Algebraic n-valued groups, Kronecker sums and (x, y, z)-Wendt matrices

Victor M. Buchstaber

Steklov Mathematical Institute of Russian Academy of Sciences
Steklov International Mathematical Center, Moscow

The 6-th International Conference
"Groups and quandles in low-dimensional topology"
Regional Scientific and Educational Mathematical Center, TSU
Tomsk, June 10–11, 2025

In various areas of research, there arises a natural operation on a space, say X, in which the product (addition) of a pair of points is a subset of X.

The literature on multivalued groups and their applications is extensive and includes works starting from the 19th century, mostly in the context of the hypergroup concept.

In 1971, S.P. Novikov and the author introduced a construction, suggested by the theory of characteristic classes of vector bundles, in which the product of each pair of points is an n-multiset, i.e. an unordered set of n points, possibly with repetitions.

This construction led to the notion of an n-valued group.

The n-valued groups

The author gave an axiomatic definition of n-valued formal groups (n-f groups) and developed their theory in a series of papers.

Theorem (V.M. Buchstaber, 1976)

The 2-f group in complex cobordisms is universal in the class of 2-f groups over torsion-free rings, provided that $\mathrm{inv}(x) = x$.

This result led to the solutions to problems in algebraic topology and stimulated the development of the algebraic theory of n-valued groups.

At present, a number of authors have obtained results on the theory of n-valued groups (formal, finite, discrete, topological, algebraical, algebraic-geometrical) with applications in various fields of mathematics and mathematical physics.

The focus of the talk will be on the structure of algebraic n-valued groups and the connection of their theory with matrix algebra and classical results motivated by Fermat's Last Theorem.

The symmetric power of a space

Denote n-th symmetric power of a space X by $(X)^n$, i.e. $(X)^n = X^n/\Sigma_n$, where the symmetric group Σ_n acts by permuting the factors.

We will consider a point in $(X)^n$ as a subset of X with n points (possibly with repetitions), i.e. as an n-multiset.

Example. The spaces $(\mathbb{C})^n = \mathbb{C}^n/\Sigma_n$ and $\mathbb{C}^n$ can be identified using the mapping

$$\mathcal{S} : \mathbb{C}^n \to \mathbb{C}^n : \ (z_1, z_2, \ldots, z_n) \to e_r(z_1, z_2, \ldots, z_n), \ 1 \leqslant r \leqslant n,$$

where e_r is r-th elementary symmetric polynomial.

The projectivization of the mapping $\mathcal{S}$ induces a homeomorphism $(\mathbb{CP}^1)^n \to \mathbb{CP}^n$.

The n-valued groups

The n-valued multiplication (addition) on X is given by the mapping

$$\mu : X \times X \to (X)^n \ : \ \mu(x,y) = x * y = [z_1, \dots, z_n], \ z_k = (x*y)_k.$$

Neutral element. The point $e \in X$ such that

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

Inverse element. The mapping $\mathrm{inv}\colon X \to X$ such that

$$e \in \mathrm{inv}(x) * x \ \text{ and } \ e \in x * \mathrm{inv}(x) \ \text{ for any } \ x \in X.$$

Associativity. The n^2-sets

$$[x * (y*z)_1, x * (y*z)_2, \dots, x * (y*z)_n],$$
$$[(x*y)_1 * z, (x*y)_2 * z, \dots, (x*y)_n * z]$$

coincide for everyone $x, y, z \in X$.

Commutativity. The n-sets $x * y$ and $y * x$ coincide for everyone $x, y \in X$.

The mapping μ defines the structure of an n-valued group on X if it is associative and there exist e and inv.

The $(n, 1)$-valued rings

Definition

An $(n, 1)$-valued ring is a set X with operations

$$\mu : X \times X \to (X)^n : \mu(x, y) = x * y \quad \text{and} \quad \xi : X \times X \to X : \xi(x, y) = x \cdot y$$

such that μ defines on X the structure of an n-valued commutative group, and ξ defines the structure of an 1-valued semigroup with the condition of two-sided distributivity:

Set $x * y = [z_1, \ldots, z_n]$.
Then, for any x, y and u in X,

$$(x * y) \cdot u = [z_1 \cdot u, \ldots, z_n \cdot u] = (x \cdot u) * (y \cdot u),$$

$$u \cdot (x * y) = [u \cdot z_1, \ldots, u \cdot z_n] = (u \cdot x) * (u \cdot y).$$

The 2-valued group and the $(2,1)$-ring on $\mathbb{Z}_+$

Let us consider non-negative integers $\mathbb{Z}_+$, which are a semigroup on addition. Let us introduce the 2-valued commutative addition on $\mathbb{Z}_+$ by

$$\mu\colon \mathbb{Z}_+ \times \mathbb{Z}_+ \to (\mathbb{Z}_+)^2 \ : \ x * y = [x+y, |x-y|].$$

Neutral element: $e = 0$.

Inverse element: $\mathrm{inv}(x) = x$.

Associativity: 4-sets

$$(x * y) * z = [x+y+z, |x-y-z|, x+|y-z|, |x-|y-z||]$$

and

$$x * (y * z) = [x+y+z, |x+y-z|, |x-y|+z, ||x-y|-z|]$$

coincide for any $x, y, z \in \mathbb{Z}_+$.

The 2-valued group $\mathbb{Z}_+$ with the usual multiplication of numbers "$\cdot$" is a $(2,1)$-ring.

Constructions of the n-valued groups

For any $m \in \mathbb{N}$, the n-valued group X with the operation μ_n can be considered as an mn-valued group with the operation

$$\mu_n^m : X \times X \xrightarrow{\mu_n} (X)^n \xrightarrow{(D)^m} (X)^{mn}, \quad \text{where } D \text{ is diagonal.}$$

Definition

A mapping $f : X \to Y$ is called a homomorphism of n-valued groups if

$$f(e_X) = e_Y, \ f(\mathrm{inv}_X(x)) = \mathrm{inv}_Y(f(x)) \ \text{ for everyone } \ x \in X,$$

$$\text{and } \ \mu_Y(f(x), f(y)) = (f)^n \mu_X(x, y) \ \text{ for everyone } \ x, y \in X.$$

Definition

An n-valued group X is called reducible if there exists an isomorphism $f : X \to Y$, where Y is an n-valued group with the operation $\mu_n = \mu_k^m$, $n = mk$.

The coset groups

Let G be some (1-valued) group with multiplication μ_1, neutral element e_G, and inverse mapping $\mathrm{inv}_G(u) = u^{-1}$.

Let A, $|A| = n$, be some finite subgroup of the automorphism group $Aut\ G$.

Consider the orbit space $X = G/A$ of the group G under the action of the group A and the quotient mapping $\pi\colon G \to X$.

Let us define an n-valued multiplication

$$\mu\colon X \times X \to (X)^n \ :\ \mu(x,y) = [\pi(\mu_0(u, v^a)),\ a \in A],$$

where $u \in \pi^{-1}(x)$, $v \in \pi^{-1}(y)$, and v^a is the image of the action of an element $a \in A$ on $v \in G$.

Theorem

The multiplication μ defines on $X = G/A$ the structure of an n-valued coset group (G, A) with a neutral element $e_X = \pi(e_G)$ and a uniquely defined mapping $\mathrm{inv}(x) = \pi(u^{-1})$, where $\pi(u) = x$.

Algebraic n-valued groups

Definition

An algebraic n-valued group is an algebraic variety X with an n-valued operation μ that is defined on some dense subset $Y \subset X \times X$ in the Zariski topology and satisfies the axioms in n-valued groups.

The theory of algebraic n-valued groups and its connection with the theory of integrable dynamical systems of discrete time was developed in the works of V.M. Buchstaber and A.P. Veselov.

Set

$$P(z; x, y) = \sum_{k=0}^{n} F_k(x, y) z^{n-k}, \tag{1}$$

where $F_k(x, y) \in \mathbb{C}[x, y]$ and

$$F_0(0, 0) = 1. \tag{2}$$

This defines an operation $*$, that assigns to $x, y \in \mathbb{C}$ the multiset $x * y$ of roots of the polynomial (1) in the variable z.

Consequents from the axioms

From the axiom of the neutral element $x = 0$,

$$P(z; 0, y) = F_0(0, y)(z - y)^n. \tag{3}$$

The inverse element axiom states that there exists an algebraic mapping $\mathrm{inv} : \mathbb{C} \to \mathbb{C}$ such that, for any $x \in \mathbb{C}$,

$$F_n(x, \mathrm{inv}(x)) = F_n(\mathrm{inv}(x), x) = 0. \tag{4}$$

Let us introduce an algebraic function $z(x, y) = [z_1(x, y), \ldots, z_n(x, y)]$, where $z_j = z_j(x, y)$, $j = 1, \ldots, n$, are the roots of the polynomial P.

In terms of the theory of extensions of algebraic function fields, the associativity condition is written as the identical equality of two polynomials in the variable t:

$$\prod_{i,j=1}^{n} (t - z_i(z_j(x, y), z)) = \prod_{i,j=1}^{n} (t - z_i(x, z_j(y, z))). \tag{5}$$

Associativity equation

Set $R_k(x,y) = \frac{F_k(x,y)}{F_0(x,y)}$.

Note that

$$\prod_{i,j=1}^{n}(t - z_i(z_j(x,y),z)) = \prod_{j=1}^{n}\left(t^n + \sum_{k=1}^{n} R_k(z_j(x,y),z)t^{n-k}\right).$$

Corollary

The coefficients of the polynomials in t in the associativity equation (5),

$$\prod_{j=1}^{n}\left(t^n + \sum_{k=1}^{n} R_k(z_j(x,y),z)t^{n-k}\right) = \prod_{j=1}^{n}\left(t^n + \sum_{k=1}^{n} R_k(x,z_j(y,z))t^{n-k}\right),$$

are rational functions of the variables x, y, and z.

The universal n-valued algebraic group

Set $\mathcal{R}_n = \mathbb{C}[a_{i,j,k} \,:\, 0 \leqslant i,j \leqslant n_k,\ 0 \leqslant k \leqslant n]$. Consider a polynomial

$$\Pi_n(z;x,y) = \sum_{k=0}^{n} \mathcal{F}_k(x,y) z^{n-k}, \quad \text{где } \mathcal{F}_k(x,y) = \sum a_{i,j,k} x^i y^j \in \mathcal{R}_n[x,y].$$

Proposition

In the ring $\mathcal{R}_n$, there exists the uniquely defined ideal $\mathcal{J}_n$ such that the polynomial

$$\Pi_n^*(z;x,y) = \sum_{k=0}^{n} \mathcal{F}_k^*(x,y) z^k$$

defines a universal commutative n-valued algebraic group over the ring $\mathcal{U}_n = \mathcal{R}_n/\mathcal{J}_n$, where $\mathcal{F}_k^*(x,y) = \sum a_{i,j,k}^* x^i y^j \in \mathcal{U}_n[x,y]$, $a_{i,j,k}^* = \pi(a_{i,j,k})$, and $\pi : \mathcal{R}_n \to \mathcal{U}_n$ is a canonical projection.

By definition, for any n-valued algebraic group with the polynomial $P(z;x,y) = \sum_{k=0}^{n} F_k(x,y) z^{n-k}$ over any commutative $\mathbb{C}$-algebra K, there exists a uniquely defined ring homomorphism $\varphi : \mathcal{U}_n \to K$ such that $\varphi^*(\Pi_n^*(z;x,y)) = P(z;x,y)$, i.e. $F_k(x,y) = \sum \varphi(a_{i,j,k}^*) x^i y^j$.

The n-algebraic n-valued groups

Definition

An n-algebraic n-valued group on $\mathbb{C}$ is the algebraic n-valued group with multiplication

$$* : (\mathbb{C} \times \mathbb{C}) \backslash \{(x, y) \mid F_0(x, y) = 0\} \longrightarrow \mathrm{Sym}^n(\mathbb{C}) \ ,$$

$$(x, y) \longmapsto [z_1, ..., z_n]$$

where z_j are the roots of the polynovial (1) such that each of the variables x and y is included in it to a degree not exceeding n, and this polynomial satisfies conditions (2), (3), (4) и (5).

We will denote this group by $\mathbb{G}(P)$.

Definition

The n-algebraic n-valued group is called symmetric if the polynomial $P(z; (-1)^n x, (-1)^n y)$ is symmetric in x, y, z.

Symmetric 1-algebraic 1-valued groups

From the condition $F_0(0,0) = 1$, an n-algebraic n-valued group on $\mathbb{C}$ is a formal n-valued group on $\mathbb{C}$ since the operation μ is defined in a neighborhood of $0 \in \mathbb{C}$.

It is defined on the whole $\mathbb{C}$ if and only if $F_0(x,y) \equiv 1$.

Proposition

The universal symmetric 1-algebraic 1-valued group $\mathbb{G}(\Pi_1)$ is defined over $\mathbb{C}[\alpha]$ and is given by the polynomial

$$\Pi_1(z;x,y) = (1+\alpha xy)z - x - y.$$

It is isomorphic to the algebraic 1-valued group of matrices of the form $\begin{pmatrix} 1 & x \\ \alpha x & 1 \end{pmatrix}$ up to multiplication by non-zero complex numbers, since

$$\begin{pmatrix} 1 & x \\ \alpha x & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ \alpha y & 1 \end{pmatrix} = (1+\alpha xy) \begin{pmatrix} 1 & \frac{x+y}{1+\alpha xy} \\ \alpha \frac{x+y}{1+\alpha xy} & 1 \end{pmatrix}.$$

Symmetric 2-algebraic 2-valued groups

Theorem (V.M. Buchstaber, M.I. Kornev, 2025)

The universal symmetric 2-algebraic 2-valued group $\mathbb{G}(\Pi_2^*)$ is defined over the coefficient ring

$$\mathbb{C}[k_2, k_4, k_6, k_8]/(4k_8 - k_4^2 + k_6 k_2) \cong \mathbb{C}[k_2, k_4, k_6],$$

and is given by the symmetric polynomial

$$\Pi_2^*(z; x, y) = e_1^2 - 4e_2 + [2k_2 + 2k_4 e_1 + 2k_6 e_2 + (k_4^2 - k_6 k_2)e_3]e_3.$$

A proof of this theorem was obtained according to the definition of a universal family using the computer algebra system Wolfram Mathematica.

This result was first obtained by V.M. Buchstaber and A.P. Veselov as a corollary of the two-valued formal groups classification.

Symmetric 3-algebraic 3-valued groups

Theorem (V.M. Buchstaber, M.I. Kornev, 2025)

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

1. $\Pi_3^{*,1}(z;-x,-y) = e_1^3 - 27e_3$. In this case, we get a 3-valued group $\mathbb{G}_3$.
2. $\Pi_3^{*,2}(z;-x,-y) = (e_1 + \alpha e_3)^3$. In this case, the corresponding 3-valued group is obtained by the diagonal construction

$$G \times G \xrightarrow{\mu} G \xrightarrow{\mathrm{Sym}^3 \circ \mathrm{diag}} \mathrm{Sym}^3(\mathrm{G})$$

from the universal symmetric 1-algebraic 1-valued group $G(\Pi_1)$, constructed using the polynomial

$\Pi_1^*(z;-x,-y) = (1+\alpha xy)z + x + y = e_1 + \alpha e_3$.

This new result was obtained according to the definition of a universal family using the computer algebra system Wolfram Mathematica.

n-valued groups $\mathbb{G}_n$ on $\mathbb{C}$

Set $\varepsilon = \exp\frac{2\pi i}{n}$. Using the automorphism $z \to \varepsilon z$, we introduce the n-valued coset addition

$$\mu\colon \mathbb{C}\times\mathbb{C} \to (\mathbb{C})^n \ : \ x * y = [z_1, \dots, z_n],\ z_k = (\sqrt[n]{x} + \varepsilon^k \sqrt[n]{y}\,)^n.$$

Neutral element: $e = 0$. Inverse element: $\mathrm{inv}(x) = (-1)^n x$.

We obtain commutative algebraic n-valued groups $\mathbb{G}_n$ with the law $p_n(z; x, y) = 0$, where

$$p_n(z; x, y) = (z - z_1)\cdots(z - z_n)$$

are polynomials with integer coefficients. The first polynomials are

$$\begin{aligned}
p_1 =& z - x - y,\\
p_2 =& (z + x + y)^2 - 4(xy + yz + zx),\\
p_3 =& (z - x - y)^3 - 27xyz,\\
p_4 =& ((z + y + x)^2 - 4(xy + yz + zx))^2 - 2^7(z + y + x)xyz.
\end{aligned}$$

The polynomial $p_n(z; (-1)^n x, (-1)^n y)$ is symmetric with respect to x, y, z. More over, it is homogeneous.

Polynomials $P_n(e_1, e_2, e_3)$ and prime numbers

Set $P_n(e_1, e_2, e_3) = p_n(z; (-1)^n x, (-1)^n y)$, where e_1, e_2, e_3 are elementary symmetric polynomials.

$$P_5 = e_1^5 - 5^4 e_3(e_1^2 - 5e_2),$$

$$P_6 = e_1^6 - 2^2 \cdot 3\, e_1^4 e_2 - 2 \cdot 3^4 \cdot 17\, e_1^3 e_3 + 2^4 \cdot 3\, e_1^2 e_2^2 - \\ - 2^3 \cdot 3^4 \cdot 19\, e_1 e_2 e_3 - 2^6 e_2^3 + 3^3 \cdot 19^3\, e_3^2,$$

$$P_7 = e_1^7 - 7^4 e_3 \left(5e_1^4 - 2 \cdot 7^2 e_1^2 e_2 - 7^4 e_1 e_3 + 7^3 e_2^2\right),$$

$$P_{11} = e_1^{11} - 11^4 e_3 \Big[5 \cdot 53\, e_1^8 - 2 \cdot 11^2 \cdot 197\, e_1^6 e_2 - 11^3 \cdot 61 \cdot 1499\, e_1^5 e_3 + \\ + 2 \cdot 11^4 \cdot 41\, e_1^4 e_2^2 - 11^5 \cdot 17 \cdot 2957\, e_1^3 e_2 e_3 - 11^6\ e_1^2 (5e_2^3 - 2 \cdot 67^3\, e_3^2) - \\ - 2^2 \cdot 7 \cdot 11^7 \cdot 67\, e_1 e_2^2 e_3 + 11^7 (e_2^4 - 67^3\, e_2 e_3^2)\Big].$$

Match to the number n a set of primes that occur as divisors of the coefficients of the polynomials $P_n(e_1, e_2, e_3)$.

Question:

What patterns are revealed as a result of this matching?

Groups G_n and polynomials $p_n(z; x, y)$

Groups G_n and the polynomials $p_n(z; x, y)$ arise and play an important role in various areas of mathematics and mathematical physics.

In the paper of V.M. Buchstaber and A.N. Kholodov, 1989, the polynomials $p_n(z; x, y)$ describe the shifts T_x^y on homogeneous coalgebras with eigenfunctions $b_n(\lambda x)$, which are hypergeometric. Here

$$T_x^y : Q[[x]] \to Q[[x, y]], \quad T_x^y b_n(x) = b_n(x) b_n(y),$$

$$b_n(x) = {}_0F_{n-1}\left(\frac{1}{n}, \ldots, \frac{n-1}{n}; \frac{(n-1)!}{n^{n-1}} x\right).$$

We get:

$$b_1(x) = e^x, \; b_2(x) = ch(\sqrt{2x}),$$

where $ch(x)$ is hyperbolic cosine.

In the paper of I. Gaiur, V. Rubtsov, and D. van Straten, 2024, the authors described the relationship between the polynomials $p_n(z; x, y)$ and multiplicative kernels in the sense of Kontsevich, Bessel kernels and potentials in the Landau–Ginzburg model.

The Kronecker sums

Definition

Let A and B be arbitrary square matrices over the field $\mathbb{C}$ of orders m and n, respectively, and let I_n, I_m be the identity matrices.
The Kronecker sum $A \boxplus B$ of matrices A and B is the $(mn \times mn)$-matrix

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

Kronecker sums are important in various problems of the theory of differential equations, quantum computing, machine learning, and robotics.

They are used in studies of matrix equations (Riccati, Lyapunov, Sylvester) and matrix difference operators on grids.

In terms of the Kronecker sum, one can formulate:

the criterion for the existence and uniqueness of a solution to a matrix equation $AX + XB = C$,

and the Rauth–Hurwitz stability criterion to determine whether all roots of the characteristic polynomial of a linear system have negative real parts.

Eigenvalues of the matrices and the Kronecker sums

Consider the multisets $[\lambda_1, \ldots, \lambda_m]$ and $[\mu_1, \ldots, \mu_n]$ of eigenvalues of the matrices A and B.

Proposition (C. Stephanos, 1900)

Set $p(x, y) = \sum_{j,k=0}^{\ell} c_{jk} x^j y^k \in \mathbb{C}[x, y]$. Then

$$[p(\lambda_r, \mu_s),\ r = 1, \ldots, m,\ s = 1, \ldots, n]$$

is the multiset of eigenvalues of the matrix

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

Corollary

$[\lambda_r + \mu_s,\ r = 1, \ldots, m,\ s = 1, \ldots, n]$ is the multiset of eigenvalues of the Kronecker sum $A \boxplus B$.

The Frobenius accompanying matrices

Definition

The matrix

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

is called the Frobenius accompanying matrix $F(a_{n-1}, \ldots, a_0)$ of the polynomial $f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in \mathbb{C}[t]$.

The Frobenius accompanying block matrix $F(A_{n-1}, \ldots, A_0)$ of the matrix polynomial

$$f(t) = t^n + A_{n-1}t^{n-1} + \ldots + A_0 \in \mathrm{Mat}_m(\mathbb{C})[t].$$

is defined similarly.

The Frobenius matrices and the Kronecker sums

Let us introduce the characteristic polynomial $\chi(t; A)$ of the $(n \times n)$-matrix A

$$\chi(t; A) = det(tI_n - A),$$

where I_n is the identity $(n \times n)$-matrix.

The multiset of roots of the polynomial $\chi(t; A)$ coincides with the multiset of eigenvalues of the matrix A.

Set $f(t) = t^m + a_{m-1}t^{m-1} + \ldots + a_0$. Then $\chi(t; F(a_{m-1}, \ldots, a_0)) = f(t)$.

Proposition

Let $[\lambda_j]$ and $[\mu_k]$ be the multisets of roots of the polynomials

$$f(t) = t^m + a_{m-1}t^{m-1} + \ldots + a_0 \quad \text{и} \quad g(t) = t^n + b_{n-1}t^{n-1} + \ldots + b_0.$$

Then $[\lambda_j + \mu_k]$ is the multiset of roots of the characteristic polynomial of degree mn

$$\chi(t; F(a_{m-1}, \ldots, a_0) \boxplus F(b_{n-1}, \ldots, b_0)).$$

Groups $\mathbb{G}_n$, polynomials $p_n(z; x, y)$, and the Kronecker sums

Proposition (V.M. Buchstaber, M.I. Kornev, 2025)

(1) For x, y, z and for $t^n = z$, the following equality holds:

$$p_n(z; x, y) = \chi\big(t; F(\underbrace{0, \dots, 0, -x}_{n}) \boxplus F(\underbrace{0, \dots, 0, -y}_{n})\big).$$

(2) The polynomial $p_n(z; (-1)^n x, (-1)^n y)$ is symmetric in the variables x, y and z.

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

The Wendt theorem

Definition

The Wendt matrix W_n is the circulant of the polynomial $(1+x)^n - x^n$

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

Theorem (E. Wendt, 1894)

Let $p > 3$ be a prime, and let $q = 2kp + 1$ be a prime for some $k \geqslant 1$.
Then there exist integers a, b, c, not divisible by q, such that

$$a^p + b^p + c^p \equiv 0 \mod q$$

if and only if q is a divisor of $\det W_{2k}$.

n-admissible prime numbers

Theorem (J. Dirichlet, 1837)

Let m and n be natural coprime numbers.
There exists an infinite set of prime numbers q in the arithmetic progression $m + kn$.

Definition

A prime number q is called n-admissible if and only if the equation $x^n = 1$ has n solutions in the ring of q-adic integers $\mathbb{Z}_q$.

Every prime number q is 2-admissible.

Proposition

A prime number $q > n$ is n-admissible if and only if it belongs to the arithmetic progression $1 + kn$.

q-adic n-valued groups

Denote by $\mathcal{X}_q^n \subset \mathbb{Z}_q$ the image of the mapping $\mathbb{Z}_q \to \mathbb{Z}_q : a \to x = a^n$.

Corollary

For every n-admissible prime $q > n$, the set $\mathcal{X}_q^n$ is an $(n,1)$-ring
with n-valued coset addition given by an automorphism $\varepsilon : \mathbb{Z}_q \to \mathbb{Z}_q : a \to \varepsilon a$ of the n-th order, where $\varepsilon^n = 1$,
and with a 1-valued multiplication in $\mathcal{X}_q^n$ given by the usual multiplication in $\mathbb{Z}_q$.

Example. $n = 3,\ q = 7,\ \varepsilon \in \mathbb{Z}_7$, where $\varepsilon^3 = 1$ and $\varepsilon \equiv 2 \mod 7$.

Addition in a (3,1)-valued ring $\mathcal{X}_7^3 \subset \mathbb{Z}_7$:

$x * y = [z_1, z_2, z_3]$, where $x = a^3,\ y = b^3,\ z_k = c_k^3$ and $c_k = a + \varepsilon^k b \in \mathbb{Z}_7$,
$k = 1, 2, 3$.

Matrices $W_n(z; x, y)$

Definition

The Toeplitz matrix

$$\mathrm{Circ}_y(a_0, ..., a_{n-1}) = \begin{pmatrix} a_0 & ya_1 & ya_2 & \cdots & ya_{n-1} \\ a_{n-1} & a_0 & ya_1 & \ddots & \vdots \\ a_{n-2} & a_{n-1} & a_0 & \ddots & ya_2 \\ \vdots & \ddots & \ddots & \ddots & ya_1 \\ a_1 & \cdots & a_{n-2} & a_{n-1} & a_0 \end{pmatrix}$$

is called a y-circulant $\mathrm{Circ}_y(a_0, ..., a_{n-1})$.

Definition (V.M. Buchstaber, M.I. Kornev, 2025)

An y-circulant such that

$$a_0 = w^n + (-1)^{n+1}x + y, \quad a_k = \binom{n}{k} w^k, \quad k = 1, \ldots, n-1, \quad w^n = z$$

is called a matrix $W_n(z; x, y)$.

Groups $\mathbb{G}_n$ and the Wendt matrices W_n

Set $w = t$.

Theorem (*) (V.M. Buchstaber, M.I. Kornev, 2025)

(1) The polynomial $p_n(z; x, y)$, which defines addition in the n-valued group $\mathbb{G}_n$, is the determinant of the matrix $W_n(z; x, y)$.

(2) $W_n(1; (-1)^n x, 1) = W_n - tI_n$, where $t = x - 1$ and W_n is the Wendt matrix.

Corollary

$$\chi(t, W_n) = p_n(x; (-1)^n, (-1)^n), \text{ where } t = (-1)^n x - 1,$$

$$W_n = W_n(1; (-1)^n, 1),$$

$$\det W_n = p_n\left((-1)^n; (-1)^n, (-1)^n\right).$$

Examples

Set $p_n = p_n(z; (-1)^n x, (-1)^n y)$ and $z = w^n$.

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

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

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

Addition in $\mathbb{G}_n$ and characteristic polynomials

Proposition (V.M. Buchstaber, M.I. Kornev, 2025)

1. $(-1)^n * (-1)^n$ is the multiset of roots of the characteristic polynomial $\chi(t, W_n)$, where $t = (-1)^n x - 1$.
2. $1 * 1$ is the multiset of roots of the characteristic polynomial $\chi(t, \widetilde{W}_n)$, where $\widetilde{W}_n$ is the $(-1)^n$-circulant and $t = x + (-1)^{n+1}$.
3. $1 * (-1)^n$ is the multiset of roots of the characteristic polynomial $\chi(t, W_n)$, where $t = x - 1$.

Application of the Wolstenholme Theorem

Theorem (V.M. Buchstaber, M.I. Kornev, 2025)

For any prime $n \geqslant 5$, the polynomial

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

is divisible by n^4xyz.

The proof is based on our theorem (*) and the classical result:

Theorem (J. Wolstenholme, 1862)

The number

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

is divisible by n^3 for any prime $n \geqslant 5$.

Expansion in powers of e_1

Theorem (V.M. Buchstaber, M.I. Kornev, 2025)

For every prime number $n \geqslant 5$, there exists a function $\xi_n : [0, n-3] \to \mathbb{Z}$ such that $\xi_n(k) = 0,\ k = 0, 1;\ \xi_n(k) > 0,\ k > 1;\ \xi_n(n-3) = n-4,$ and

$$p_n(z; -x, -y) = p_n(e_1, e_2, e_3) = e_1^n - n^4 e_3 \left(\sum_{k=0}^{n-3} n^{\xi_n(k)} \pi_{n,k}(e_2, e_3) e_1^{n-k-3} \right),$$

where
$\pi_{n,k}(e_2, e_3) = \sum_{2i+3j=k} \alpha_{n,i,j} e_2^i e_3^j,\ i \geqslant 0,\ j \geqslant 0,\ \alpha_{n,i,j} \in \mathbb{Z},\ (\pi_{n,k}(e_2, e_3), n) = 1.$

Examples:

$$\xi_5 : [0, 2] \to (0, 0, 1);$$
$$\xi_7 : [0, 4] \to (0, 0, 2, 4, 3);$$
$$\xi_{11} : [0, 8] \to (0, 0, 2, 3, 4, 5, 6, 7, 7);$$
$$\xi_{13} : [0, 10] \to (0, 0, 2, 3, 4, 5, 6, 7, 8, 9, 9),$$

where $\pi_{13,9}(e_2, e_3) = \alpha_{13,3,1}\, e_2^3 e_3 + 13\alpha_{13,0,3} e_3^3,\ \ (\alpha_{13,3,1}, 13) = 1,\ (\alpha_{13,0,3}, 13) = 1.$

A Wolstenholme primes

Definition

A prime number n for which $\binom{2n-1}{n-1} - 1$ is divisible by n^4 is called a Wolstenholme prime.

Currently, only two Wolstenholme primes are known: $16\,843$ and $2\,124\,679$. The next Wolstenholme prime, if it exists, must be greater than 10^{11}.

The Wolstenholme Theorem and the Catalan numbers

Definition

The numbers $C_n = \frac{2n!}{n!(n+1)!}$ are called the Catalan numbers (1838).

$\{C_n\} = \{1, 2, 5, 14, 42, 132, 429, \ldots\}$ is one of the most famous sequences of enumerative combinatorics.

For example, the number C_n is equal to:

- the amount of triangulations of a convex $(n+2)$-gon;
- the amount of vertices of the associahedron (Stasheff polyhedron) $As^{n-1} \subset \mathbb{R}^{n-1}$.

Using the Wolstenholme Theorem, we obtain:

Proposition

The number $(n+1)C_n - 2$ is divisible by n^3 when $n > 3$ is a prime number, and it is divisible by n^4 when n is the Wolstenholme prime.

Problem. Find a realization of this Proposition in terms of the combinatorics of the Stasheff polyhedra.

References


V.M.Buchstaber, S.P.Novikov,
Formal groups, power systems and Adams operators.
Math. USSR Sbornik, 13:1 (1971), 80–116.


V.M.Buchstaber,
Two-valued formal groups. Algebraic theory and applications to cobordism, I-II.
Math. USSR-Izv., 39:5, 1975, 987–1006; 10:2, 1976, 271–308.


V.M.Buchstaber, A.N.Kholodov,
Groups of formal diffeomorphisms of the superline, generating functions
for polynomial sequences, and functional equations.
Math. USSR-Izv., 35:2, 1990, 277–305.


V.M.Buchstaber, A.P.Veselov,
Integrable correspondences and algebraic representations of multivalued groups.
Internat. Math. Res. Notices, N 8, 1996, 381–400.


V.M.Buchstaber,
n-valued groups: theory and applications.
Moscow Math. J., 6:1, 2006, 57–84.

References


P.Lancaster, M.Tismenetsky,
The Theory of Matrices: With Applications.
Computer Science and Scientific Computing. Elsevier Science, 1985.


P.Ribenboim,
Fermat's Last Theorem for Amateurs.
Springer New York, NY, 1st edition, 1999.


H.D.Ursell,
The degrees of radical extensions.
Canadian Mathematical Bulletin, 17(4) (1974), 615–617.


E.Wendt,
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, 1894, 335–347.


J.Wolstenholme,
On certain properties of prime numbers.
The Quarterly Journal of Pure and Applied Mathematics, 5 (1862), 35–39.

References


V.M.Buchstaber, A.P.Veselov,
Conway topograph, $PGL_2(\mathbb{Z})$-dynamics and two-valued groups.
Russian Math. Surveys, 74:3(447), 2019, 387–430.


V.M.Buchstaber, A.A.Gaifullin, A.P.Veselov,
Classification of involutive commutative two-valued groups.
Russian Math. Surveys, 77:4 (2022), 651–727


V.M.Buchstaber, E.Yu.Vesnin,
n-valued groups, branched covering and three-dimensional hyperbolic manifolds.
Sb. Math., 215:11 (2024), 1441–1467.


I.Gaiur, V.Rubtsov, D.van Straten,
Product formulas for the Higher Bessel functions.
arXiv:2405.03015v1 [math.AG] 5 May 2024.


Victor Buchstaber, Mikhail Kornev,
n-Valued Groups, Kronecker Sums, and Wendt's (x, y, z)-Matrices.
arXiv:2505.04296v1 [math.GR] 7 May 2025.

Thank You for your attention!