Един метод за научно изследване в математиката

ПРОФ. Д-Р НИКОЛА ЗЯПКОВ

Шуменски Университет "Епископ К. Преславски"

Нека A е едно непразно множество. Всяко биективно изображение на A в себе си наричаме преобразуване на множеството A.

Нека G е множеството на всички преобразувания на A. Ако $\varphi \in G$, то обратното изображение φ^{-1} също е биективно изображение. Композицията на две преобразувания на A също е преобразуване на A и тази композиция е асоциативна.

Следователно множеството G е група, която наричаме група от преобразувания на A.

Ръководен принцип в съвременната математика е следният: Когато имаме едно множество, то трябва да се определи неговата група от преобразувания. Изучаването на тази група е мощен метод за научно изследване и получаване на важни резултати в математиката. Голяма роля играят подгрупите на G, които оставят неподвижни някои от елементите на A.

В случая, която A е една алгебрична структура (група, пръстен, поле, векторно пространство и т.н.), то G е групата от автоморфизми на тази структура и бележим $\mathrm{Aut}(A) = G$.

Един от първите математици, който прилага този метод е гениалният френски математик Еварист Галоа (1811-1832). Той намира критерий за разрешимост в радикали на общото уравнение $f(x) = 0$. Този критерий Галоа намира, като използва гениалната идея на всяко уравнение да съпостави група от субституции на корените на уравнението. Чрез използването на тази група, нейни подгрупи и свързаните с тях радикални разширения на полето от коефициенти той намира критерий за разрешимост на едно уравнение в радикали [1].

Тази група наричаме група на Галоа на даденото уравнение и я означаваме с $\mathrm{Gal}(f)$. Е. Галоа доказва, че общото уравнение $f(x) = 0$ е решимо в радикали тогава и само тогава, когато $\mathrm{Gal}(f)$ е разрешима група.

Горният пример може да бъде обобщен и за полета K с произволна характеристика (виж. например [2]).

Групата на Галоа на общото уравнение от n-та степен е изоморфна на S_n (симетричната група). Тъй като S_n е неразрешима при $n \geq 5$, то от този критерий веднага следва теоремата на Абел-Руфини за нерешимост в радикали на общото уравнение от степен $n \geq 5$.

Определение 1. Крайното разширение E на полето K наричаме нормално разширение (раз. на Галоа) на полето K, ако K е неподвижно подполе на групата на G от $\mathrm{Aut}(E)$. Групата G е група на Галоа на норм. разш. E на K, бележим $\mathrm{Gal}(E/K)$.

Теорема 2 (Основна теорема в теорията на Галоа [2]). Нека E е нормално разширение на полето K с група на Галоа G. Съществува биективно изображение между подгрупите на G и междинните за E и K полета. За дадено междинно разширение F съответната подгрупа H на G съвпада с множеството от всички автоморфизми на E, които оставят неподвижни елементите на F. За дадена подгрупа H на G, съответното междинно поле се състои от онези елементи на E,

Следствие 3. Нека E е нормално разширение на полето K с група на Галоа G и C е междинно разширение на K, като $\mathrm{Gal}(E/C) = H$. Тогава C е нормално разширение на K тогава и само тогава, когато H е нормална подгрупа на G, като $\mathrm{Gal}(C/K) \cong G/H$.

Това означава, че е в сила точната редица

$$1 \to H \to G \to G/H \cong \mathrm{Gal}(C/K) \to 1. \tag{1}$$

От тук по естествен начин възниква и така наречената задача за вложимост на полета, която в известна степен е обратна теорема на Следствие 3. Нашата формулировка е следната: Нека K е разширение на Галоа на полето k и $\mathrm{Gal}(K/k) = F$ и е дадена точната редица от крайни групи

$$1 \to H \to G \xrightarrow{\alpha} F = \mathrm{Gal}(K/k) \to 1. \tag{2}$$

Да решим задачата за вложимост $(K/k, G, \alpha)$ означава да построим полето L, съдържащо K и нормално над k, като $\mathrm{Gal}(L/k) = G$ и за всеки елемент $g \in G$ ограничението му върху K да съвпада с $\alpha(g)$.

Ако $F = \{\mathrm{id}\}$, то получаваме така наречената Обратна задача в теорията на Галоа: за дадено поле K и дадена крайна група G да се построи разширение на Галоа L на K с група на Галоа G.

Класическата обратна задача в теорията на Галоа е задачата, когато $K = \mathbb{Q}$. Въпросът дали всички крайни групи могат да се реализират като групи на Галоа над $\mathbb{Q}$ е един от най-предизвикателните проблеми в математиката, който все още не е решен.

Първото систематично изучаване на Обратната задача започва през 1892 г., когато Д. Хилберт установява следният резултат:

Теорема 4. За всяко $n \geq 1$ симетричната група S_n и алтернативната група A_n се реализират като групи на Галоа над $\mathbb{Q}$.

Следващият важен резултат е получен през 1937 г. от А. Шолц [3] и Х. Райнхард [4], които доказват следната теорема.

Теорема 5. За всяко нечетно просто число p, всяка крайна p-група се реализира като група на Галоа над $\mathbb{Q}$.

За полета от алгебрични числа и разрешими групи Обратната задача е решена от И. Р. Шафаревич през 1954 г. в цикъл от работите [5, 6, 7, 8], като е доказана.

Теорема 6. Всяка разрешима група може да се реализира като група на Галоа над поле от алгебрични числа.

Измежду простите групи, проективните групи $PSL(2, p)$ за някои нечетни прости числа p са първите реализирани като групи на Галоа.

Теорема 7 (Ших [9]). Нека p е нечетно просто число, такова че 2, 3 или 7 са квадратични неостатъци по модул p. Тогава $PSL(2,p)$ се реализира като група на Галоа над $\mathbb{Q}$.

Теорема 8 (Мале и Мацат [10]). Нека p е нечетно просто число и $p \neq \pm 1 (\mathrm{mod} 24)$. Тогава могат да бъдат построени семейства от полиноми над $\mathbb{Q}(t)$ с група на Галоа $PSL(2,p)$.

Измежду 26-те спорадични прости групи, всичките с изключение евентуално на една, а именно групата на Матьо M_{23} (нейният ред е $2^{18}.3^{13}.5^2.7.11.13.17.23$), са реализирани като група на Галоа над $\mathbb{Q}$ от Мацат и неговите сътрудници.

Групата на Фишер-Гриея известна като "чудовището" е най-голямата спорадична проста група. Нейният ред е:

$$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.59.71.$$

През 1984 г. Томсън успя да докаже следната теорема за съществуване.

Теорема 9 (Томсън [11]). Групата "чудовище"е група на Галоа над $\mathbb{Q}$.

По-късно някои семейства от прости линейни групи са реализира-ни като групи на Галоа над $\mathbb{Q}$.[12]

За още факти относно Обратната задача може да се обърнем към статията на Михайлов и Зяпков "Обратната задача в теорията на Галоа" [13].

Един от успешните подходи за решаването на Обратната задача е задачата за вложимост на полета. В общия случай за решение на задачата за вложимост се допуска алгебра на Галоа.

Определение 10. Асоциативната и комутативна крайномерна сепарабелна алгебра A над полето k ще наричаме S-алгебра.

Определение 11. S-алгебрата над полето k наричаме алгебра на Галоа с група на Галоа G, ако съществува хомоморфизъм на групата G в групата от автоморфизми над k на алгебрата A и A притежава G-нормален базис над k.

Определение 12. Когато решението на задачата за вложимост е поле, то такова решение се нарича собствено решение.

Едно необходимо (но не достатъчно) условие за решимост на задачата за вложимост $(K/k, G, \alpha)$ е намерено от Д. К. Фадеев [14] и Х. Хасе [15]. Това условие е условие за съгласуваност.

По-кратко доказателство на Теорема 6 дава през 1976 г. В. И. Ишханов [16]. Шафаревич в своето доказателство на Теорема 6 (обем 123 стр.) въвежда класове от полета, наречени шолцеви, а Ишханов въвежда класове от полета, наречени квазишолцеви. И вида полета се определят в аритметични термини.

През 1977 г. Н. П. Зяпков и А. В. Яковлев [17] въвеждат нов клас от полета – универсално съгласувани полета. Те се определят чисто алгебрично (в хомологични термини). Те доказват, че всяка група от нечетен ред е група на Галоа над полета от алгебрични числа. Доказателството е по-ясно и по-конкретно в сравнение с доказателствата на Шафаревич и Ишханов. Друго доказателство на този факт е направено от Нойкирх ([18,19]).

Определение 13. Казваме, че разширението на Галоа k/K с група на Галоа F е универсално съгласувано от период q, ако полето K съдържа примитивен корен на единицата ξ от степен q и за всяка подгрупа F_0 на F хомоморфизмът $H^2(F_0, \langle\xi\rangle) \to H^2(F_0, K^*)$, индуциран от влагането $\langle\xi\rangle \to K^*$ е нулев.

Теорема 14([17]). Разширението на Галоа K/k,съдържащо примитивен корен на единицата от степен q е универсално съгласувано от период q тогава и само тогава, когато условието за съгласуваност е изпълнено за всички задачи за вложимост $(K/k, G, \alpha)$ с абелово ядро от период q.

Условието на Теорема 14 е опростено чрез:

Теорема 15([17]). Нека K/k е разширение на Галоа с група на Галоа F, съдържащо примитивен корен на единицата от степен q. Нека $\varphi : S \to F$ е епиморфизъм на свободната група S върху F, $R = \mathrm{Ker}\varphi$, $G = S/[R,R]R^q$, α е епиморфизъм на G върху F, индуциран от φ. Разширението K/k е универсално съгласувано тогава и само тогава, когато условието за съгласуваност е изпълнено за задачата $(K/k, G, \alpha)$.

Определение 16. Разширението на Галоа K/k, несъдържащо корен p-ти на единицата (p–просто число) наричаме универсално съгласувано от период p^n, ако полето K_1, получено от K чрез присъединяване на корен p-ти на единицата, съдържа примитивен корен на единицата от степен p^n, е универсално съгласувано съгласно Определение 13.

Определение 17. Разширението на Галоа K/k, несъдържащо корени на единицата от степени $p_1, p_2, \ldots, p_m$ (p_i– различни прости числа) наричаме универсално съгласувано от период $p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$, ако е универсално съгласувано за всеки от периодите $p_1^{n_1}, p_2^{n_2}, \ldots, p_m^{n_m}$.

В [18] е доказана следната важна теорема:

Теорема 18. Нека $p_1, p_2, \ldots, p_m$ са различни нечетни прости числа, а числото $q = p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$, K/k е универсално съгласувано разширение от период q (съгласно Определение 17). Тогава за всяка задача за вложимост $(K/k, G, \alpha)$ с ядро група от ред делящ q (не непременно абелова) съществува решение, което е поле.

Тъй като ядрото на α е група от нечетен прост ред, то тази група е разрешима съгласно знаменитата теорема на Фейт и Томсън ([20]). Този факт се използва съществено при доказателството на теоремата.

Теорема 19([26]). За всяко нечетно число q съществува универсално съгласувано от период q разширение на Галоа K_q над полето на рационалните числа $\mathbb{Q}$ от нечетна степен.

От този резултат следва.

Теорема 20([18]). За всяка група G от нечетен ред съществува разширение на Галоа на поле от алгебрични числа с група на Галоа G.

Реализирането на 2-групи като групи на Галоа е важно и бързо развиващо се направление в Теорията на Галоа.

По-нататък в изложението ще искаме решението на задачата за вложимост, свързана с точната редица

$$1 \to A \to G \xrightarrow{\alpha} F = \mathrm{Gal}(K/k) \to 1 \tag{3}$$

да бъде поле (а не алгебра на Галоа).

Важно място заемат задачите, свързани с точната редица

$$1 \to C_2 \to H \to F = \mathrm{Gal}(K/k) \to 1, \tag{4}$$

където C_2 е циклична група от ред 2.

Съгласно известната теорема ([1], I, §10) всяка задача (3) с 2-ядро A може да се сведе към някоя задача от вида (4). Критерий за разрешимостта на (4) ни дава следната теорема.

Теорема 21([22]). Нека K/k е крайно разширение на Галоа с характеристика различна от 2 и нека

$$1 \to C_2 \to H \to F = \mathrm{Gal}(K/k) \to 1, \tag{5}$$

е неразцепимо разширение на групи с характеристичен клас $c \in H^2(F, C_2)$. Тогава задачата за вложимост, свързана с (5) е разрешима тогава и само тогава, когато $j(c) = 1$ в $H^2(F, K^*)$, където изображението $j : H^2(F, C_2) \to H^2(F, K^*)$ се индуцира от включването $C_2 = \{\pm 1\} \subset K^*$.

Определение 21 ([23]). Ако A и B са крайномерни прости алгебри над полето K, то ще казваме, че те са еквивалентни ($A \sim B$), ако за естествените числа m и n алгебрата $A \otimes K_m$ е изоморфна на алгебрата $B \otimes K_n$ (K_m и K_n са съответно алгебри на матриците от ред m и n с елементи от полето K).

Тази релация е релация на еквивалентност. Нека $B(K)$ е множеството от класовете на еквивалентност. В $B(K)$ въвеждаме произведение на класове по правилото $[A][B] = [A \otimes_K B]$. Относно тази операция $B(K)$ е абелова група, която наричаме група на Брауер на полето K.

Когато $F = \mathrm{Gal}(K/k)$ групата на Брауер ще означаваме с $\mathrm{Br}(K/k)$. Кохомологичната група $H^2(F, K^*)$ е канонично изоморфна на относителната група на Брауер $\mathrm{Br}(K/k)$. Съгласно този изоморфизъм можем да считаме, че $j(c)$ е елемент на $\mathrm{Br}(K/k)$. Този елемент$j(c)$ ще наричаме препятствие на задачата (4). Тъй като $j(c)^2 = 1$, то следва [24], че кръстосаното произведение $[K, F, c]$ може да се представи като произведение на кватернионни алгебри.

Определение 22. Нека k е поле с характеристика различна от 2 и $a, b \in k^*$. Кватернионна алгебра (или алгебра на кватернионите) $(a, b/k)$ наричаме алгебрата над k, породена от елементите i и j с релациите $i^2 = a, j^2 = b, ij = -ji$. Съответно с (a, b) ще означаваме класът на еквивалентност $(a, b/k)$ в групата на Брауер $\mathrm{Br}(k)$. Ще казваме, че $(a, b/k)$ се разпада, ако $(a, b/k)$ е изоморфна на матричната алгебра $M_2(k)$, т.е. $(a, b) = 1 \in \mathrm{Br}(k)$.

Определение 23. Ще казваме, че елементите $a \in k^* \backslash k^{*^2}$ и $b \in k^* \backslash k^{*^2}$ са квадратично независими, ако $ab \notin k^{*^2}$, т.е. $k(\sqrt{a}) \neq k(\sqrt{b})$. Елементът $a \in k^* \backslash k^{*^2}$ наричаме ригиден, ако множеството от елементи на k, представени чрез квадратичната форма $< 1, a >= x^2 + ay^2$ е точно $k^{*^2} \cup ak^{*^2}$.

Ще разгледаме реализирането на $\mathbb{Q}_8$ като група на Галоа над поле с характеристика, различна от 2.

Кватернионната група $\mathbb{Q}_8$ има ред 8 и се задава с представянията $\mathbb{Q}_8 = \langle \sigma, \tau | \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma = \sigma^{-1}\tau \rangle$.

Теорема 24([25]). Нека характеристиката на полето K е различна от 2. Задачата

$$1 \to C_4 = \langle \sigma \rangle \to \mathbb{Q}_8 \to C_2 = \langle \rho \rangle = \mathrm{Gal}(k\sqrt{b}/k) \to 1$$

е разрешима тогава и само тогава, когато съществува елемент $a \in k^* \backslash k^{*^2}$, така че a и b са квадратично независими и $(a, ab)(b, b) = (a, -b)(b, b) = 1 \in \mathrm{Br}(k)$.

Диедралната група от ред 16 се задава така:

$$D_{16} \cong \left\langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^7\tau \right\rangle.$$

Теорема 25([26]). Задачата

$$\to C_4 = \left\langle \sigma^2 \right\rangle \to D_{16} \xrightarrow[\substack{\sigma \to \rho_1 \\ \tau \to \rho_2}]{} C_2^2 = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \to 1$$

е разрешима тогава и само тогава, когато $(a, b) = 1 \in \mathrm{Br}(k)$, $(a, 2) = (-b, x) \in \mathrm{Br}(k)$ за някое $x \in k^*$.

Разглеждаме следните групи:
$D_{8n} \cong \langle \sigma, \tau | \sigma^{4n} = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle$ – диедрална група,

$SD_{8n} \cong \langle \sigma, \tau | \sigma^{4n} = \tau^2 = 1, \tau\sigma = \sigma^{2n-1}\tau \rangle$ – полудиедрална група.

Ще изследваме задачи за вложимост, получени от груповите разширения от $H^2(D_{8n}, \mu_2)$ и $H^2(SD_{8n}, \mu_2)$.

Съгласно [27] $H^2(D_{8n}, \mu_2) \cong \mu_2^3$ и всички неразцепими редици дават следните шест неизоморфни групи:
$G_1 \cong D_{16n}, G_2 \cong SD_{16n}, G_3 \cong Q_{16n}$,
$G_4 = \langle \sigma, \tau, \rho | \sigma^{4n} = 1, \tau^2 = \rho, \rho^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle, \rho$ – централен елемент,

$G_5 = \langle \sigma, \tau, \rho | \sigma^{4n} = 1, \tau^2 = \rho, \rho^2 = 1, \tau\sigma = \sigma^{-1}\tau\rho \rangle, \rho$ – централен елемент,

$G_6 = \langle \sigma, \tau, \rho | \sigma^{4n} = 1, \tau^2 = 1, \rho^2 = 1, \tau\sigma = \sigma^{-1}\tau\rho \rangle, \rho$ – централен елемент.

Освен това $H^2(SD_{8n}, \mu_2) \cong \mu_2^2$ и всички неразцепими редици дават следните три неизоморфни групи
$G_7 = \left\langle \sigma, \tau, \rho | \sigma^{4n} = 1, \tau^2 = \rho, \rho^2 = 1, \tau\sigma = \sigma^{2n-1}\tau \right\rangle, \rho$ – централен елемент,

$G_8 = \left\langle \sigma, \tau, \rho | \sigma^{4n} = 1, \tau^2 = \rho, \rho^2 = 1, \tau\sigma = \sigma^{2n-1}\tau\rho \right\rangle, \rho$ – централен елемент,

$G_6 = \left\langle \sigma, \tau, \rho | \sigma^{4n} = 1, \tau^2 = 1, \rho^2 = 1, \tau\sigma = \sigma^{2n-1}\tau\rho \right\rangle, \rho-$ централен елемент.

Теорема 27([28]). Нека H е група изоморфна на D_{8n} или SD_{8n} и нека L/F е H-разширение, съдържащо биквадратичното разширение $K/F = F(\sqrt{a}, \sqrt{b})/F$. Тогава препятствието за задачата

$$1 \to \mu_2 \to G_i \to H = \mathrm{Gal}(L/F) \to 1$$

за $i = 4$ и $i = 7$ е $(b, -1) \in \mathrm{Br}(F)$.

Теорема 28([28]). Нека H е група изоморфна на D_{8n} или SD_{8n} и $H = \mathrm{Gal}(L/F)$, като L/F съдържа биквадратичното разширение $K/F = F(\sqrt{a}, \sqrt{b})/F$. Тогава препятствието за задачата

$$1 \to \mu_2 \to G_i \to H = \mathrm{Gal}(L/F) \to 1$$

за $i = 6$ и $i = 9$ е $(a, -1) \in \mathrm{Br}(F)$.

Теорема 29([28]). Нека H е група изоморфна на D_{8n} или SD_{8n} и $H = \mathrm{Gal}(L/F)$, като L/F съдържа биквадратичното разширение $K/F = F(\sqrt{a}, \sqrt{b})/F$. Тогава препятствието за задачата

$$1 \to \mu_2 \to G_i \to H = \mathrm{Gal}(L/F) \to 1$$

за $i = 5$ и $i = 8$ е $(ab, -1) \in \mathrm{Br}(F)$.

Нека F_q е крайно поле с $q = p^m$ елемента (p -просто число) и нека F_q^n е n-мерното векторно пространство над F_q.

Определение 30. Всяко k-мерно подпространство C на F_q^n наричаме линеен код с дължина n и размерност k, бележим $[n, k]$ код.

Определение 31. Разстояние (на Хеминг) $d(x, y)$ между два вектора $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ от F_q^n наричаме броя на координатите, в които те се отличават, т.е. $d(x, y) = |\{i | x_i \neq y_i\}|$.

Определение 31. Тегло (на Хеминг) $wt(x)$ на вектора $x = (x_1, x_2, \ldots, x_n) \in F_q^n$ наричаме броя на ненулевите му координатите, т.е. $wt(x) = |\{i | x_i \neq 0\}|$.

Определение 32. Минимално разстояние $d(C)$ на кода C наричаме най-малкото от разстоянията между две различни кодови думи, т.е. $d(C) = \min\{d(x, y) | x, y \in C, x \neq y\}$.

Минимално тегло на C наричаме най-малкото тегло от всички ненулеви тегла на векторите в C.

Тъй като C е линеен код, то минималното разстояние и минималното тегло съвпадат. Това число ще означаваме с d и казваме, че C е q-ичен $[n, k, d]$ код или $[n, k, d]_q$ код.

Всеки базис на кода C, разгледан като подпространство с размерност k, се състои от k на брой максимално линейно независими вектора.

Ако запишем тези k вектора във вид на матрица с размерност $k \times n$, то получаваме така наречената пораждаща матрица G на кода C.

В линейното пространство F_q^n с фиксиран автоморфизъм σ на полето F_q задаваме скаларно произведение по следния начин $(u, v) = \sum_{i=1}^{n} u_i \sigma(v_i)$, където $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n)$.

Например в полето F_2 има единствен автоморфизъм и това е тъждественият автоморфизъм. Тогава в F_2 скаларното произведение е $(u, v) = \sum_{i=1}^{n} u_i v_i$.

Определение 33. Нека C е линеен $[n, k]$ код. Кодът $C^{\perp} = \{u \in F_q^n | (u, v) = 0, \forall v \in C\}$ наричаме дуален код на C.

Тъй като $C^{\perp}$ е ортогоналното допълнение на подпространството C, добре известно е, че $\dim C + \dim C^{\perp} = n$. Следователно $C^{\perp}$ е линеен $[n, n-k]$ код.

Определение 34. Ако $C \subset C^{\perp}$, C наричаме слабо дуален код.

Определение 35. Ако $C = C^{\perp}$, то C наричаме самодуален код.

Ясно е, че ако C е самодуален код, то неговата размерност е $\frac{n}{2}$, т.е. той е $\left[n, \frac{n}{2}\right]$-код, т.е. самодуални кодове има само за четни дължини на векторите (кодовите думи).

Определение 36. Спектър на кода C наричаме $(n+1)$-орката $(A_0, A_1, \ldots, A_n)$, където A_i $(i = 0, 1, \ldots, n)$ е броят на кодовите думи с тегло i. Хомогенният полином $W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$ наричаме тегловна функция на кода C.

Ако положим $x = 1$, получаваме нов вид на тегловната функция

$$W_C(1, y) = W_c(y) = \sum_{i=0}^{n} A_i y^i.$$

Ясно е, че за всеки линеен код $A_0 = 1$ и ако кодът е $[n, k, d]$, то $A_1 = A_2 = \ldots = A_{d-1} = 0$.

Информация за теглата на самодуалните кодове ни дава следната важна теорема.

Теорема 37(Gleason-Pierce [29]). Нека C е формален самодуален код над F_q, на който теглата на кодовите думи са кратни на цялото число $t > 1$. Тогава е изпълнено едно от следните условия:

(1) $q = 2, t = 2$;

(2) $q = 2, t = 4$;

(3) $q = 3, t = 3$;

(4) $q = 4, t = 2$;

(5) $t = 2$ и C е тривиален;

(6) $[n, n/2, d]-$код с тегловна функция $(y^2 + (q-1)x^2)^{n/2}$.

Определение 38. Самодуалните кодове, които удовлетворяват условието (1) на Теорема 37 ще наричаме едночетни самодуални кодове или кодове от тип I.

Определение 39. Самодуалните кодове, които удовлетворяват условието (2) на Теорема 37 ще наричаме двойночетни самодуални кодове или кодове от тип II.

Известно е, че дължината на всеки двойночетен самодуален код се дели на 8. За горната граница на минималното разстояние на самодуалните кодове са известни теоремите.

Теорема 40 ([29]). Ако C е двоичен двойночетен самодуален $[n, n/2, d]$ код, то $d \leq 4\left[\frac{n}{24}\right] + 4$.

Теорема 41[Rains (1998)]. Ако C е двоичен самодуален $[n, n/2, d]$ код, то

$$d \leq \begin{cases} 4\left[\frac{n}{24}\right] + 4, n \not\equiv 22 \pmod{24}, \\ 4\left[\frac{n}{24}\right] + 6, n \equiv 22 \pmod{24}. \end{cases}$$

Ако n е кратно на 24 и $d = 4\left[\frac{n}{24}\right]$, то кодът C е двойночетен.

Определение 42. Ако един двоичен самодуален код достига горната граница от Теорема 41, то той се нарича екстремален код. Съответно кодът наричаме оптимален, ако не съществува самодуален код с по-голямо минимално разстояние за същата дължина.

Ясно е, че всеки екстремален код е оптимален, но обратното не винаги е вярно. Например за $n = 26$ не съществуват екстремални кодове.

Двойночетните самодуални кодове не съществуват за дължина $n > 3928$ [30].

Определение 43. Два линейни $[n, k, d]$ кода над полето F_q наричаме еквивалентни, ако всички кодове думи на единия код, могат да се получат от кодовите думи на другия код, чрез последователност от следните трансформации:

(1) пермутация на координатите;

(2) умножение на елементите в дадена координата с ненулев елемент на F_q;

(3) прилагане на автоморфизъм на полето към елементите във всички координатни позиции.

Всяка от горните трансформации запазва теглото на Хеминг и изобразява един $[n, k, d]_q$ код в $[n, k, d]_q$ код. Редица от трансформации (1) и (2) е еквивалентна на умножение отдясно на кодовите думи от първия код с подходяща $n \times n$ мономиална матрица, т.е. матрица, съдържаща точно един ненулев елемент от F_q във всеки ред и стълб.

Можем още да казваме, че два кода C_1 и C_2 са еквивалентни, ако съществува мономиална матрица $M \in \mathrm{Mon}(n, q)$ и автоморфизъм γ на полето F_q, за което е изпълнено $C_1 M\gamma = C_2$. (Тук $C_1 M = \{uM | u \in C_1\}$).

Така определената релация е релация на еквивалентност и тя разбива множеството от всички кодове с дадени параметри на класове на еквивалентност.

Задачата за класификация на кодове се състои в това, да се намери броят на класовете на еквивалентност и да се посочи представител от всеки клас.

Определение 44. Автоморфизъм на линеен код C наричаме всяка последователност от трансформациите в Определение 43, която изобразява всяка кодова дума от C в кодова дума също от C.

Всеки автоморфизъм на кода C може да се представи като наредената двойка (M, γ), за която е изпълнено $CM\gamma = C$. ($M \in \mathrm{Mon}(n, q)$, γ е автоморфизъм на полето F_q).

Нека G е множеството от всички автоморфизми на кода C. В G въвеждаме операцията умножение по правилото $(M_1, \gamma_1)(M_2, \gamma_2) = (M_1 M_2, \gamma_1 \gamma_2)$.

Относно тази операция G е група, която наричаме група от автоморфизми на кода C и бележим с $\mathrm{Aut}(C)$.

За двоични кодове само трансформацията от тип (1), т.е. пермутация на координатите, е нетривиална. Така че групата от автоморфизми на двоичен линеен код с дължина n може да бъде разглеждана като подгрупа на симетричната група S_n.

Основната идея за използването на автоморфизми при построяването на комбинаторни обекти идва от R. Austee, M. Hall Jr. И J. G. Thompson, които през 1980 г. публикуват работата [31], където използват автоморфизми за търсена на проективна равнина от ред 10.

Нека C е двоичен $[n, n/2, d]$ самодуален код, притежаващ автоморфизъм σ от тип $p-(c,f)$, т.е. σ се представя като произведение на c цикъла с дължина p и има f неподвижни точки. Това означава, че σ има ред p (p - нечетно просто число).

Без ограничение на общността можем да считаме, че $\sigma = (1,2,\ldots,p)(p+1,p+2,\ldots,2p)\ldots((c-1)p+1,(c-1)p+2,\ldots,cp)$ е разлагането на σ на независими цикли. Нека $\Omega_1 = \{1,2,\ldots,p\}, \Omega_2 = \{p+1,p+2,\ldots,2p\},\ldots,\Omega_c = \{(c-1)p+1,(c-1)p+2,\ldots,cp\}$ са циклите, а $\Omega_{c+1} = \{cp+1\}$, $\Omega_{c+2} = \{cp+2\}$, $\ldots$, $\Omega_{c+f} = \{cp+f\}$ са неподвижните точки на σ.

Разглеждаме следните две подмножества на C:

$$F_\sigma(C) = \{v \in C | v\sigma = v\},$$

$$E_\sigma(C) = \{v \in C | wt(v|\Omega_i) \equiv 0 (\mathrm{mod}\ 2), i = 1, 2, \ldots, c + f\},$$

където $v|\Omega_i$ е рестрикцията на v върху Ω_i.

Теорема 45 ([32]). $F_\sigma(C)$ и $E_\sigma(C)$ са подкодове на C, $C = F_\sigma(C) \oplus E_\sigma(C)$ и $\dim E_\sigma(C) = \frac{(p-1)c}{2}$.

От тази теорема следва, че за кода C съществува пораждаща матрица от вида $\mathrm{gen}C = \begin{pmatrix} \mathrm{gen}F_\sigma & \\ \mathrm{gen}E_\sigma & O \end{pmatrix}$,където O е матрица от тип $\frac{c(p-1)}{f} \times f$.

В. Йоргов подобрява този метод като дава необходими и достатъчни условия за еквивалентност на получените кодове в зависимост от типа на автоморфизма [33].

През последните 20 години са получени голям брой резултати за конструиране и класификация на екстремални или оптимални самодуални двоични кодове като се използва този метод.

Един от първите резултати за пълна класификация на самодуални кодове с определен автоморфизъм е получен през 1996 г. от В. Йоргов и Н. Зяпков. В сила е теоремата.

Теорема 46 ([34]). Съществуват 45 нееквивалентни двойночетни самодуални $[40, 20, 8]$ кодове, притежаващи автоморфизъм от ред 5.

Броят на всички самодуални двоични кодове при по-големи дължини расте експоненциално и дори класификацията само на оптимални кодове на този етап е невъзможна. Затова често се въвежда ограничение на кода, свързано с неговата група от автоморфизми.

Теорема 47 ([35]). Редът на групата от автоморфизми на самодуален $[72, 36, 14]$ код може да бъде само произведение от степените на простите числа 2, 3, 5, 7 и 11.

Интересна е групата от автоморфизми на двоичния самодуален $[96, 48, 20]$ код. А. Щерев, В. Йоргов и Н. Зяпков през 1990 г. [36] доказаха, че единствените нечетни прости числа, които могат да бъдат ред на автоморфизъм на този код са 47, 31, 23, 11, 7, 5 и 3. В същата публикация [36] бяха изключени простите числа 47 и 31. През 2002 г. Р. Дончева [37] изключи простите числа 23, 11 и 7. Изследванията върху този код продължават до момента. Н. Янков през 2013 доказа следния резултат:

Теорема 48([38]). Не съществува двоичен самодуален двойночетен $[96, 48, 20]$ код с автоморфизъм от тип $9 - (10, 0, 6)$.

При доказателството на тази теорема се използват резултати, свързани със структурата на двоичните самодуални кодове с автоморфизъм от ред квадрат на нечетно просто число [39].

Също така Н. Янков разработи метод за конструиране на самодуални двоични кодове с автоморфизъм от ред произведение на два нечетни прости числа. Като се използва този метод Н. Янков, Ст. Буюклива и В. Вилемс доказаха следната теорема:

Теорема 49 ([40]). Не съществува двоичен двойночетен самодуален $[96, 48, 20]$ код притежаващ автоморфизъм от ред 15.

От много автори са изследвани екстремалните самодуални двойночетни кодове $[24k, 12k, 4k + 4]$ за $k = 3, 4$. Най-малката дължина, за която не е известно дали съществува екстремален самодуален двойночетен код от горния тип е при $k = 3$, т.е. това е самодуалния [72, 36, 16] код. Изследванията на групата му от автоморфизми са започнали през 1982 г, с работата на Дв. Конуей и В. Плесс [41]. Тези изследвания са продължени от редица учени: Дж. Томсън, К. Хъфман, В. Йоргов, Ст. Буюклиева, В. Вилемс и др.

До момента е доказано, че групата от автоморфизми на този код има ред 5, 7, 10, 14; или ред d, който е делител на 18 или 24; или е групата $A_4 \times C_3$.

Като използва метода за конструиране на самодуални кодове с автоморфизъм от ред p^2 за нечетно просто число p [39] и резултатите от [42] Н. Янков доказва следната теорема:

Теорема 50([43,44]). Не съществува двоичен двойночетен самодуален $[72, 36, 16]$ код притежаващ автоморфизъм от ред 9.

В 1870 г. Феликс Клайн (1849-1925), който е бил в Париж се запознава с работите на К. Жордан и Е. Галоа. Той достига до извода, че централно място при изучаването на геометрията трябва да се даде на понятието група.

Тези свои идеи Клайн излага през 1872 г. в знаменитата си "Ерлангенска програма"[45]. Това е неговата встъпителна лекция при избирането му за професор (тогава на 23 г.) в университета в Ерланген (Германия). При излагането на неговите идеи ще се придържаме при изложението по този въпрос към източниците [46] и [47].

Клайн формулира предмета на геометрията по следния начин:

“Геометрията е наука, изучаваща свойствата на фигурите, които са инвариантни относно някаква група от преобразувания”

Предметът на геометрията може да се формулира по следният начин: Дадено е множество M и нека G е група от преобразувания на M. Съвкупността от величините, фигурите, свойствата за тях, които са инвариантни при произволно преобразуване на групата, се нарича G-геометрия на множеството M.

Нека т. N има координати (x, y, z) спрямо ортонормирана координатна система в пространството $Oxyz$. Да съпоставим на т. N т. N' с координати (x', y', z'), които се получават от равенството

$$X' = A + BX, \tag{6}$$

където

$$X' = \begin{pmatrix} x' & y' & z' \end{pmatrix}^T, A = \begin{pmatrix} a & b & c \end{pmatrix}^T, B$$

е ортогонална матрица от трети ред, т.е. $BB^T = E$.

Това преобразование наричаме еднаквост в пространството.

Непосредствено се проверява, че множеството от еднаквостите в пространството е група и всяка еднаквост запазва разстоянието между две точки в пространството. Породената от тази група геометрия наричаме метрична геометрия в пространството.

Аналогично на матричното равенство (6) можем да зададем следното преобразуване:

$$X' = A + BX, \tag{7}$$

където B е неособена матрица от трети ред и координатите на точките са относно афинна координатна система в пространството. Това преобразуване наричаме афинно преобразуване в пространството.

Тези преобразувания също образуват група, която наричаме афинна група. Породената от нея геометрия наричаме афинна геометрия.

В сила са теоремите:

Теорема 51([47]). Всяко афинно преобразуване преобразува афинната координатна система в афинна координатна система; обратно, за всеки две афинни координатни системи съществува точно едно афинно преобразуване, което привежда едната координатна система в другата.

Теорема 52([47]). Всяко афинно преобразуване преобразува равнина в равнина, права в права, безкрайна точка в безкрайна точка и запазва простото отношение на 3 т. върху една права.

Нека т. N има координати (x^1, x^2, x^3, x^4) относно проективната координатна система $K = [A_1A_2A_3A_4; E]$ в разширеното евклидово пространство R_3. Да съпоставим на т. N, т. N' с координати $[\overline{x^1}, \overline{x^2}, \overline{x^3}, \overline{x^4}]$, които се получават от равенството

$$\overline{X} = CX, \tag{8}$$

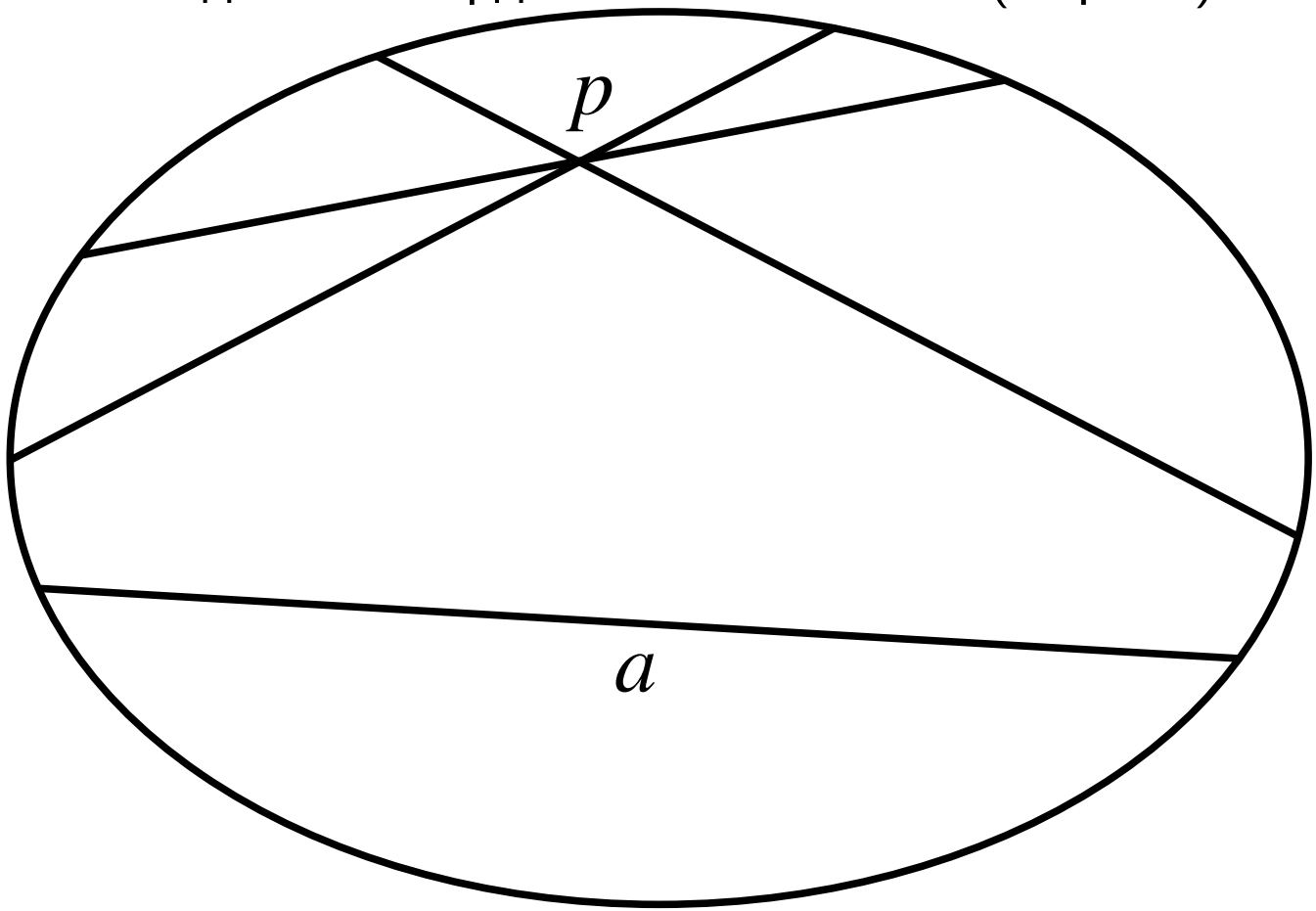
където $\overline{X} = (\overline{x^1} \;\; \overline{x^2} \;\; \overline{x^3} \;\; \overline{x^4})^T, X = (x^1 \;\; x^2 \;\; x^3 \;\; x^4), C$ е неособена матрица от четвърти ред.

Това преобразуване наричаме проективно преобразуване в разширеното евклидово пространство. Тези преобразувания образува група, която се нарича проективна група, а породената от нея геометрия – проективна геометрия на разширеното евклидово пространство. В сила е следната теорема.

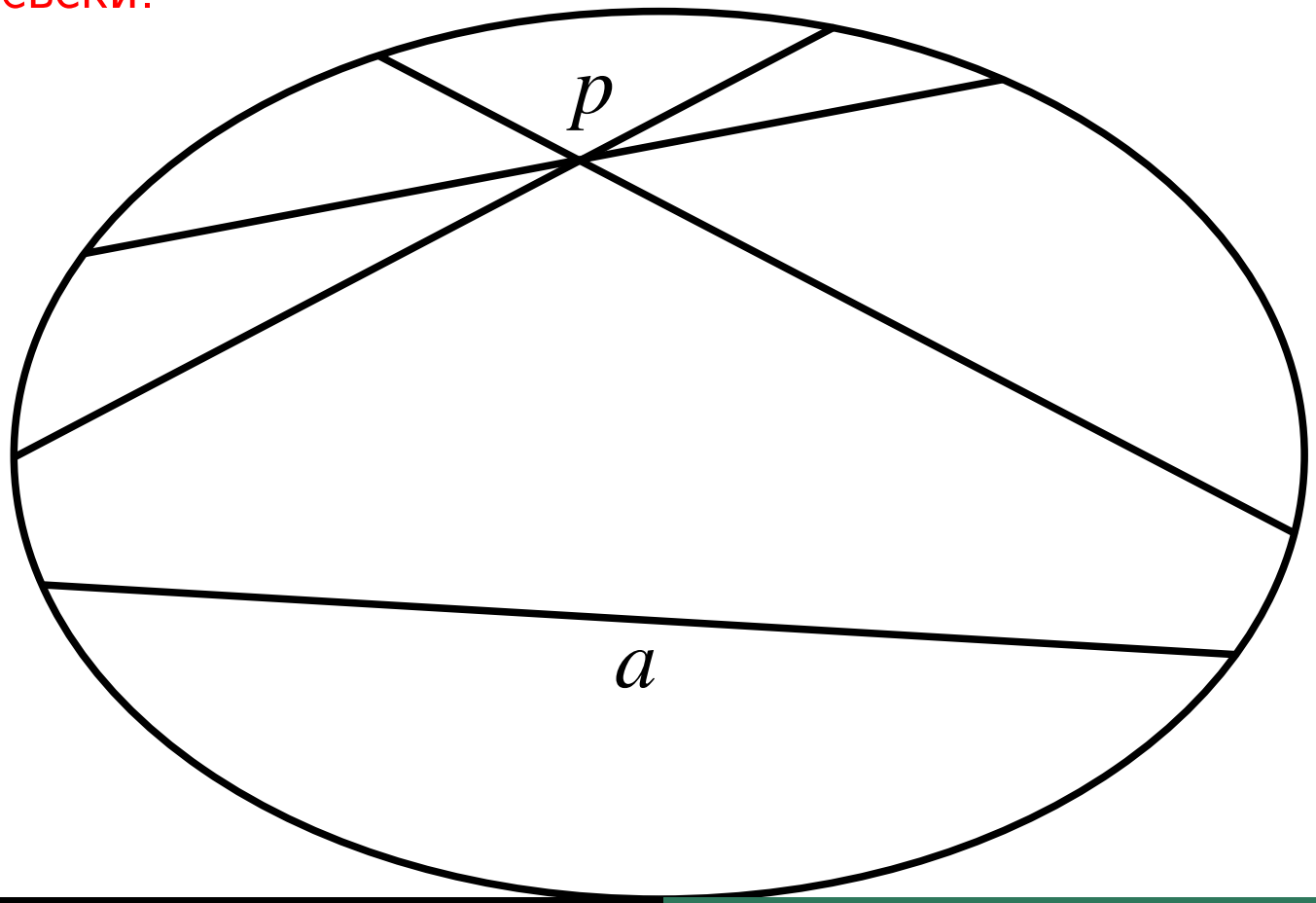
Теорема 53 ([47]). Всяко проективно преобразуване преобразува равнина в равнина, права в права и запазва двойното отношение на четири точки.

По-късно Феликс Клайн [48] разработва модели, чрез които успява да включи неевклидовите геометрии на Лобачевски и Риман в груповата схема, начертана в неговата ерлангенска програма.

Нека в проективната равнина е дадено реално конично сечение k (овална крива). Точките на тази крива можем да считаме за безкрайно отдалечените елементи в този модел на геометрията на Лобачевски, точките на модела са всички точки в проективната равнина, лежащи върху областта оградена от k, правите на модела са хордите на линията k (Черт. 1).



В този модел са в сила всички аксиоми за еквлидовата геометрия с изключение на аксиомата за успоредните прави. От черт. 1 се вижда, че през т. P от модела, нележаща на правата a могат да се построят безбройно много прави, които не пресичат правата a, т.е. са успоредни на правата a. Този модел се нарича проективен модел на двумерната геометрия на Лоабчевски.



Всяко проективно преобразуване на проективната равнина, което оставя на място линията k наричаме автоморфизъм относно k. Множеството на всички такива автоморфизми е група.

Геометрията на Лобачевски може да се разгледа като теория, изучаваща свойствата на фигурите и свързаните с тях величини, които остават инвариантни, относно тази група от автоморфизми.

Геометрията на Риман (двумерната) допуска сходно тълкуване. Разглеждаме проективната равнина, в която са въведени хомогенни проективни координати (x_1, x_2, x_3). Точките и правите на модела са всички точни и прави на проективната равнина. Разглеждаме уравнението

$$x_1^2 + x_2^2 + x_3^2 = 0. \tag{9}$$

Автоморфизмите са линейни преобразувания, които привеждат уравнението (9) в уравнение от същият вид. Те също образуват група. Породената от тази група геометрия е двумерната геометрия на Риман.

Аналогично се строят проективни модели на двете неевклидови геометрии от по-голяма размерност.

Изложеният до тук метод е част от една по-голяма теория, наречена “Теория на инвариантите”, която се прилага почти във всички дялове на математиката.

Литература

1. E. Galois. Memoire sur les conditions de resolubilite des equations par radicaux, J. Math. Pures Appl., 11 (1846), 417-433.
2. И. Михайлов, Н. Зяпков, Висша алгебра и теория на Галоа, Фабер, 2004
3. Scholz A., Konstruktion von Zahlokoprern mit beliebiger Gruppe von Primzahlpotenzordnung, Math. Z., 1936, Bd. 42, S. 161-188
4. Reichardt H., Konstruktion von Zahlokoprern mit gegebener Galoisgruppe von Primzahlpotenzordnung, J. reine anrew. Math., 1937, Bd. 177, S. 1-5
5. Шафаревич И., О задаче погружении полей, ДАН СССР, 1954, Т. 95, № 3, 459-461
6. Шафаревич И., О построении полей с заданной группой Галуа порядка , Изв. АН СССР, Сер. Мат., 1954, Т. 18, № 3, 261-296
7. Шафаревич И., Об одной теореме существования в теории алгебраических чисел, Изв. АН СССР, Сер. Мат., 1954, Т. 18, № 4, 327-334

8. Шафаревич И., О задачи погружения полей, Изв. АН СССР, Сер. Мат., 1954, Т. 18, № 5, 389-418
9. Shih, K. Y., On the construction of Galois extensions of function fields and number fields, Math. Ann. 207 (1974), 99-120
10. Malle G., Matzat B. H., Realisierung von Gruppen PSL2(Fp) als Galoisgruppen uber Q, Math. Ann. 272 (1985), pp. 549-565
11. Thompson J. G., Some finite groups which appear as Gal(L/k), where J. Algebra 89 (1984), 437-499
12. Malle G., Matzat B. H., Inverse Galois Theory, Springler Monographs in Mathematics, Springler-Verlag, 1999
13. Michailov I., Ziapkov N., The Inverse Problem in Galois Theory, Proceedings of the Thirty Seventh Spring Conference of the Union of Bulgarian Mathematicians, Borovec, Bulgaria (2008), 17-28
14. Фаддеев Д. К., Об однойн гипотезе, ДАН СССР, 1954, Т. 94, № 6, С. 1012-1016
15. Hasse H., Existenz and Manningfaltigkeit Algebren mit vorgegebener Galoisgruppe uber einem Teilkoprer des Grundkoprers, Math Nachr., 1948, Bd. 1, № 1, 40-61, Bd. 1, № 4, 213-217

16. Ишханов В. В., О полупрямой задаче погружения с ниьлпотентным ядром, Изв. АН СССР, Сер. Мат., 1976, Т. 40, № 1, С. 3-25
17. Зяпков Н. П., Яковлев А. В., Универсально согласные разширения Галуа, Зап. научн. сем. ЛОМИ, 1977, Т. 71, 133-152
18. Neukirch J., On solvable number fields, Invent. math., 1979, v. 52, № 62, 135-164
19. Neukirch J., Schmidt A., Wingberg K., Cohomology of number fields, Grundlehren der Mathematischen Wissenschaften 323, Springler-Verlag, 2000
20. Feit, W., Thompson J., Solvability of groups of odd order, Pacific Journal of Mathematics, vol. 13, pp. 775-1029, 1963
21. Ишханов В. В., Лурье Б. Б., Фаддеев Д. К., Задача погружения в теории Галуа, Наука, Москва, 1990
22. Schneps L., Explicit Realizations of Subgroups of GL2(F3) as Galois Groups, J. Number Theory, 39, 1991, pp. 5-13
23. Херстейн И., Некоммутативные кольца, Москава, Мир, 1972

24. Merkurjev A., On the norm residue symbol of degree 2, Soviet Math. Dokl., 24, 1981, 546-551
25. Michailov I., Ziapkov N., Embedding obstructions for the generalized quaternion group, J. Algebra, 226, № 1, 2000, 375-389
26. Michailov I., Ziapkov N., Embedding problems with Galois groups of order 16, Math. Balk., New Series, v.15, 2001, Fasc. 1-2, 99-108
27. Michailov I., Noether's problem for some groups of order 16n, Acta Arithmetica, 143, 2010, pp. 277-290
28. Ziapkov N., Some relatives of the dihedral group as Galois groups, C.R. de' l Academie bulgarie des Sciences, T. 62,No 9, 2009, pp. 1063-1066
29. MacWilliams F.J., Sloane N.J.A., The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977
30. Zhang S., On the nonexistence of extremal self-dual codes, Discrete Math., 91, 1999, 277-286
31. Anstee R., Hall M. Jr., Thompson J. G., Planes of order 10 do not have a collineation of order 5, Journ. Combin. Theory, ser. A, 29, 1980, 39-58

32. Huffman W.C., Automorphisms of codes with application to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory, 28 (1982) 511-521
33. Yorgov V.Y., A method for constructing inequivalent self-dual codes with applications to length 56, IEEE Trans. Inform. Theory, 33 (1987) 77-82
34. Йоргов В., Зяпков Н., Дважды четные самодуалные [40, 20, 8] - коды с автоморфизмом нечетного порядка, Проблемы передачи информации, Москва, т. 32, 1996, вып.3, 41-46
35. Yorgov V. Ziapkov N., On the Group of a [72, 36, 14] Self-Dual Code, Intern. Workshop on Optimal Codes and Related Topics, Bulgaria, 1995, 143-145
36. Shterev A., Yorgov V., Ziapkov N., A [96, 48, 20] doubly-even self-dual code not have automorphisms of order 47 and 31, Intern. workshop ACCT, Leningrad, 1990, 191-194
37. Dontcheva R., On the doubly-even self-dual codes of length 96, IEEE Trans. Inform. Theory, 48, No 2, 2002, 557-561

38. Yankov N., On the binary self-dual [96, 48, 20] codes with an automorphism of order 9, Proceedings of the Seventh International Workshop on Optimal Codes and Related Topics, Albena, Bulgaria, 2013, pp. 193-198 39. Bouyuklieva B, Russeva R., Yankov N., On the Structure of Binary Self-Dual Codes Having an Automorphism of Order a Square of an Odd Prime, IEEE Trans. Inform. Theory, vol. 51, no. 10, pp. 3678-3686, 2005
40. Bouyuklieva S., Willems W., Yankov N., On the Automorphisms of Order 15 for a Binary Self-Dual [96, 48, 20] Code, to appear in Designs, Codes and Cryptography, pp. 1-13, 2015
41. Conway J., Pless V. , On primes dividing the group order of a doubly-even (72, 36, 16) code and the group order of a quaternary (24, 12, 10) code, Discrete Mathematics, vol. 38, no. 2-3, pp. 157-162, 1982
42. Bouyuklieva S., Some MDS codes over GF(64) connected wuth the binary doubly-even [72, 36, 16] code, Serdica Journal of Computing, vol. 1, pp. 185-192, 2007

43. Yankov N., A putative doubly even [72, 36, 16] code does not have an automorphism of order 9, IEEE Trans. Inform. Theory, vol. 58, no. 1, pp. 159-163, 2012
44. Yankov N., Near MDS codes over GF(64) related to doubly-even self-dual [72, 36, 16] code over GF(2), Proceedings of MATHTECH, vol. 1, 2010, pp. 71-76
45. Klein F., Verschiedene Betrachtung uber neuere geometrische Forschunden, Erlangen, 1872
46. Klein F., Elementarmathematik vom hoheren Standpunkte aus zweiter band (Geometrie), Berlin, 1925
47. Станилов Гр., Аналитична геометрия, София, 1979
48. Клайн Ф., Высшая геометрия, 1939
49. Зяпков Никола, Групи от автоморфизми в теорията на Галоа и в теорията на кодирането, Издателство "Фабер", ISBN:978-619-00-0899-6,2019,141 стр.(монография).