УДК 512.623.314(091)

Рябухо О.М., Мазніва Н.С.

[1] *кандидат фізико-математичних наук, доцент кафедри алгебри, ДВНЗ «ДДПУ»*

[2] *студентка 5 курсу фізико-математичного факультету, ДВНЗ «ДДПУ»*

e-mail: ren_elena@mail.ru

РОЗВИТОК ТЕОРІЇ ҐАЛУА В РОБОТАХ М.Г. ЧЕБОТАРЬОВА

В статті наведений огляд основних робіт М.Г. Чеботарьова з теорії Ґалуа, зроблений аналіз його досліджень та описані перспективи застосувань.

Ключові слова: *теорія Ґалуа, група Ґалуа, незвідний многочлен, рівняння з наперед заданою групою.*

Вступ

15 червня 2014 року науковий математичний світ відзначає 130-ту річницю з дня народження видатного математика і педагога, вихованця Київського Університету св. Володимира М.Г.Чеботарьова.

Миколай Григорович Чеботарьов народився 15 червня 1894 року в Кам'янець-Подільську. У 1912 році він закінчив місцеву гімназію і разом з батьками переїхав до Києва. В цьому ж році він був прийнятий у Київського університету на фізико-математичний факультет. Це був рік розквіту наукового алгебраїчного семінару Д.О. Граве, у роботі якого вже приймали участь О.Ю. Шмідт, М.Ф. Кравчук, Б.М. Делоне та інші. До роботи семінару активно долучився і М.Г. Чеботарьов. Влітку, 1913 року, після закінчення першого курсу він переклав з німецької мови на російську велику частину підручника Вебера з алгебри. Це було знайомство з теорію Галуа, яку професор Д.О.Граве на той час читав студентам третього курсу.

У 1916 році після закінчення університету М.Г. Чеботарьов був залишений для підготовки до професорського звання, готувався до магістерських екзаменів, які складав у 1918р.

Наукову діяльність М.Г. Чеботарьова можна розділити на три періоди: київський (1918-1921рр.), одеський (1921-1927рр.) і казанський (1927-1947рр.). До київського періоду відносяться дослідження питань з різних розділів математики: виділення алгебраїчної частини в абелевих інтегралах, задача, обернена задачі Чірнгаузена, про поверхні переносів, визначення щільності множин простих чисел, які належать до заданого класу підстановок та інші.

У кінці 1921р. Чеботарьов переїхав до Одеси. Там він працював секретарем науково-дослідницької кафедри при Одеському інституті народної освіти та продовжив наукові дослідження, над якими почав роботу ще в Києві.

Вагомим алгебраїчним дослідженням М.Г. Чеботарьова київського і початку одеського періоду його творчості є робота, яка присвячена вирішенню проблеми Фробеніуса [1]. Цю роботу в 1926р. Чеботарьов представив в Українську академію наук як докторську дисертацію, яку захистив у 1927 р. Його опонентами були Д.О. Граве, М.Ф. Кравчук і Г.В. Пфейффер. Після захисту дисертації Чеботарьов був запрошений в Казанський університет, де працював до кінця життя.

Найбільш плідною і багатогранною була науково-педагогічна діяльність М.Г. Чеботарьова в казанський період. У Казані він створив першокласну математичну школу, яка розвивалася за різними напрямками. Чеботарьов, як і його вчитель Граве, вимагав самостійної творчої роботи від студентів, починаючи з молодших курсів. Його учні працювали в усіх напрямках, за якими працював він сам. Більшість із них стали видатними радянськими вченими: Д.І. Адо, М.М. Мейман, Л.І. Гаврілов та інші. Вони з великим успіхом розробили ідеї свого вчителя в області теорії безперервних груп, напівпростих алгебр Лі, теорії поліномів, що продовжуються та інші. До приїзду Чеботарьова в Казань цими питаннями там ніхто не займався.

У Казані М.Г.Чеботарьов був беззмінним директором науково-дослідницького інституту математики і механіки, а з 1943 р. — головою Казанського фізико-математичного суспільства. В 1929 р. М.Г. Чеботарьов був обраний членом-кореспондентом АН СРСР, а у 1943 р. йому було присвоєно звання заслуженого діяча науки РРФСР. М.Г. Чеботарьов лауреат Державної премії СРСР, нагороджений орденом Леніна, двома орденами Трудового Червоного Прапору і медалями. Помер М.Г. Чеботарьов 24 червня 1947 р. в Москві у зеніті своєї творчої діяльності.

У 1947 р. президіям АН СРСР заснував премію ім. М.Г.Чеботарьова, яка «присуджується» один раз в три роки за кращу роботу з математики. Його іменем названо науково-дослідницький інститут математики і механіки при Казанському університеті.

Дана робота присвячена дослідженню наукової спадщини М.Г. Чеботарьова.

Мета дослідження полягає у вивченні основних положень теорії Ґалуа в роботах Чоботарьова, зокрема, дослідженню задачі про знаходження рівнянь з наперед заданою групою Ґалуа.

Рівняння з наперед заданою групою

Задача про знаходження рівнянь з наперед заданою групою Ґалуа вперше була поставлена в загальному вигляді Д. Гільбертом [2] в кінці XIX ст. Ним же у 1892р. вона була розв'язана для випадку симетричних і знакозмінних груп. Розв'язання Гільберта базується на його ж теоремі про незвідність, згідно з якою, якщо одночлен від декількох змінних незвідний над даним полем, то можна для одних із цих змінних підібрати такі значення, що після підстановки їх многочлен залишається незвідним відповідно останніх змінних над тим же полем.

Ця теорема є типовою теоремою «існування», тому розв'язання Гільберта не давало практичного способу знаходження шуканих рівнянь.

М. Бауер (1907р.) розв'язав задачу для симетричних груп в такий спосіб, який дійсно виконується на практиці. Для свого розв'язання даної задачі він використав теорему Дедекінда про зв'язки між розкладанням лівої частини рівняння на незвідні за простим модулем множники і циклами підстановок його групи Ґалуа.

Важливі результати у цьому напрямку були отримані Е.Нетер (1918р.) для випадку, коли деяка система функцій, які залежать від заданої групи, має так званий раціональний базис. Метод Нетер також заснований на вживанні теореми Гільберта про незвідність многочлена відповідно деяких змінних.

Незалежно від Бауера Чеботарьов для розв'язання задачі знаходження рівнянь з наперед заданою групою Ґалуа використовує теорему Дедекінда. В першій своїй роботі [3] (1926р.), присвяченої знаходженню алгебраїчних рівнянь з наперед заданою групою Ґалуа, він показав, що для випадку симетричної групи, якщо тільки можна знайти циклічні групи підстановок, які містяться в симетричній групі, але не містяться в жодній з її підгруп, то можна так скорегувати спосіб Бауера, що з його допомогою одержати всі можливі рівняння з симетричною групою, а також розв'язати задачу для груп, які допускають раціональний базис. При цьому побудова шуканих рівнянь виконується за скінченну кількість дій.

Крім того в цій же роботі [3] Чеботарьов довів теорему Дедекінда без використання теорії ідеалів. Нагадаємо теорему Дедекінда.

Якщо незвідний многочлен n-ого степеня

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_{n-1}x + p_n \tag{1}$$

має розклад на k незвідних множників за модулем p, (p не належить p дискримінантур многочлена)

$$f(x) \equiv f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x) \qquad (\mathrm{mod}\ p) \tag{2}$$

з відповідними степенями $n_1, n_2, \ldots, n_k (n_1+n_2+\ldots+n_k = n)$ то в групі Ґалуа цього рівняння міститься підстановка, яка складається із циклів порядків $n_1, n_2, \ldots, n_k$.

Доведення цієї теореми у Чеботарьова складається з двох частин: спочатку доводиться існування в групі Ґалуа підстановки циклів $n_1, \ldots, n_k$, а потім можливість такого способу нумерувати корені рівняння (1) і конгруенції (2), щоб група конгруенції була дільником групи рівняння.

Метод Чеботарьова на відміну від методу Бауера дає можливість побудувати всі рівняння з симетричною групою. Згідно способу Чеботарьова необхідно взяти підстановку циклу n-ого порядку, $n-1$-ого і транспозицію. Подальші міркування основані на теоремі Фробеніуса, оберненій теоремі Дедекінда. Якщо група Галуа рівняння (1) містить підстановку, яка складається із циклів порядків $n_1, \ldots, n_k$, то існує нескінченна множина таких простих чисел, що відповідна конгруенція (2) розкладається в добуток незвідних за модулем p множників степенів $n_1, n_2, \ldots, n_k$. Будь-яке рівняння без афекту, тобто з симетричною групою, містить підстановки трьох вказаних Чеботарьовим циклічних типів, отже, існує нескінченна множина простих модулів, за якими ліва частина рівняння або залишається незвідною, або розкладається на лінійний множник і множник $(n-1)$-го степеня, або на квадратний множник і $n-2$ лінійних. Труднощі побудови рівнянь з наперед заданою несиметричною групою, як показав Чеботарьов, полягають в тому, що при побудові рівнянь, до групи яких входили б підстановки заданих циклічних типів, можливий випадок, коли в цю групу входять і підстановки циклічного типу, які не містяться в заданій групі.

У роботі [3] Чеботарьов формулює задачу таким чином. Нехай $P = p_1 \cdot p_2 \cdot \ldots \cdot p_m$ — добуток вибраних простих модулів, $a_1, a_2, \ldots, a_n$ — вирахування класів за модулем p, які підібрані так, щоб рівняння

$$f(x) = x^n + a_n x^{n-1} + \ldots + a_{n-1}x + a_0 = 0 \tag{3}$$

мало групу, яка містить підстановки заданих циклічних типів. $z(x_1, x_2, \ldots, x_n)$ — функція, яка належить до заданої групи і задовольняє рівняння

$$F(z) = z^k + b_1 z^{k-1} + \ldots + b_{k-1}z + b_k = 0 \tag{4}$$

коефіцієнти якого $b_1, b_2, \ldots, b_k$ є цілими раціональними функціями від $a_1, a_2, \ldots, a_n$. Конгруенція $F(z) \equiv 0$ за кожним з модулів $p_1, p_2, \ldots, p_k$, а отже, і за модулем P має раціональний корінь.

Якщо замість $a_1, a_2, \ldots, a_n$ взяти $A_1 = a_1 + \alpha_1 P$, $A_2 = a_2 + \alpha_2 P$, $\ldots$, $A_n = a_n + \alpha_n P$, то коефіцієнти $b_1, b_2, \ldots, b_k$ рівняння (4) будуть раціональними функціями від $\alpha_1, \alpha_2, \ldots, \alpha_n$. Позначимо їх $\beta_1, \beta_2, \ldots, \beta_k$ і тоді конгруенція

$$\overline{F(z)} = z^k + \beta_1 z^{k-1} + \ldots + \beta_{k-1} z + \beta_k \equiv 0 \pmod{p}$$

буде мати раціональні корені при всіх значеннях $\alpha_1, \alpha_2, \ldots, \alpha_k$. Розв'язання задачі зводиться до знаходження чисел $\alpha_1, \alpha_2, \ldots, \alpha_k$ так, щоб рівняння $\overline{F(z)} = 0$ мало раціональні корені. Остання задача в загальному випадку не розв'язана. Чеботарьов показав, що задача легко розв'язується в окремому випадку, коли функції

$$a_1(x_1, x_2, \ldots, x_n), \ldots, a_n(x_1, x_2, \ldots, x_n), z(x_1, x_2, \ldots, x_n)$$

володіють раціональним базисом, тобто коли існують такі раціональні функції $\xi_1, \xi_2, \ldots, \xi_n$, через які раціонально виражаються всі раціональні функції $a_1, a_2, \ldots, a_n, z$. Такі функції знайдені лише для $n = 1$ і $n = 2$. Чеботарьов розглядає тільки той випадок, коли раціональний базис існує. Тоді необхідною і достатньою умовою того, що група рівнянь (3) була заданою групою або її дільником, є раціональність величин $\xi_1, \xi_2, \ldots, \xi_n$.

У 1934 р. М.Г. Чеботарьов у великій статті [4], яка присвячена проблемам сучасної теорії Галуа, зробив глибокий аналіз існуючих розв'язків задачі про знаходження алгебраїчних рівнянь з наперед заданою групою Галуа. Він встановив зв'язки між розв'язками описаної задачі і питанням вивчення полів раціональних функцій; сформулював задачу в більш загальній формі — у вигляді трьох задач:

1. Знайти будь-які рівняння, група яких була б ізоморфною групі Галуа;
2. Знайти загальну параметричну форму коефіцієнтів рівняння, група якого була б ізоморфною групі G або її підгрупі. Подання коефіцієнтів в цій формі має бути необхідною і достатньою умовою того, щоб група рівняння була ізоморфною групі G або її підгрупі.
3. Знайти спосіб для визначення рівнянь, група яких ізоморфна групі G, причому цей спосіб повинен охоплювати всі рівняння цього роду, якщо його достатньо продовжити.

Висновки

У результаті проведених історично-математичних досліджень можна стверджувати, що наукова спадщина М.Г. Чеботарьова збагатила вітчизняну і світову науку.

Роботи знаного математика відрізнялися чіткістю постановки проблеми, пошуками нових методів розв'язання задач, доведенням розв'язків до повного алгоритму.

У своєму відгуку про М.Г. Чеботарьова у зв'язку з висуненням його кандидатури у члени АН УРСР у 1938 р. Д.О. Граве писав: «...Знаменитый французский математик Э. Галуа был убит на дуэли в возрасте 21 года, и, несмотря на это, ему удалось создать теорию, которая в продолжении более 100 лет занимает умы лучших представителей математики. Начиная с вопросов алгебры, она постепенно вошла в новые части математики. Чеботарев посвящает теории Ґалуа книги. Этим он показал глубокое понимание исторических перспектив хода развития математики....»

Теорія Ґалуа беззаперечно не втратила своєї актуальності і має широке коло застосувань. Зокрема в сучасних системах захисту інформації використовуються алгоритми, що ґрунтуються на властивостях груп точок еліптичних кривих у полях Ґалуа [8]. Саме з їх допомогою будуються найефективніші на сьогодні алгоритми тестування простоти і розкладу чисел на множники.

Література

1. *Чеботарев Н.Г.* Определение плотности совокупности простых чисел, принадлежащих к заданому классу подстановок. — Собр. соч. т. I, 1949. — С. 26–65.
2. *Чеботарев Н.Г.* К задаче нахождения алгебраических уравнений с наперед заданой группой. — Собр. соч. т. I, 1949. — С. 87–94.
3. *Чеботарев Н.Г.* Исследование о плотности простых чисел. — Собр. соч. т. I, 1949. — С. 102–118.
4. *Чеботарев Н.Г.* Об одной алгебраической проблеме Гильберта. — Собр. соч. т. I, 1949. — С. 267–281.
5. *Чеботарев Н.Г.* Алгебра I (Алгебра полиномов и полей), в кн.: Математика в СССР за 30 лет. — М., 1948. — С. 89–105.
6. *Чеботарев Н.Г.* Проблемы современной теории Галуа. — Труды всесоюзного математического съезда т. I, 1934. — С. 164–205.
7. *Чеботарев Н.Г.* Основы теории Галуа. ч. I. — ГТТИ, М.–Л., 1934. ч. II. — ОНТИ, 1937. — 160 с.
8. *Колеснікова О.О.* Реалізація шифру Ель-Гамаля на еліптичній кривій / О.О. Колеснікова, Є.М. Пірус, О.М. Рябухо // Збірник наукових праць фізико-математичного факультету СДПУ. — 2011. — Випуск 1. — С. 73–77.