$

For $n = 3$ an explicit form is given:

$$u^6 + v^6 + w^6 - 2u^3v^3 - 2u^3w^3 - 2v^3w^3 = 0.$$

From the proof of Proposition 4 we obtain:

Theorem 1. Let F_n be the Fermat curve (16), $n \geq 2$. Then the dual curve is given by the equation $\{F_n^\vee(u, v, w) = 0\}$, where

$$F_n^\vee(u, v, w) = p_{n-1}(w^n; u^n, v^n).$$

Note that the polynomials can be realized as the determinants of generalized Wendt's matrices [BK25, Theorem 4].

We now show that projective duality between X_n and $X_n^\vee$ yields a shift operator in a certain family of n-valued algebraic monoids $\mathbb{M}_n(\mathbb{C}P^1)$.

Theorem 2. 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 $x \in \mathbb{C}P^1 \backslash \{\infty\}$, and the value $\infty * \infty$ is undefined. In homogeneous coordinates the multiplication

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

is given by

$$(x_1 : x_0) * (y_1 : y_0) = (b_n : b_1 : \cdots : b_0), \tag{17}$$

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 $(1 : 0)$.

Proof. View the n-valued law $p_n(z; (-1)^n x, (-1)^n y)$ on $\mathbb{C}$ as the expression of the desired law on $\mathbb{C}P^1$ in the chart $z = 1$:

$$\begin{gathered} \mu :\ \mathbb{C}P^1 \times \mathbb{C}P^1 \to \mathrm{Sym}^n(\mathbb{C}P^1) \\ (x, y) = ((x_1 : x_0), (y_1 : y_0)) \mapsto [(w_1 : 1), \ldots, (w_n : 1)], \end{gathered}$$

where $w_1, \ldots, w_n$ are the roots in the variable z of the polynomial $p(z; x, y)$. Identify $\mathrm{Sym}^n(\mathbb{C}P^1)$ with $\mathbb{C}P^n$ via the isomorphism

$$\begin{gathered} \varphi :\ \mathrm{Sym}^n(\mathbb{C}P^1) \longrightarrow \mathbb{C}P^n \cong G(1, n, 2) \\ \boldsymbol{u} = [(u_{11} : u_{10}), \ldots, (u_{n1} : u_{n0})] \longmapsto \big(z_1 u_{10} - z_0 u_{11}\big) \cdots \big(z_1 u_{n0} - z_0 u_{n1}\big) = \varphi(\boldsymbol{u})(z_1 : z_0), \end{gathered} \tag{18}$$

under which the point $\boldsymbol{u}$ of the symmetric power goes to the homogeneous form $\varphi(\boldsymbol{u})(z_1 : z_0)$, a product of n linear forms

$$\ell_j(z_1 : z_0) = z_1 u_{j1} - z_0 u_{j0},$$

i.e. to a point of the Chow variety $G(1, n, 2)$. Then by Vieta's formulas the composition $\varphi \circ \mu$ yields the desired law (17).

It is easy to see that

$$b_n = (x_1 y_0 + (-1)^{n+1} x_0 y_1)^n,$$

each b_j is divisible by $(x_0 y_0)^j$ for $j = 1, \ldots, n$, and $b_0 = (x_0 y_0)^n$. Hence the multiplication (17) is defined for all pairs $(x, y) \in \mathbb{C}P^1 \times \mathbb{C}P^1$ except $(\infty, \infty) = ((1 : 0), (1 : 0))$. Moreover, the element ∞ has no inverse.

Associativity of the resulting operation is obvious. $\square$

Theorem 3. Under projective duality the curve X_n $(n \geq 2)$ goes to

$$X_n^\vee = \{\ (uvw)^{n-1} p_{n-1}(1/w; 1/u, 1/v) = 0\ \} \subset (\mathbb{C}P^2)^*.$$

The composition of the duality $X_n \mapsto X_n^\vee$ with the subsequent Möbius transformation $(u, v, w) \mapsto (1/u, 1/v, 1/w)$ defines a shift operation $\mathbb{M}_n(\mathbb{C}P^1) \mapsto \mathbb{M}_{n-1}(\mathbb{C}P^1)$ in the family of algebraic n-valued monoids.

Proof. Follows from Proposition 4. $\square$

The next fact was first obtained in [GRS24, Theorem 2.3]. A direct proof was given in the recent work [BK25]. We present another proof using the theory of projective duality, which clarifies the nature of this result.

Proposition 5 [GRS24]**.** The discriminant $\Delta_t(P)$ of the polynomial

$$P(t) = (zt^{n-1} + y)(1 + t)^{n-1} + (-1)^{n-1}xt^{n-1}$$

with respect to the variable t, which is a polynomial of degree $4n - 6$, is related to $p_n(z; x, y)$ by

$$(-1)^n(n-1)^{2n-2}(xyz)^{n-2}\, p_n(z; x, y) = \Delta_t(P)$$

for each $n \geq 2$.

Proof. Consider the curve $X_n^\vee$. We already know it is parametrized by (14). Then, by the definition of the $X_n^\vee$-discriminant, the curve $X_n^{\vee\vee}$ is an irreducible component of the discriminant of the polynomial obtained by restricting the line (12) to $X_n^\vee$, i.e. in the chart $\{w = 1\}$ the curve $X_n^{\vee\vee}$ is the discriminant in t of

$$\frac{1}{(-1-t)^{n-1}} \cdot x + \frac{1}{t^{n-1}} \cdot y + 1 = 0. \tag{19}$$

Taking the projective closure of the polynomial in the left-hand side of (19) yields $p_n(z; x, y)$ up to a constant factor. It is easy to see that if $xyz = 0$, then for $n \geq 2$ the polynomial $P(t)$ has a multiple root, hence $\Delta_t(P) = 0$. This means that $\Delta_t(P)$ is divisible by a certain power of the monomial xyz. By [GRS24, Theorem 2.2], $\Delta_t(P)$ has no other singular components. The required statement now follows by comparing degrees. $\square$

In connection with Bessel kernels for solutions of Picard–Fuchs differential equations for the kernel

$$K_n = \sum_{j,k} \binom{j+k}{k} \frac{x^j y^k}{z^{j+k}},$$

the iterated analogue of the polynomials $p_n(z; x, y)$ was considered in [GRS24]:

$$p_{n,m}(z; \boldsymbol{x}) = \prod_{k_1,\dots,k_m=1}^{n} \left(\sqrt[n]{z} + \varepsilon^{k_1}\sqrt[n]{x_1} + \cdots + \varepsilon^{k_m}\sqrt[n]{x_m}\right). \tag{20}$$

The polynomial $p_{n,m}(z; x)$ defines an m-ary n^{m-1}-valued algebraic operation

$$\mu(x_1, \dots, x_m) = [z \mid p_{n,m}(z; x) = 0].$$

Denote by $\mathcal{O}_{n,m}(\mathbb{C}P^1)$ the variety $\mathbb{C}P^1$ with the operation μ.

Let

$$X_{n,m} = \{\, p_{n,m} = 0 \,\}$$

be the hypersurface in $\mathbb{C}P^m$. For integers $n \geq 2$ and $m \geq 2$ define

$$P_{n,m} = (u_1 \cdots u_m w)^{n-1} p_{n-1}(w^{-1}; u_1^{-1}, \ldots, u_m^{-1}).$$

By the same technique as in Theorem 3 we obtain the following.

Theorem 4. The composition of the duality ($m \geq 2$, $n \geq 2$)

$$X_{n,m} \mapsto X_{n,m}^{\vee} = \{P_{n,m} = 0\} \subset (\mathbb{C}P^m)^*$$

with the subsequent Möbius transformation

$$(u_1, \ldots, u_m, w) \mapsto (1/u_1, \ldots, 1/u_m, 1/w)$$

defines a shift operation

$$\mathcal{O}_{n,m}(\mathbb{C}P^1) \mapsto \mathcal{O}_{n-1,m}(\mathbb{C}P^1)$$

in the family of m-ary n^{m-1}-valued algebraic structures $\mathcal{O}_{n,m}(\mathbb{C}P^1)$.

This result clarifies the statement of [GRS24, Theorem 3.2] concerning the relationship between the polynomial $p_{n,m}(z; \boldsymbol{x})$ and the discriminant of the homogeneous polynomial

$$P(\boldsymbol{u}) = (u_1 \cdots u_m)^{n-1} \left(z + (-1)^n \left(\sum_{j=1}^{m} u_j \right)^{n-1} \cdot \sum_{j=1}^{m} \frac{x_j}{u_j^{n-1}} \right),$$

taken with respect to the variables $u_1, \ldots, u_m$ in the sense of [GKZ94, Chapter 13].

The observation from Theorem 1 has an iterated analog.

Theorem 5. Let $F_{n,m}$ be a Fermat hypersurface

$$F_{n,m} = \{x_1^n + x_2^n + ... + x_m^n = z^n\}$$

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

$$F_n^{\vee} = \{p_{n-1,m}(w^n; u_1^n, ..., u_m^n) = 0\} \tag{21}$$

in $(\mathbb{C}P^m)^*$ with the dual coordinates $u_1, ..., u_m, w$, where $p_{n,m}$ denotes the polynomial (20).

In [GKZ94, Example 4.16], it was noticed that the dual hypersurface can be defined by

$$u_1^{\frac{n}{n-1}} + \dots + u_m^{\frac{n}{n-1}} = z^{\frac{n}{n-1}}$$

and that the irrational equation can be replaced by a polynomial equation of degree $n(n-1)^{m-1}$. Theorem 5 clarifies this observation giving the concrete realization (21) of the polynomial equation. The determinant expression for (21) when $n = 2$ and $m = 3$, one can find in [BK25, Example 9].

Fermat hypersurfaces play an important role in various problems of algebraic topology and algebraic geometry. Their topology has been studied in various works. For example, each Fermat hypersurface $F_{2,m}$ is diffeomorphic to the homogeneous space $SO(m+1)/(SO(2) \times SO(m-1))$ of oriented planes in $\mathbb{R}^{m+1}$ [KN69, Chapter XI, Example 10.6].

4 The Laws $p_n(z; x, y)$ and Discriminants of Field Extensions

To formulate the next proposition we need a definition first introduced for algebraic number fields by Dedekind [Ded71, Seite 429]. We give a general version following [Sut16, Lecture 12, Definition 12.5]:

Definition 10. Let R be a commutative ring with unit, and let $R \subset S$ be a finite extension such that S is a free R-module. For any elements $e_1, \dots, e_n \in S$ their *discriminant* is

$$\Delta(e_1, \dots, e_n) = \det\big(\mathrm{Tr}_{S/R}(e_i e_j)\big)_{ij},$$

where $\mathrm{Tr}(-)$ denotes the trace of the R-linear map $S \to S$ given by multiplication by $e_i e_j$.

In the case of interest, Definition 10 reduces to the classical definition of the discriminant of a polynomial.

Lemma 1 (Lecture 12, Proposition 12.6 [Sut16])**.** Let $K \subset L$ be a finite separable extension of degree n, let Ω be a normal closure of L (over K), and let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings $L \to \Omega$ over K. Then:

(i) For any elements $e_1, \dots, e_n \in L$ one has

$$\Delta(e_1, \dots, e_n) = \det(\sigma_i(e_j))_{ij}^2.$$

(ii) For any $x \in L$ one has

$$\Delta(1, x, \dots, x^{n-1}) = \prod_{i<j} \big(\sigma_i(x) - \sigma_j(x)\big)^2.$$

Under the basis change $\boldsymbol{e}' = \boldsymbol{e}C$, $C \in \mathrm{Mat}_K(n)$, the discriminant changes by

$$\Delta_{L/K}(\boldsymbol{e}') = \det(C)^2\, \Delta_{L/K}(\boldsymbol{e}).$$

In the case where K is the field of fractions of a Dedekind domain A, L/K is a finite separable extension, and B is the integral closure of A in L, this allows one to define the discriminant $\Delta_{L/K}$ of the extension L/K as the fractional ideal generated by the set

$$\{\Delta(\boldsymbol{e}) \mid \boldsymbol{e} \text{ is an } A\text{-basis of the } A\text{-module } B\}.$$

In our case the ring $\mathbb{Q}[x, y]$ is not Dedekind.

Proposition 6. For each integer $n \geq 2$, the discriminant of the polynomial $p_n(z; x, y)$ with respect to the variable z coincides with the discriminant $\Delta(1, \theta, \ldots, \theta^{n-1})$ for the extension $\mathbb{Q}(x, y) \subset \mathbb{Q}(\theta)$, where $\theta = (\sqrt[n]{x} + \sqrt[n]{y})^n$.

Proof. Indeed, as already noted, $p_n(z; x, y)$ is the minimal polynomial of $\theta = (\sqrt[n]{x} + \sqrt[n]{y})^n$. □

5 Cubics and n-Valued Coset Addition Laws

This section describes the polynomials that define all possible (up to isomorphism) coset addition laws in algebraic n-valued monoids and groups on $\mathbb{C}P^1$ modeled by cubic curves. We introduce and recall some definitions and constructions.

Let

$$\delta_{\boldsymbol{a}} = \Delta_t\big(t^3 + a_1 t^2 + a_2 t + a_3\big)$$

be the discriminant with respect to t. Then

$$\delta_{\boldsymbol{a}} = -4a_3 a_1^3 + a_2^2 a_1^2 + 18 a_2 a_3 a_1 - 4a_2^3 - 27a_3^2. \tag{22}$$

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

$$\mathcal{E} = \{\, y^2 = x^3 + a_1 x^2 + a_2 x + a_3 \,\}. \tag{23}$$

As an abelian variety over $\mathbb{C}$, a cubic admits only automorphisms of orders 2, 3, 4, and 6 [Har77, Corollary 4.7]. We consider in turn the cases of a nonsingular and a singular irreducible cubic $\mathcal{E}$ and the resulting structures of 2-, 3-, 4-, and 6-valued groups and monoids.

5.1 The Case of a Nonsingular Cubic

Assume the point $\boldsymbol{a} = (a_1, a_2, a_3)$ does not lie on the singular locus $\{\delta_{\boldsymbol{a}} = 0\}$. Let complex parameters α, g_2, g_3 be such that the curve $\mathcal{E}$ is rewritten as

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

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

$$\begin{cases} x_3 = -x_1 - x_2 - 3\alpha + \left(\dfrac{y_1 - y_2}{x_1 - x_2}\right)^2, \\ y_3 = (x_1 - x_3) \cdot \dfrac{y_1 - y_2}{x_1 - x_2} - y_1. \end{cases} \tag{24}$$

In the coincident case, (24) is understood via the limit as $x_2 \longrightarrow x_1$.

5.1.1 2-Valued Structures on $\mathbb{C}P^1$

There is a branched double covering

$$\pi : \mathcal{E} \longrightarrow \mathbb{C}P^1, \tag{25}$$

defined in the chart $\{z = 1\}$ by $\pi(x, y) = x$ and $\pi(\infty) = \infty$, with branch points at the roots of $x^3 + a_1x^2 + a_2x + a_3$ and at ∞. The fibers of π are in bijection with the points of the orbit space $\mathcal{E}/\langle\sigma\rangle$ for the involution

$$\begin{aligned} \sigma : (x, y) &\mapsto (x, -y), \\ \infty &\mapsto \infty \end{aligned} \tag{26}$$

Applying the coset construction [Buc06, Theorem 1] to the involution σ on the group of points of the elliptic curve, we obtain a structure $\mathcal{E}_{\langle\sigma\rangle}$ of a coset algebraic 2-valued group on $\mathbb{C}P^1$ with neutral element at ∞:

$$x_1 * x_2 = \left[-x_1 - x_2 - 3\alpha + \left(\frac{y_1 \pm y_2}{x_1 - x_2}\right)^2\right]. \tag{27}$$

Proposition 7. The values of (27) are the roots of a quadratic polynomial $D(z; x_1, x_2)$ in z:

$$D(z; x_1, x_2) = \Theta_0(x_1, x_2)\, z^2 + \Theta_1(x_1, x_2)\, z + \Theta_2(x_1, x_2), \tag{28}$$

where

$$\Theta_0 = 16(x_1 - x_2)^2,$$
$$\Theta_1 = 8\big(2g_3 + g_2(x_1 + x_2 + 2\alpha) - 4\big(x_1x_2(x_1 + x_2) + 6x_1x_2\alpha + 3(x_1 + x_2)\alpha^2 + 2\alpha^3\big)\big),$$
$$\begin{aligned}\Theta_2 = {} & \big(g_2 + 4x_1x_2\big)^2 + 16g_2(x_1 + x_2)\alpha + 24\big(g_2 - 4x_1x_2\big)\alpha^2 \\ & - 64(x_1 + x_2)\alpha^3 - 48\alpha^4 + 16g_3(x_1 + x_2 + 3\alpha).\end{aligned}$$

Proof. Direct computation via Vieta's formulas in any computer algebra system (e.g., `Wolfram Mathematica`). □

Theorem 6. The following statements hold:

(i) If $\delta_{\boldsymbol{a}} \neq 0$, the algebraic 2-valued group $\mathbb{G}_{\mathbb{C}P^1}(D_{\boldsymbol{a}}) \cong \mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ with identity ∞ is the regular coset group $\mathcal{E}_{\langle\sigma\rangle}$ for the group of points of the elliptic curve

$$\mathcal{E} = \{\, y^2 = x^3 + a_1x^2 + a_2x + a_3 \,\} \tag{29}$$

with respect to the involution $\sigma : (x, y) \mapsto (x, -y)$. In homogeneous coordinates, the group $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ on $\mathbb{C}P^1$ has zero $(0 : 1)$ and addition

$$\mu_{\boldsymbol{a}} :\ \mathbb{C}P^1 \times \mathbb{C}P^1 \longrightarrow \mathbb{C}P^2$$
$$(x_1 : x_0) * (y_1 : y_0) = (u_2 : u_1 : u_0)$$

with

$$\begin{cases} u_2 = (x_1y_0 - x_0y_1)^2, \\ -\frac{1}{2}u_1 = x_1x_0\big(2a_1y_1y_0 + a_2y_1^2 + y_0^2\big) + x_1^2y_1\big(a_2y_0 + 2a_3y_1\big) + x_0^2y_0y_1, \\ u_0 = x_1^2y_1\big(a_2^2y_1 - 4a_3(a_1y_1 + y_0)\big) - 2x_0x_1y_1\big(a_2y_0 + 2a_3y_1\big) + x_0^2y_0^2. \end{cases} \tag{30}$$

(ii) The isomorphism class of the coset algebraic 2-valued group $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ is completely determined by the j-invariant of the elliptic curve (29):

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

Proof. **(i)** Express α, g_2, g_3 from (5.1) and substitute into the formulas of Proposition 7. Using the isomorphism

$$\varphi :\ \mathrm{Sym}^2(\mathbb{C}P^1) \longrightarrow \mathbb{C}P^2$$
$$[(u_1 : u_0), (v_1 : v_0)] \mapsto (u_1v_1 :\ u_1v_0 + u_0v_1 :\ u_0v_0),$$

we obtain the homogeneous expression for the law $\nu_{\boldsymbol{a}}$ defined by the Kontsevich polynomial $D_{\boldsymbol{a}}(-x, -y, -z)$. From

$$B_{\boldsymbol{a}}(z; x, y) = (xyz)^2 D_{\boldsymbol{a}}(-1/z; -1/x, -1/y)$$

it follows that, after the Möbius transformation

$$x \mapsto 1/x,\ y \mapsto 1/y,\ z \mapsto 1/z,$$

we get the addition formulas $\mu_{\boldsymbol{a}} : \mathbb{C}P^1 \times \mathbb{C}P^1 \longrightarrow \mathbb{C}P^2$ in homogeneous coordinates with zero 0.

We show that $\mathrm{inv}(\infty) = \infty$ in $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ when $|a_2|^2 + |a_3|^2 \neq 0$. In $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ one has

$$(1:0) * (y_1 : y_0) = \big(y_0 :\ -2(2a_3y_1^2 + a_2y_0y_1) :\ a_2^2y_1^2 - 4a_1a_3y_1^2 - 4a_3y_0y_1\big).$$

For $(x_1 : x_0) * (y_1 : y_0) = \varphi^{-1}(u_2 : u_1 : u_0)$ to contain the point $(0:1)$, it is necessary and sufficient that $u_2 = 0$, hence $y_0 = 0$. Therefore

$$(1:0) * (1:0) = (0 :\ -4a_3 :\ a_2^2 - 4a_1a_3).$$

Thus $\mathrm{inv}(\infty)$ exists (and equals ∞) iff $|a_2|^2 + |a_3|^2 \neq 0$.

(ii) An isomorphism of 2-valued groups of the form $\mathbb{G}_{\mathbb{C}P^1}(D_{\boldsymbol{a}})$ consists of an automorphism of $\mathbb{C}P^1$ and an isomorphism $\psi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ of abelian varieties (see Definition 6). It is well known [Har77, Lemma 4.9] that any morphism ψ of elliptic curves preserving the marked points (neutral elements) is a group homomorphism. The claim then follows from the fact that the isomorphism class of an elliptic curve is determined by its j-invariant [Har77, Theorem 4.1].

□

Theorem 7. Let $\mathcal{E} = \{y^2 = f(x)\}$ be an elliptic curve, where $f(x) = x^3 + a_1x^2 + a_2x + a_3$. Then:

(i) The doubling elements of the 2-valued group $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}}(z; x, y))$ are precisely the elements of the form $1/w$, where w ranges over the branch points of the branched covering

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

(ii) The single-valued group of doubling points of the 2-valued group $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ is isomorphic to the Klein four-group $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Proof. **(i)** To find all doubling elements of $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}}(z;x,y))$, argue as in Example 6 and obtain

$$\Delta_z\big(B_{\boldsymbol{a}}(z;x,y)\big) = 16xy(a_3x^3 + a_2x^2 + a_1x + 1)(a_3y^3 + a_2y^2 + a_1y + 1) = 0 \tag{31}$$

for any $x \in \mathbb{C}$ and fixed $y \in \mathbb{C}$. From (31) it follows that either $y = 0$ or $f(1/y) = 0$—these y's are exactly the images of the branch points of the branched covering π.

(ii) We have seen that the order of the group $\mathbb{W}$ of doubling points equals 4. Since $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ is involutive, each nonzero element of $\mathbb{W}$ has order 2. Hence $\mathbb{W} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

□

From the classification of symmetric 2-algebraic 2-valued groups on $\mathbb{C}$ (see Definition 4 and Example 5), it follows that every 2-algebraic 2-valued group on $\mathbb{C}$ is defined by a polynomial $B_{\boldsymbol{a}}(z;x,y)$ whose discriminant factorizes with separated variables,

$$\Delta_z\big(B_{\boldsymbol{a}}(z;x,y)\big) = 16\,x^4 f(1/x) \;\cdot\; y^4 f(1/y),$$

cf. (31).

We note that an important first application of (31) was obtained by Dragović in [Dra10] (see also [Dra14]), based on a remarkable relation between the associativity equation for a 2-valued group on $\mathbb{C}$ and the integration method for the Kovalevskaya top.

The separation property in the discriminant factorization fails for the n-valued laws $p_n(z;x,y)$ (Example 7) already at $n = 3$. For instance,

$$\Delta_z\big(p_3(z;x,y)\big) = -3^9\,x^2(x-y)^2y^2.$$

5.1.2 3-Valued Structures on $\mathbb{C}P^1$

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]. Introduce the slope

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

Then the addition law for points (x_1,y_1) and (x_2,y_2) on the elliptic curve $\mathcal{E}$ takes the form

$$\begin{cases} x_3 = -x_1 - x_2 + m^2, \\ y_3 = m(x_1 - x_3) - y_1. \end{cases} \tag{32}$$

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,

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

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

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

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

Write the 3-valued law:

$$\begin{aligned}y_1 * y_2 &= [\,\pi\big((x_1, y_1) \oplus (\varepsilon^k x_2, y_2)\big) \mid k = 0, 1, 2\,]\\ &= \left[\, m_k\left(2\sqrt[3]{y_1^2 - c} + \varepsilon^k \sqrt[3]{y_2^2 - c} - m_k^2\right) - y_1 \,\right],\end{aligned} \tag{33}$$

where for each $k = 0, 1, 2$ we set

$$m_k = \frac{y_1 - y_2}{\sqrt[3]{y_1^2 - c} - \varepsilon^k \sqrt[3]{y_2^2 - c}}.$$

Theorem 8. On $\mathbb{C}P^1$, for each nonzero $c \in \mathbb{C}$ there exists a structure (which we call *equiharmonic*) of an algebraic 3-valued coset group $\mathbb{G}_{3,\mathrm{eqh}}(\mathbb{C}P^1)$ with neutral element 0, inversion map $\mathrm{inv}(x) = -x$, and addition given by the polynomial $p_{3,\mathrm{eqh}}(z; x, y)$, where

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

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

Proof. A direct computation using Vieta's formulas shows that $p_{3,\mathrm{eqh}}(z; x, y)$ has as its roots the elements of the multiset (33). $\square$

In [BK25, Theorem 2] all symmetric 3-algebraic 3-valued groups on $\mathbb{C}$ were classified. There are only two series of such groups: the groups $\mathbb{G}_{3,\mathrm{eqh}}(\mathbb{C}P^1)$ and the diagonal of a formal group G. The group G is defined by the Hirzebruch genus that assigns to an oriented manifold its signature.

Proposition 8. The set $\{0,\ \pm 1/\sqrt{c}\}$ of iterating elements of the 3-valued group $\mathbb{G}_{3,\mathrm{eqh}}(\mathbb{C}P^1)$ is (as a 3-valued subgroup) the diagonal construction of a 1-valued group isomorphic to $\mathbb{Z}/3$.

Proof. Let y be an iterating element in $\mathbb{G}_{3,\mathrm{eqh}}(\mathbb{C}P^1)$. Then for any $x \in \mathbb{C}$ the discriminant of the polynomial $p_{3,\mathrm{eqh}}(z; x, y)$ vanishes:

$$-3^9x^2y^2(cx^2-1)^2(cy^2-1)^2(x-y)^2\big(9c^2x^2y^2 - cx^2 + 8cxy - cy^2 + 1\big)^2 = 0.$$

Thus precisely the elements $0, \pm 1/\sqrt{c}$ are iterating. Let $w = 1/\sqrt{c}$. We have the multiplication table

$$\begin{aligned} w * w &= [-w, -w, -w], \\ -w * w &= w * (-w) = [0, 0, 0]. \end{aligned}$$

Hence the iterating elements acquire a group structure isomorphic to $\mathbb{Z}/3$. □

5.1.3 4-Valued Structures on $\mathbb{C}P^1$

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

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

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 the branched double covering

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

with branch points 0 and ∞.

Write the 4-valued addition law:

$$\begin{aligned} x_1 * x_2 &= \big[\, \pi_4\big((x_1, y_1),\ \varphi_4^r(x_2, y_2)\big) \mid r = 0, \ldots, 3 \,\big] \\ &= \left[\left(-\sqrt{x_1} - (-1)^\ell\sqrt{x_2} + m_{\ell,k}^2\right)^2 \,\middle|\, k, \ell = 0, 1 \right], \end{aligned} \tag{34}$$

where

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

Theorem 9. 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 $\mathbb{G}_{4,\mathrm{har}}(\mathbb{C}P^1)$ with neutral element 0, whose addition is given by the polynomial

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

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

Proposition 9. The iterating elements of the 4-valued group $\mathbb{G}_{4,\mathrm{har}}(\mathbb{C}P^1)$ form the set $\{0, -1/b\}$, which is not any 4-valued subgroup (nor even a submonoid).

Proof. Let y be an iterating element in $\mathbb{G}_{4,\mathrm{har}}(\mathbb{C}P^1)$. Then for any $x \in \mathbb{C}$ the discriminant of $p_{4,\mathrm{har}}(z; x, y)$ vanishes:

$$\begin{aligned} & x^3 y^3 (bx+1)^2 (by+1)^2 (x-y)^2 \left(b^2 xy - 1\right)^2 \left(b^2 x^2 + 4b^2 xy + 2bx + 1\right)^2 \\ & \quad \cdot \left(b^2 x^2 y + 2bxy + 4x + y\right)^2 \left(4b^2 xy + b^2 y^2 + 2by + 1\right)^2 \left(b^2 x y^2 + 2bxy + x + 4y\right)^2 = 0. \end{aligned}$$

Hence precisely 0 and $-1/b$ are iterating elements of $\mathbb{G}_{4,\mathrm{har}}(\mathbb{C}P^1)$. Since

$$p_{4,\mathrm{har}}(z; -1/b, -1/b) = 256\, z^2/b^2,$$

the product $(-1/b) * (-1/b)$ is not defined in the 4-valued group $\mathbb{G}_{4,\mathrm{har}}(\mathbb{C}P^1)$. □

5.1.4 6-Valued Structures on $\mathbb{C}P^1$

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

$$\begin{aligned} \varphi_6 : \mathcal{E} & \to \mathcal{E} \\ (x, y) & \mapsto (\varepsilon x, -y), \\ \infty & \mapsto \infty. \end{aligned}$$

It is easy to see that 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 projection

$$\begin{aligned} \pi_6 : \mathcal{E} &\to \mathbb{C}P^1 \\ (x, y) &\mapsto y^2, \\ \infty &\mapsto \infty. \end{aligned}$$

Write the 6-valued addition law:

$$\begin{aligned} y_1 * y_2 &= [\pi_6((x_1, y_1), \varphi_6^r(x_2, y_2)) \mid r = 0, \ldots, 5] \\ &= \left[\left(m_{\ell,k} \left(2\sqrt[3]{y_1 - c} + \varepsilon^k \sqrt[3]{y_2 - c} - m_{\ell,k}^2 \right) - \sqrt{y_1} \right)^2 \mid k = 0, 1, 2; \ell = 0, 1 \right], \end{aligned} \tag{35}$$

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 10. On $\mathbb{C}P^1$, for each nonzero $c \in \mathbb{C}$ there exists a structure (which we call *equiharmonic*) of an involutive 6-valued algebraic coset group $\mathbb{G}_{6,\mathrm{eqh}}(\mathbb{C}P^1)$ with neutral element 0 and addition given by the polynomial $p_{6,\mathrm{eqh}}(z; x, y)$, for which

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

and e_k is the k-th elementary symmetric function. All such 6-valued groups are isomorphic.

Proposition 10. The set $\{0, 1/c\}$ of iterating elements of the 6-valued group $\mathbb{G}_{6,\mathrm{eqh}}(\mathbb{C}P^1)$ is not any 6-valued subgroup (nor even a submonoid).

Proof. Let y be an iterating element in $\mathbb{G}_{6,\mathrm{eqh}}(\mathbb{C}P^1)$. Then for any $x \in \mathbb{C}$ the discriminant of the polynomial $p_{6,\mathrm{eqh}}(z; x, y)$ vanishes:

$$x^5y^5(cx-1)^4(cy-1)^4(x-y)^4\left(27c^2x^3+81c^2x^2y-54cx^2-18cxy+27x+y\right)^4\ldots$$

From this it follows that the elements $0, 1/c$, and only they, are iterating. Since

$$p_{6,\mathrm{eqh}}(z; 1/c, 1/c) = 2^{18}z^3(cz+1)^3/c^3,$$

we have:

$$1/c * 1/c = [0, 0, 0, -1/c, -1/c, -1/c]\,.$$

Because the element $-1/c$ is not iterating, the set $0, 1/c$ is not any 6-valued submonoid of the group $\mathbb{G}_{6,\mathrm{eqh}}(\mathbb{C}P^1)$. $\square$

5.2 Nodal Case

We now turn to singular cubics.

Example 13. The change of variables

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

shows that the algebraic 2-valued monoid $\mathbb{M}_{\mathrm{mult}}(\mathbb{C}P^1)$ from Example 6 is isomorphic to the monoid $\mathbb{G}_{\mathbb{C}P^1}(B_{\boldsymbol{a}})$ with $a_1 = 1, a_2 = a_3 = 0$. This monoid corresponds to the cubic $\{y^2 = x^2(x+1)\}$.

Let $\boldsymbol{a}$ be such that the polynomial

$$P(x) = x^3 + a_1x^2 + a_2x + a_3 \tag{36}$$

has a double root. In this case the equation of the curve $\mathcal{E}$ takes the form ($\alpha \neq \beta$):

$$\mathcal{E} = \{y^2 = (x-\alpha)^2(x-\beta)\}. \tag{37}$$

Parametrize $\mathcal{E}$ by the slope m of the line passing through the node $\mathcal{O} = (\alpha, 0)$:

$$\begin{cases} x = m^2 + \beta, \\ y = m\left(m^2 + \beta - \alpha\right). \end{cases}$$

As before, there is a branched double covering

$$\begin{aligned} \mathcal{E} &\to \mathbb{C}P^1 \\ (x(m), y(m)) &\mapsto x(m), \\ \infty &\mapsto \infty. \end{aligned}$$

with branch points at α, β, and ∞.

Lemma 2. Let $m_1 \oplus m_2 = -m_3$ for points $m_1, m_2, m_3 \in \mathbb{C}P^1$ on the curve $\mathcal{E}$ with respect to the above parametrization. Then

$$m_3 = \frac{m_1 m_2 - m_+ m_-}{m_1 + m_2}, \tag{38}$$

where $m_\pm = \pm\sqrt{\alpha - \beta}$ and $[m_1, m_2] \neq [m_+, m_-]$.

Proof. The points (x_1, y_1), (x_2, y_2) and $(x_3, -y_3)$ on the curve $\mathcal{E}$ with slopes $m_j = y_j/(x_j - \alpha)$ (where $x_j \neq \alpha$ and $j = 1, 2, 3$), such that $m_1 \oplus m_2 = -m_3$, lie on one line, hence

$$\det\begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} = 0.$$

Therefore

$$(m_1 - m_2)(m_2 - m_3)(m_1 - m_3)(m_1 m_2 - m_2 m_3 - m_1 m_3 - m_+ m_-) = 0.$$

If $m_1 \neq m_2$, the claim follows immediately, since in this case the points m_j are pairwise distinct (otherwise m_1 or m_2 would be singular). For the case $m_1 = m_2$, the value of m_3 is given by the same formula (38) by continuity. □

Proposition 11. The Möbius transformation

$$m \mapsto \frac{m + m_-}{m + m_+} \tag{39}$$

establishes an isomorphism of 1-valued algebraic monoids $\mathcal{E} \cong M_{\mathrm{mult}}(\mathbb{C}P^1)$.

Proof. Let $m_1 \oplus m_2 = -m_3$. It suffices to prove the identity

$$\frac{m_1 + m_-}{m_1 + m+} \cdot \frac{m_2 + m_-}{m_2 + m+} \cdot \frac{-m_3 + m_-}{-m_3 + m+} = 1. \tag{40}$$

Consider the polynomial

$$Q(x) = (x + m_1)(x + m_2)(x - m_3).$$

Let $a = m_+ = -m_-$. By Vieta's formulas and by Lemma 2 we have

$$Q(x) = x^3 + (m_1 + m_2 - m_3)x^2 - a^2 x - m_1 m_2 m_3.$$

We see that $Q(a) = Q(-a)$, therefore we obtain the desired identity (40). $\square$

Example 14. Consider the involution ι on the monoid $\mathcal{E}(\mathbb{C})$ such that $\iota : m \mapsto -m$ for $m \in \mathbb{C}$ and $\iota(\infty) = \infty$. By Lemma 13, this is an automorphism. Then the orbit space $\mathbb{C}P^1/\langle\iota\rangle$ is identified with $\mathbb{C}P^1$ via the map

$$\begin{aligned} \psi : \mathbb{C}P^1 &\to \mathbb{C}P^1 \\ z &\mapsto z^2. \end{aligned}$$

The monoid $\mathbb{C}P^1$ together with the involution ι gives a coset 2-valued algebraic monoid $\mathbb{M}_{\mathrm{node}}(\mathbb{C}P^1) = \mathcal{E}_{\langle\iota\rangle}$ with operation

$$m_1 * m_2 = \left[\left(\frac{\sqrt{m_1}\sqrt{m_2} \pm a}{\sqrt{m_1} \pm \sqrt{m_2}}\right)^2\right] \tag{41}$$

defined on the set $\mathrm{Sym}^2(\mathbb{C}P^1)\backslash[a, a]$, where $a = \alpha - \beta$. The values $m_1 * m_2$ are the roots of the quadratic trinomial

$$(m_1 - m_2)^2 z^2 - 2\left(a^2(m_1 + m_2) - 4a m_1 m_2 + m_1 m_2(m_1 + m_2)\right) z + (a^2 - m_1 m_2)^2.$$

Writing the addition law (41) in the original coordinates (x, y) of the curve $\mathcal{E}$, we obtain the algebraic law

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

The values $x_1 * x_2$ are the roots (in z) of the symmetric polynomial $D_{\alpha,\beta}(-z; -x_1, -x_2) = (x_1 x_2 z)^2 B_{\alpha,\beta}(1/z; 1/x_1, 1/x_2)$, where

$$\begin{aligned} B_{\alpha,\beta}(z; x_1, x_2) = {} & \left((\alpha^2 x_1 x_2 - 1)^2 - 4\alpha\beta x_1 x_2(\alpha x_1 - 1)(\alpha x_2 - 1)\right) z^2 \\ & - 2\left(-2\beta x_1 x_2(\alpha x_1 - 1)(\alpha x_2 - 1) + \alpha x_1 x_2(\alpha(x_1 + x_2) - 4) + x_1 + x_2\right) z \\ & + (x_1 - x_2)^2. \end{aligned}$$

In elementary symmetric functions:

$$B_{\alpha,\beta}(z; x_1, x_2) = \quad e_1^2 + e_1 e_3\left(-2\alpha^2 - 4\alpha\beta\right) + 4\alpha^2\beta e_2 e_3 - 4e_2 + e_3^2\left(\alpha^4 - 4\alpha^3\beta\right) + e_3(8\alpha + 4\beta).$$

By Vieta's formulas, the polynomial $B_{\alpha,\beta}(z; x_1, x_2)$ coincides with the Buchstaber polynomial $B_{\boldsymbol{a}}(z; x_1, x_2)$ for

$$\begin{cases} a_1 = -2\alpha - \beta, \\ a_2 = \alpha^2 + 2\alpha\beta, \\ a_3 = -\alpha^2\beta \end{cases}$$

In other words, the polynomial $D_{\alpha,\beta}(-z; -x_1, -x_2)$ is the Kontsevich polynomial $D_{\boldsymbol{a}}(-z; -x_1, -x_2)$ with parameters lying on the singular divisor $\{\delta_{\boldsymbol{a}} = 0\}$. From the projective classification of singular cubics it follows that in the nodal case (37) there is, up to isomorphism, only one monoid $\mathbb{M}_{\text{node}}(\mathbb{C}P^1)$.

Recall that every irreducible nodal cubic in $\mathbb{C}P^2$ is projectively equivalent to the cubic $y^2 z = x^2(x + z)$ [FW69, Exercise 5-24]. We formulate the main result of this section, which follows from all of the above:

Theorem 11. Let α and β be distinct complex numbers, and let $\mathcal{E}$ be the singular cubic given in the affine chart $\{z = 1\} \subset \mathbb{C}P^2$ by

$$y^2 = (x - \alpha)^2(x - \beta).$$

Then the addition of points on $\mathcal{E}$ and the involution

$$\begin{aligned} \sigma : (x, y) &\mapsto (x, -y), \\ \infty &\mapsto \infty \end{aligned} \tag{42}$$

define on $\mathbb{C}P^1$ a unique (independent of the parameters α and β, up to isomorphism) structure of a 2-valued coset algebraic monoid $\mathbb{M}_{\text{node}}(\mathbb{C}P^1)$ 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 polynomial $D_{\alpha,\beta}(-z; -x_1, -x_2)$ from Example 14. The element α is absorbing, i.e., $x * \alpha = \alpha * x = \alpha$ for any $x \in \mathbb{C}P^1 \setminus \{\alpha\}$. The product $\alpha * \alpha$ is not defined. Moreover, the element 0 has an inverse ($\mathrm{inv}(0) = 0$, $0 * 0 = \left[\alpha(1 - \alpha/(4\beta)), \infty\right]$) if and only if $\alpha \neq 0$.

Proposition 12. The set of doubling points for $\mathbb{M}_{\text{node}}(\mathbb{C}P^1)$ consists of three points: ∞, α, and β.

5.3 Cuspidal Case

Finally, consider the case of a triple root

$$\mathcal{E} = \{y^2 = (x - \alpha)^3\}.$$

Introduce the parametrization by the slope $m = y/(x-\alpha)$ of the line passing through its cusp. Then Lemma 2 (in the limit $\beta \to \alpha$) immediately yields:

Lemma 3. The addition law on the elliptic curve $\mathcal{E} = \{y^2 = (x-\alpha)^3\}$ has the form:

$$m_3 = \frac{m_1 m_2}{m_1 + m_2}. \tag{43}$$

We obtain the following easily.

Proposition 13. The Möbius transformation $m \mapsto 1/m$ establishes an isomorphism between the 1-valued algebraic monoids $\mathcal{E}(\mathbb{C}) \cong M_{\mathrm{cusp}}(\mathbb{C}P^1)$ (see Example 2).

Example 15. The set $\mathbb{M}_{\mathrm{node}}(\mathbb{C}P^1)$ from Example 14 tends, as $\alpha \to \beta$, to the monoid $\mathbb{M}_{\mathrm{cusp}}(\mathbb{C}P^1)$ with identity ∞ and multiplication

$$x_1 * x_2 = \left[\frac{(x_1-\alpha)(x_2-\alpha)}{(\sqrt{x_1-\alpha} \pm \sqrt{x_2-\alpha})^2} + \alpha \right]. \tag{44}$$

Thus, the coset monoid $\mathcal{E}_{\langle\sigma\rangle} = \mathbb{M}_{\mathrm{cusp}}(\mathbb{C}P^1)$ on $\mathbb{C}P^1$, constructed from the curve $\mathcal{E}$ and the involution (42), in this case has neutral element ∞, absorbing element 0, and the addition law (44).

Proposition 14. The monoids $\mathbb{M}_{\mathrm{cusp}}(\mathbb{C}P^1)$ and $\mathbb{M}_2(\mathbb{C}P^1)$ are isomorphic.

Proof. The map

$$x \mapsto \frac{1}{x-\alpha}$$

defines an isomorphism $\mathbb{M}_{\mathrm{cusp}}(\mathbb{C}P^1) \to \mathbb{M}_2(\mathbb{C}P^1)$. □

Recall that every irreducible cuspidal cubic in $\mathbb{C}P^2$ is projectively equivalent to the cubic $\{y^2 z = x^3\}$ [FW69, Exercise 5-24].

Theorem 12. Let $\alpha \in \mathbb{C}$ and let $\mathcal{E}$ be the singular cubic given in the affine chart $z = 1 \subset \mathbb{C}P^2$ by

$$\mathcal{E} = \{y^2 = (x-\alpha)^3\}.$$

Then the following statements hold:

(i) The addition of points on $\mathcal{E}$ and the involution (42) define on $\mathbb{C}P^1$ a unique (independent of the parameter α, up to isomorphism) structure of a 2-valued coset algebraic monoid $\mathbb{M}_2(\mathbb{C}P^1)$.

(ii) The group from Theorem 8 tends, as $c \to 0$, to the monoid $\mathbb{M}_3(\mathbb{C}P^1)$.

(iii) The group from Theorem 9 tends, as $b \to 0$, to the monoid $\mathbb{M}_4(\mathbb{C}P^1)$.

(iv) The group from Theorem 10 tends, as $c \to 0$, to the monoid $\mathbb{M}_6(\mathbb{C}P^1)$.

Proposition 15. The set of doubling points for $\mathbb{M}_{\mathrm{cusp}}(\mathbb{C}P^1)$ consists of two points: ∞ and α.

References

[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

[BK25] Buchstaber V., Kornev M. n-Valued Groups, Kronecker Sums, and Wendt's Matrices. arXiv:2505.04296. https://doi.org/10.48550/arXiv.2505.04296

[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

[Ded71] Dedekind R. (editor). *Vorlesungen über Zahlentheorie von P.G. Lejeune Dirichlet*. Druck und Verlag von Friedrich Vieweg und Sohn, Braunschweig, umgearbeitete und vermehrte auflage edition (1871)

[Dol12] Dolgachev I.V. *Classical Algebraic Geometry: A Modern View*. Cambridge University Press (2012). https://doi.org/10.1017/CBO9781139084437

[Dra10] Dragović V. Generalization and Geometrization of the Kowalevski Top. Communications in Math. Phys., 298(1) (2010) 37–64. https://doi.org/10.1007/s00220-010-1066-z

[Dra14] Dragović V. Discriminantly Separable Polynomials and Quad-Equations. Journal of Geometric Mechanics, 6(3) (2014) 319–333. https://doi.org/10.3934/jgm.2014.6.319

[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

[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

[GRS24] Gaiur I., Rubtsov V., Straten D. Product Formulas for the Higher Bessel functions. arXiv:2405.03015. https://arxiv.org/abs/2405.03015

[Har77] Hartshorne R. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, NY (1977). https://doi.org/10.1007/978-1-4757-3849-0

[KN69] Kobayashi S., Nomizu K. *Foundations of Differential Geometry*, volume 2. Interscience Publishers, reprinted by Wiley Classics Library (1996) edition (1969)

[Sut16] Sutherland A. An MIT course: Number theory I (2016). https://math.mit.edu/classes/18.785/2016fa/lectures.html

Victor Buchstaber
Steklov Mathematical Institute of Russian Academy of Sciences
Email: buchstab@mi-ras.ru

Mikhail Kornev
Steklov Mathematical Institute of Russian Academy of Sciences
Email: mkorneff@mi-ras.ru