Безущак О. О., Рябухо О. М., Сущанський В. І.

ТЕОРІЯ ҐАЛУА В МОНОГРАФІЧНОМУ ВИКЛАДІ ПРОФЕСОРА В. П. ЄРМАКОВА «АЛГЕБРАЇЧНІ РІВНЯННЯ, ЩО РОЗВ'ЯЗУЮТЬСЯ В РАДИКАЛАХ»

Проведено аналіз однієї з перших публікацій з теорії Ґалуа на теренах України – мемуарів професора Київського університету св. Володимира Василя Єрмакова про розв'язування алгебраїчних рівнянь у радикалах та порівняльний аналіз з іншими тогочасними працями відомих математиків, присвяченими теорії Ґалуа.

1. Вступ

Видатний український математик, член-кореспондент Петербурзької академії наук, професор Київського університету св. Володимира і Київського політехнічного інституту Василь Петрович Єрмаков (1845–1922) залишив після себе поважну наукову і науково-педагогічну спадщину. Мабуть, найбільш відомим із його наукових результатів є ознака збіжності й розбіжності знакосталих рядів, відкрита ним у 26-річному віці. Це один з потужних засобів дослідження рядів, який широко використовувався в працях багатьох математиків. Науковий інтерес до цього результату незмінно залишається на високому рівні, про що свідчать численні дослідження математиків різних країн, в яких використовується зазначена ознака. Найбільш цитованою на даний момент працею В. П. Єрмакова є стаття [1], результати і методи якої, а також уведені до неї поняття знайшли широке застосування у різних галузях теоретичної фізики: теорії узагальненої симетрії, теорії гравітації, теорії узагальнених осциляторів. Нині загальновживаними є такі поняття, як система диференціальних рівнянь Єрмакова (або Єрмакова – Кеплера), процедура Єрмакова – Левіса, інваріанти Єрмакова – Левіса, кути Єрмакова, які вперше було впроваджено в [1].

Більшість робіт В. П. Єрмакова стосується аналізу, теорії спеціальних функцій, теорії диференціальних рівнянь, варіаційного числення. Відомий він також своїми працями в галузі педагогіки математики, діяльністю на ниві популяризації математичних знань (див. [2]). Дещо осторонь, на перший погляд, від основних його зацікавлень стоять великі статті [3–5], опубліковані на межі XIX і XX століть в «Университетских відомостях», присвячені теорії Ґалуа. Проте, якщо помітити, що перед цим вийшли друком праці щодо розв'язання диференціальних рівнянь у квадратурах, які використовують апарат неперервних груп перетворень, розвинутих Софусом Лі, то зрозумілою стає закономірність зацікавлень В. П. Єрмакова новими досягненнями тогочасної алгебри.

У даній роботі ми проводимо докладний аналіз праць В. П. Єрмакова [3], [4], присвячених розв'язуванню алгебраїчних рівнянь у радикалах. Основну увагу при цьому буде звернено на оригінальність підходів В. П. Єрмакова, ті нові факти та ідеї, які запропоновано автором у цих працях. Крім того, ми хочемо показати, як саме вкладаються дослідження В. П. Єрмакова в контекст сучасної теорії Ґалуа. Тісно пов'язана з вищеназваними працями також праця В. П. Єрмакова [5], де досліджується загальний вигляд радикальних виразів, які при перестановках змінних набувають фіксованого числа значень. Проте цю працю ми не аналізуємо, оскільки основні її ідеї вже зустрічаються в [4].

§ 1. Теорія Ґалуа як вчення про відповідності між частково впорядкованими множинами

З точки зору сучасної математики теорія Ґалуа – це дисципліна, яка вивчає відповідності Ґалуа і їх застосування. Відповідність Ґалуа в найширшому розумінні цього слова визначається таким чином [6].

Нехай $(X_1,\le_1),(X_2,\le_2)$ – дві частково впорядковані множини. Пара відображень $\varphi: X_1 \to X_2$, $\psi: X_2 \to X_1$ називається відповідністю Галуа між $(X_1,\le_1)$ та $(X_2,\le_2)$, якщо виконано такі вимоги:

1. Відображення φ і ψ антитонними, тобто для довільних $x,y \in X_1$ (відповідно $u,v \in X_2$) з нерівності $x \le_1 y$ (відповідно $u \le_2 v$) випливає нерівність $\varphi(x) \ge_2 \varphi(y)$ (відповідно $\psi(u) \ge_1 \psi(v)$).

2. Для довільних елементів $x \in X_1$ та $y \in X_2$ мають місце нерівності $\psi(\varphi(x)) \ge_1 x$, $\varphi(\psi(y)) \ge_2 y$, де символом $\ge$ позначено відношення порядку, обернене до $\le$.

Елементи $\psi(\varphi(x))$ та $(\psi(y))$ називаються Галуа-замиканнями елементів $x \in X_1, y \in X_2$ відповідно. Елемент називається Галуа-замкненим, якщо він збігається зі своїм Галуа-замиканням. Відповідність Галуа (φ,ψ) називається повною, якщо відображення φ, ψ є взаємно оберненими бієкціями. Відповідності Галуа природним чином виникають у різних розділах універсальної алгебри, наприклад, у теорії реляційних і функціональних алгебр (клонів) [7], комбінаторному аналізі, теорії решіток [6] тощо. Класичний приклад відповідності Галуа, звідки, власне, і походить його назва, виник у теорії полів. А саме: нехай $K \subset L$ – скінченне (сепарабельне) розширення полів. Для довільного проміжного підполя $E, K \subseteq E \subseteq L$, символом $Gal(L/E)$ позначимо групу всіх автоморфізмів поля L, для яких E є полем нерухомих точок. Частково впорядковані (відповідним включенням) множини всіх проміжних підполів розширення і всіх підгруп групи $G = Gal(L/K)$ є гратками щодо дій перетину підполів чи, відповідно, підгруп та композиту підполів і, відповідно, підгруп. Позначимо ці ґратки символами $IF(L/K)$ та $SG(L/K)$ і покладемо для довільної підгрупи $H \in SG(L/K)$:

$$invH = \{x \in L \mid x^g = x \text{ для довільного } g \in H\}.$$

Позаяк $invH \in IF(L/K)$, то маємо два відображення:

$$\varphi: IF(L/K) \to SG(L/K), \psi: SG(L/K) \to IF(L/K),$$

що визначені рівностями:

а) $\varphi(E) = Gal(L/E), E \in IF(L/K)$,

б) $\psi(H) = Inv(H), H \in SG(L/K)$.

Основна теорема теорії Галуа говорить, що така пара відображень (φ,ψ) для довільного скінченного розширення $K \subset L$ є відповідністю Галуа. Якщо розширення сепарабельне, то ця відповідність є повною [8], [9]. Зазначимо, що для нескінчених розширень полів відповідності Галуа також визначаються, але тут уже доводиться працювати з проскінченними групами [10]. Наявність відповідності Галуа дає змогу характеризувати властивості розширень полів мовою теорії груп. Саме ця ідея і лежить в основі класичної теорії Галуа. А саме, нехай задано деяке рівняння з числовими коефіцієнтами

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0. \qquad (1)$$

Символом F позначимо його поле коефіцієнтів (тобто найменше за включенням числове поле, яке містить числа $a_0, a_1, \ldots, a_n$), а символом K – його поле розкладу (найменше розширення поля F, яке містить усі корені (1). Група автоморфізмів $Gal(F/K)$ називається групою Галуа рівняння (1). Критерій розв'язності рівняння (1) у радикалах (теорема Галуа) формулюється таким чином:

Рівняння (1) *розв'язується в радикалах тоді й лише тоді, коли його група Галуа є розв'язною групою.*

Наведене вище визначення групи Галуа рівняння (1) було впроваджене Кронекером. Сам Галуа визначав цю групу дещо інакше (хоча й у рівносильний спосіб) чином. Нехай $x_1^0, x_2^0, \ldots, x_n^0$ – корені рівняння (1). Раціональним співвідношенням між коренями називатимемо довільний многочлен $\varphi(x_1, x_2, \ldots, x_n)$ від n-змінних над полем F такий, що $\varphi(x_1^0, x_2^0, \ldots, x_n^0) = 0$. Усі раціональні співвідношення між коренями даного рівняння утворюють ідеал у кільці многочленів від змінних $x_1, x_2, \ldots, x_n$ над полем коефіцієнтів рівняння (1). Симетрична група S_n діє в кільці многочленів $F[x_1, x_2, \ldots, x_n]$ перестановками індексів:

$$\varphi(x_1, x_2, \ldots, x_n)^g = \varphi(x_{1g}, x_{2g}, \ldots, x_{ng}),$$
$$\varphi \in F[x_1, x_2, \ldots, x_n], \; g \in S_n \qquad (2)$$

(символом i^g позначається образ елемента i під дією перестановки g).

Групою Галуа рівняння (1) буде підгрупа симетричної групи S_n, яка складається з тих і тільки тих перестановок, що стабілізують при дії (2) множину всіх раціональних співвідношень між його коренями. Іншими словами, група Галуа рівняння (1) складається з тих перестановок елементів множини $\{1,2,\ldots,n\}$, для яких образ φ^g довільного раціонального співвідношення $\varphi(x_1, x_2, \ldots, x_n)$ між коренями (1) знову буде раціональним співвідношенням між цими коренями. При такому підході до визначення групи Галуа потрібно навчитися певним чином характеризувати множину всіх раціональних співвідношень між коренями рівняння. Один із природних методів характеризації полягає у побудові так званих основних модулів – спеціальної системи твірних ідеалу співвідношень (див. [11], с. 78–81). Хоча таке визначення групи Галуа рівняння є громіздкішим і його не так зручно використо-

вувати при побудові загальної теорії, воно дає більші можливості для обчислень при розгляді конкретних рівнянь і успішно використовується й понині. Відповідні дослідження в цьому напрямі спираються на монографію С. О. Шатуновського [12] і праці П. Мертенса (див., напр. [13]).

§ 2. Загальна характеристика праці В. П. Єрмакова

Стаття «Алгебраические уравнения, решаемые в радикалах» розбита на 55 параграфів. Перші два параграфи - вступні. У § 1, який затитуловано «В чому суть математики», автор коротко характеризує власні філософські погляди на природу математики, описує свій метод освоєння нових результатів, звертає увагу на важливість продуманого й опрацьованого викладу результатів досліджень, що не містив би в собі нічого зайвого. У другому параграфі «Передмова» автор характеризує основний об'єкт дослідження. Він пише: «В даному дослідженні подаються три поняття: перше - корінь рівняння, друге - незвідність рівняння, третє - радикал. Потрібно на підставі цих понять дати відповідь на питання: за яких умов корені алгебраїчного рівняння виражаються в радикалах. Задача по суті проста, а тому повинна мати просте розв'язання. Але, з іншого боку, ця задача є складною, тому що для свого розв'язання вимагає впровадження багатьох нових понять і визначень». Далі автор подає коротку історію розв'язування рівнянь у радикалах, згадуючи при цьому імена Лагранжа, Абеля, Ґауса. Особливо підкреслюється видатна роль у цих дослідженнях Евариста Ґалуа. В. П. Єрмаков пише, що посмертні мемуари Ґалуа було надруковано в «Journal de mathématique» тільки в 1846 р. З того часу дослідження Ґалуа постійно були предметом захоплення, і багато математиків працювали в цій галузі. «Проте в ясні ідеї Ґалуа пізніші дослідники внесли багато плутанини, багато непотрібного, так що питання до цього часу залишається в тумані і далеко не повністю розв'язане». Автор ставить перед собою такі шість завдань, дослідженню яких і присвячено праці [3], [4]:

1. Які умови є необхідними і достатніми для того, щоб алгебраїчне рівняння розв'язувалось у радикалах?

2. Пересвідчитись, що ці умови виконуються для рівнянь степеня <4.

3. Довести, що загальне рівняння степеня >5 не розв'язується у радикалах.

4. Як дізнатися, чи розв'язується дане рівняння у радикалах, чи ні?

5. Як знаходити корені рівнянь, які розв'язуються у радикалах?

6. Як описати загальний вигляд рівняння даного степеня, яке розв'язується у радикалах?

Автор вважає, що на час написання статті на перші три питання вже було дано задовільні відповіді. Що стосується останніх трьох питань, то задовільні відповіді на них було отримано тільки для рівнянь простого степеня. Виходячи з цього, В. П. Єрмаков ставить мету в своєму дослідженні дати відповіді на них, причому в якомога простішій формі та з використанням по можливості меншої кількості нових понять. Зміст праці, хоча й дещо умовно, можна розбити на такі частини:

(i) Елементарна теорія підстановок і груп підстановок;

(ii) Симетрії радикальних виразів;

(iii) Резольвенти Ґалуа і раціональні функції коренів рівняння;

(iv) Проблема розв'язності рівнянь в радикалах, загальний вигляд розв'язного в радикалах рівняння n-го степеня.

Насправді, чіткого поділу зробити не вдається, оскільки окремі параграфи, що належать до тієї чи іншої частини (i-iv), розташовано згідно з авторським задумом побудови дослідження в цілому, а він відображає фактичну послідовність міркувань автора.

§ 3. Коротка характеризація змісту основних частин

3.1. Теорія груп

У §§ 4–8 розглядається елементарна теорія підстановок: розклад підстановки на добуток циклів (які називаються круговими підстановками), порядок підстановки, обернена підстановка, спряжені підстановки та централізатор підстановки. В §§ 9–10 вводиться поняття групи підстановок, ізоморфізму груп, розкладу групи на класи суміжності за підгрупою та доводиться теорема Лагранжа. Всі інші теоретико-групові поняття і твердження вводяться далі в міру необхідності. Так, формулюючи критерій розв'язності алгебраїчного рівняння в радикалах, автор вводить поняття розв'язної групи (не використовуючи самого терміна «розв'язне»).

Здійснюється це в дуже оригінальний спосіб, який увійшов у теоретико-групову практику лише в середині 60-х років минулого століття у зв'язку з комп'ютерними застосуваннями в теоретико-групових дослідженнях. Звичайно, розв'язні групи визначаються як такі, що містять скінченний субнормальний ряд з абелевими факторами [14]. Еквівалентне визначення – це такі

групи, ряд комутантів яких має скінченну довжину і закінчується на одиничній підгрупі. Добре відомо також, що у випадку скінченних груп розв'язність рівносильна наявності в групі субнормального ряду, всі фактори якого є циклічними групами простих порядків. Саме останнє визначення розв'язності найчастіше використовується при викладі класичної теорії Ґалуа. У праці В. П. Єрмакова скінченні розв'язні групи визначаються як такі, що містять системи твірних зі спеціальними властивостями. А саме, скінченна розв'язна група G містить систему твірних $\{s_1, s_2, ..., s_n\}$ таку, що для довільного $k(2 \le k \le n)$ підстановка s_k комутує в цілому з підгрупою, породженою $s_1, s_2, ..., s_{k-1}$. Порядком твірного s_k автор називає найменше число m_k таке, що $s_k^{m_k} \in gp\{s_1, s_2, ..., s_{k-1}\}$. Якщо група G містить систему твірних вказаного типу, то будь-який елемент цієї групи можна подати у вигляді добутку $s_1^{\alpha_1} s_2^{\alpha_2} ... s_n^{\alpha_n}$, де $0 \le \alpha_i \le m_i, i = 1, 2, ..., n$. Слід зазначити, що такий спосіб характеризації скінченних розв'язних груп по суті був заново відкритий у [15]. У цій роботі описано комплекс алгоритмів і програм для поелементних обчислень у скінченних розв'язних групах. Для цього вводяться так звані AG-системи – групові системи твірних, які задовольняють певні додаткові вимоги. Система, що складається з n твірних $a_1, a_2, ..., a_n$ і $n(n-1)/2$ елементів g_{ij} ($i = 1, ..., j$ і $j = 1, ..., n$) називається AG-системою групи G, якщо вона задовольняє таким вимогам:

1) $g_{ij} \in U_{j-1} = gp\{e, a_1, ..., a_{j-1}\} \subseteq G$ $(1 \le i \le j \le n)$;

2) $a_j^{\psi_j} = g_{ij}, 1 \le j \le n$ (тут ψ_j – деяке натуральне число);

3) $[a_i, a_j] = g_{ij}, 1 \le i \le j \le n$ (тут $[x, y] = x^{-1}y^{-1}xy$ – комутатор елементів $x, y \in G$);

4) $a_i^{\tau} \in uU_{j-1}$ для $1 \le \tau \subset \psi, 1 \le j \le n$, і певного $u \in U_j, u \ne 1$.

Доводиться, що група G має AG-систему в тому й лише в тому разі, коли вона є скінченною розв'язною групою. Далі в [15] встановлюється, що елементи групи G можна записувати в певній нормалізованій формі, над якою здійснюються необхідні обчислення. За неістотними подробицями підхід статті [15] не відрізняється від запропонованого В. П. Єрмаковим, тобто по суті заново відкриває результати праці Єрмакова. Крім того, в Єрмакова є окремий параграф (§ 22), в якому описано правила заміни спеціальних систем твірних в скінченних розв'язних групах. Наведене визначення розв'язності В. П. Єрмаков використовує для побудови дуже простого доведення теореми Ґалуа про нерозв'язність симетричних груп степеня ≥5. Серед інших результатів теоретико-групового характеру, які наводяться в праці Єрмакова, – визначення транзитивних та інтранзитивних груп підстановок, виділення підкласу правильних нетранзитивних груп (тепер такі групи називаються напіврегулярними), опис методів побудови правильних транзитивних груп. Крім того, наведено характеризацію метациклічних груп – розв'язних груп підстановок простого степеня p. Уведено також поняття примітивних та імпримітивних груп, сформульовано й доведено важливу теорему про імпримітивність групи, яка містить правильний інтранзитивний нормальний дільник. Розглядається повна лінійна група довільної скінченної вимірності n над полем із p елементів, знайдено порядок цієї групи. Як її розширення охарактеризовано n-вимірну афінну групу над полем із p елементів.

3.2. Симетрії радикальних виразів

Особливістю підходу В. П. Єрмакова до викладу основних положень теорії Ґалуа є те, що він суттєво спирається на симетрійний аналіз радикальних виразів, тобто алгебраїчних чи арифметичних конструкцій, при побудові яких використовуються лише арифметичні дії та дії добування коренів. Спочатку розглядається (§ 3) проблема знаходження числа різних значень радикального виразу. Автор пише: «Вимагається знайти число значень такого виразу. Кожному радикалу можна надавати різні значення. Різні значення радикалу n-го порядку $\sqrt[n]{a}$ отримуються, якщо ми цей радикал множимо на $\theta, \theta^2, ..., \theta^{n-1}$, де θ є уявною одиницею порядку n, тобто первісним коренем рівняння $\theta^n = 1$. Кожне значення одного радикалу може комбінуватися з кожним значенням іншого радикалу; отже, число значень радикального виразу дорівнює добутку показників усіх радикалів. Але, діючи таким чином, ми можемо помилитися; часто число значень радикального виразу є меншим від добутку показників при всіх радикалах». Кількість значень радикального виразу залежить від того, при скількох перетвореннях, що зводяться до множення радикалів, які до нього входять, на корені відповідних степенів з 1, а вираз у цілому залишається незмінним. Якщо рівняння розв'язується в радикалах і його розв'язок подано у вигляді певного радикального виразу, то вказані перетворення цього виразу відповідають підстановкам із групи Ґалуа даного рівняння. Дослідження поведінки радикальних виразів при таких перетвореннях відіграють вирішальну роль у другій частині праці (§§ 31–55), яка присвячена вивченню рівнянь, що розв'язуються в радикалах. Тут описується загальна

форма радикального виразу простого степеня, загальний вигляд циклічного рівняння четвертого степеня, загальна форма радикального виразу, який при перестановках змінних набуває п'яти різних значень. Крім того, запропоновано метод обчислення кількості різних значень радикального виразу, який базується на понятті головного радикала (число значень радикального виразу дорівнює добутку порядків його головних радикалів), наводяться визначення правильних (у яких лише зовнішні радикали можуть бути головними) і неправильних радикальних виразів, характеризуються рівняння, які мають неправильні радикальні розв'язки. Закінчується стаття викладками стосовно загальної форми радикального виразу, який набуває восьми значень та загального вигляду рівняння п'ятого степеня, що розв'язується в радикалах. Зазначимо також, що в пізнішій публікації [5] Єрмаковим було знайдено загальні форми радикальних виразів, які при перестановках змінних набувають 3, 4, 5, 6, 7, 8 і 9 значень. Авторам даної статті невідомі роботи, в яких ці дослідження знайшли б продовження.

3.3. Група Ґалуа, резольвента Ґалуа

Побудова теорії Ґалуа в праці Єрмакова розпочинається з уведення поняття резольвенти Ґалуа даного рівняння. Нехай $f(x) = 0$ – незвідне рівняння степеня n. Розглянемо раціональну функцію коренів цього рівняння $U(x_1, x_2, ..., x_n)$, яка змінює свої значення при будь-якій перестановці коренів $x_1, x_2, ..., x_n$; число таких значень для заданих $x_1, x_2, ..., x_n$ дорівнює $n!$. Позначимо їх символами $u = u_0, u_1, ..., u_{n!-1}$ і розглянемо многочлен

$$F(z) = \prod_{i=0}^{n!-1} (z - u_i).$$

Рівняння $F(z) = 0$ має степінь $n!$, і одним з його коренів є $u(x_1, x_2, ..., x_n)$. Усі корені цього рівняння будуть симетричними функціями від коренів початкового рівняння, тобто за основною теоремою про симетричні многочлени і теоремою Вієта всі вони раціонально виражаються через корені рівняння $f(x) = 0$. Многочлен $F(z)$ не зобов'язаний бути незвідним. А тому, взагалі кажучи, число $u(x_1, x_2, ..., x_n)$ є коренем деякої незвідної (над полем коефіцієнтів многочлена $f(x)$) компоненти $h(x)$ многочлена $F(x)$. Рівняння $h(x) = 0$ (степеня $\le n!$) прийнято називати резольвентою Ґалуа рівняння $f(x) = 0$. Вигляд резольвенти Ґалуа залежить від вибору раціонального виразу $u(x_1, x_2, ..., x_n)$. Але всі резольвенти Ґалуа даного рівняння є многочленами одного й того ж степеня і мають однакові властивості, а саме:

1) корені резольвенти виражаються раціонально через корені даного рівняння;

2) корені даного рівняння виражаються раціонально через один і той же корінь резольвенти;

3) всі корені резольвенти виражаються раціонально через один з її коренів;

4) кожна перестановка коренів заданого рівняння $f(x) = 0$ або не змінює резольвенти, або переводить її в нову, яка не має з початковою спільних коренів.

З наведених властивостей випливає, що розв'язність чи нерозв'язність даного рівняння в радикалах рівносильна розв'язності чи нерозв'язності в радикалах його резольвенти. Хоча при цьому, як правило, зростає степінь рівняння, але таким чином все зводиться до дослідження рівнянь, усі корені яких раціонально виражаються через один із коренів. Відповідну задачу сформульовано в § 14 праці В. П. Єрмакова: «Дано алгебраїчне рівняння, всі корені якого виражаються раціонально через один корінь; за яких умов це рівняння розв'яжеться в радикалах?».

Він пише, що на це питання можна дати цілком визначену відповідь. «Якщо відомі функції, за допомогою яких всі корені виражаються через один корінь, то ми зможемо дати відповідь, розв'язується дане рівняння в радикалах чи ні. Вказані вище функції повинні мати певні властивості, щоб це рівняння розв'язувалось у радикалах». Нехай $f(x) = 0$ – дане рівняння, $F(z) = 0$ – його резольвента, $G = \{1, s_1, s_2, ..., s_{m-1}\}$ – група підстановок, яка відповідає цій резольвенті. Група G визначається таким чином. Нехай степінь $F(z)$ дорівнює $m, m \le n!$. Корені $z_0, z_1, ..., z_{m-1}$ резольвенти є раціональними функціями коренів $x_1, x_2, ..., x_n$ даного рівняння, тобто $z_i = u_i(x_1, x_2, ..., x_n), 1 \le i \le m$. Кожна з функцій u_i змінюється при будь-якій нетотожній перестановці коренів $x_1, x_2, ..., x_n$. Якщо здійснити таку перестановку, то отримаємо новий набір чисел $z'_0, z'_1, ..., z'_{m-1}$, які будуть коренями деякого рівняння $F'(z) = 0$. Многочлени $F(z)$ і $F'(z)$ або не мають спільних коренів, або збігаються, оскільки резольвента $F(z)$ за визначенням є незвідним многочленом. А тому кожна перестановка коренів рівняння $f(x) = 0$ або не змінює резольвенти Ґалуа, або переводить її в нову форму. Група G складається з тих перестановок коренів $x_1, x_2, ..., x_n$, які не змінюють резольвенти. Порядок цієї групи дорівнює степеню m резольвенти. Оскільки, за теоремою Лагранжа, порядок підгрупи є дільником порядку групи, а G ізоморфна деякій підгрупі симетричної групи степеня n, то звідси, зокрема, дістаємо, що m є дільником числа $n!$.

Корені резольвенти виражаються раціонально через один корінь, а тому вони можуть бути записані у вигляді

$$z, \varphi_1(z), \varphi_2(z), \ldots, \varphi_{m-1}(z).$$

При цьому функції є (тотожна), $\varphi_1, \varphi_2, \ldots, \varphi_{m-1}$ утворюють групу відносно суперпозиції, яка ізоморфна групі G.

3.4. Розв'язність рівнянь у радикалах

Зовнішнім радикалом деякого радикального виразу назвемо такий його радикал, який не міститься в цьому виразі під знаком (іншого) радикала. Ключовим моментом аналізу властивостей групи підстановок G, яка відповідає резольвенті, що розв`язується в радикалах, є таке твердження (§ 14):

Якщо резольвента Ґалуа даного рівняння $f(x) = 0$ розв'язується в радикалах, то в групі G є така підстановка, дія якої на корені рівняння рівносильна множенню одного із зовнішніх радикалів (у формулі розв'язків рівняння) на корінь μ-го степеня з одиниці, де μ – степінь цього радикала.

За допомогою цього твердження далі в §14 доводиться, що група Ґалуа рівняння, яке розв'язується в радикалах, мусить мати спеціальну систему твірних (точніше кажучи, певну AG-систему), тобто бути розв'язною. Після деякої підготовчої роботи в § 21 доводиться, що в разі, коли група Ґалуа даного рівняння є розв'язною, степінь його резольвенти можна понизити, долучаючи до поля коефіцієнтів нові числа, які є значеннями певних радикальних виразів від коефіцієнтів рівняння. Звідси відразу дістаємо, що умова розв`язності групи Ґалуа рівняння є й достатньою для розв`язності його в радикалах. Довівши відповідну теорему, автор пише: «Проте не досить встановити, що рівняння розв`язується в радикалах; потрібно ще вказати правила для знаходження якомога простішої форми розв`язку в радикалах». З цією метою в § 22 аналізуються правила заміни спеціальних систем твірних у розв`язних групах, які можна використати для спрощення, твірних підстановок групи, що відповідає резольвенті Ґалуа, до випадку простих показників. Випадок незвідного рівняння простого степеня проаналізовано досить докладно, зокрема охарактеризовано можливі типи груп (так звані метациклічні групи), які можуть бути групами Ґалуа таких рівнянь. Після такого аналізу охарактеризовано алгоритм побудови загального розв`язку в радикалах рівняння простого степеня p, група Ґалуа яких є циклічною групою підстановок степеня p, або метациклічною групою, і описано загальну форму радикальних виразів простого степеня. Розвинута теорія застосовується в конкретних випадках для рівнянь малих степенів. Так, у § 36 охарактеризовано загальний вигляд рівняння четвертого степеня з циклічною групою Ґалуа, в § 37 – загальну форму радикального виразу, що набуває п`яти різних значень, а в § 54 – загальну форму рівняння п`ятого степеня, яке розв'язується в радикалах. А саме, кожне рівняння п`ятого степеня, яке розв'язується в радикалах, має вигляд

$$x^5 - 10Ax^3 - 10Bx^2 - 5Cx - D = 0,$$

де коефіцієнти A, B, C, D певним чином залежать від чотирьох параметрів. Випадок, коли A, B дорівнюють нулеві, є особливо простим, рівняння тоді матиме вигляд

$$x^5 + \frac{5\cdot(h+3)\cdot p^4}{h^2+16}\cdot x + \frac{(22-h)\cdot p^5}{h^2+16} = 0,$$

де h, p – певні числові параметри.

Для аналізу розв'язності в радикалах рівнянь складеного степеня автор вводить поняття примітивності та імпримітивності рівнянь. А саме, рівняння $f(x) = 0$ степеня $n = k \cdot l$ називається імпримітивним, якщо многочлен $f(x)$ розкладається на добуток k множників вигляду

$$f(x) = \varphi(x, y_1)\varphi(x, y_2)\ldots\varphi(x, y_k),$$

де $y_1, y_2, \ldots, y_k$ – корені незвідного рівняння $g(x) = 0$ степеня k, коефіцієнти якого виражаються раціонально через коефіцієнти початкового рівняння. В такому разі розв`язування рівняння $f(x) = 0$ зводиться до розв`язування рівняння $g(x) = 0$, а згодом – кожного з рівнянь

$$\varphi(x, y_i) = 0, i = 1, 2, \ldots, k.$$

Якщо ж такого розкладу для многочлена $f(x) = 0$ не існує, то рівняння $f(x) = 0$ називається примітивним. У § 39 праці Єрмакова поняття примітивності рівняння пов'язується з відповідною властивістю групи підстановок, що відповідає його резольвенті Галуа. А саме, доводиться, що рівняння буде примітивним в тому і лише в тому разі, коли його група Галуа є примітивною. Розроблено процедуру зведення задачі знаходження розв'язків неприміти вного рівняння до примітивного випадку. Після цього проведено аналіз радикальних виразів, які відповідають випадкам примітивних та імпримітивних рівнянь (так звані правильні та неправильні радикальні вирази). Розвинута в такий спосіб техніка застосовується до дослідження задачі розв`язності в радикалах рівнянь, степені яких є вільними від квадратів числами, та рівнянь, степені яких є прімарними числами. В останньому випадку важливу роль відіграє вираження коренів рівняння через так

званні циклічні функції – спеціальні многочлени, які не змінюються при циклічних перестановках змінних, та метациклічні функції – многочлени, які інваріантні щодо метациклічної групи. У § 52 доведено таку важливу теорему: *Корені даного рівняння прімарного степеня виражаються у радикалах через корені рівняння нижчого степеня тоді й лише тоді, коли яка-небудь метациклічна функція коренів цього рівняння виражається раціонально через його коефіцієнти.*

У результаті дістаємо певну загальну схему дослідження рівнянь із числовими коефіцієнтами на предмет їх розв'язності чи нерозв'язності в радикалах. У деяких ситуаціях ця схема «спрацьовує» досить добре, але при аналізі різних класів рівнянь можуть виникати значні труднощі.

§ 4. Праця В. П. Єрмакова в контексті тогочасної літератури з теорії Ґалуа

На час виходу друком праці В. П. Єрмакова теорія Ґалуа була розвинутою математичною дисципліною, яка вже вийшла з рамок, намічених її творцем. Проблема розв'язності рівнянь у радикалах поступово перестала бути центральною в алгебрі, але методи теорії Ґалуа ще довго відігравали в ній головну роль. Ідеї теорії Ґалуа не лише використовувались для розв'язання інших алгебраїчних проблем, але й проникли в інші розділи математики, як-от диференціальні рівняння, теорію автоморфних функцій, алгебраїчну теорію чисел тощо. Відповідно до нових сфер застосувань змінюється сама термінологія теорії Ґалуа: основними її об'єктами стають уведені Кронекером поняття поля, розширення полів і автоморфізмів поля. Дослідженням з теорії Ґалуа на той час уже було присвячено десятки статей різних авторів, кілька відомих монографій. Вона ввійшла також як один з основних розділів до ряду університетських підручників з алгебри, найбільш відомими з яких були фундаментальний тритомник Г. Вебера [16] та підручник Е. Нетто [17], а серед російськомовних видань – підручник професора Київського університету М. Є. Ващенка-Захарченка [18]. А тому на перший погляд праця В. П. Єрмакова може здатися просто епігонською спробою автора заявити про себе, та ще й у такій важливій ділянці математики. Насправді це не так. Швидкий розвиток наукової дисципліни далеко не завжди супроводжується упорядкуванням її початкових засад, вони можуть ще досить довгий час не викликати зацікавлення дослідників. Розвиток теорії Ґалуа йшов шляхом можливих узагальнень. В. П. Єрмаков поставив собі задачу – максимально спростити виклад теорії в її початковому варіанті. Хоча завдання це більше науково-методичного характеру, але при написанні праці автору довелося розв'язати кілька суто математичних проблем, найцікавішою з яких, на наш погляд, є нова характеризація скінченних розв'язних груп у термінах спеціальних систем твірних. У цілому ж робіт такого типу на той час було порівняно небагато. Серед них – ряд дисертацій, зокрема магістерська дисертація харківського математика, пізніше професора Харківського університету Д. М. Деларю (1839–1905) під назвою «Загальна теорія алгебраїчного розв'язування рівнянь» (Харків, 1864). У цій дисертації (обсягом 114 сторінок, тобто вона задовольняла б навіть вимоги ВАК України, хоча тоді ще нікому не приходило в голову оцінювати дисертації «на вагу») було розглянуто історію проблеми розв'язування рівнянь у радикалах, наведено найважливіші твердження теорії Ґалуа і розглянуто теорію абелевих (в сучасній термінології – циклічних) рівнянь. У цій праці ставилася задача лише викласти основи на той час ще зовсім нової теорії. Ніяких новацій немає також у відповідному розділі цитованого вище підручника Ващенка-Захарченка. Проведений нами аналіз інших аналогічних публікацій [19], [20] дає підстави стверджувати, що підхід В. П. Єрмакова, де основну роль відіграють спеціальні системи твірних у скінченних розв'язних групах, є цілком новим і оригінальним.

Це не означає, що праця В. П. Єрмакова позбавлена недоліків. Найголовнішим із них є те, що симетрійний аналіз радикальних виразів здійснюється не на належному рівні строгості. У деяких випадках загальні положення лише ілюструються відповідними (гарно підібраними) прикладами, а їх доведення залишається за кадром. Хоч а насправді такі доведення не є простими, а їх формалізація вимагає чималих зусиль. Незважаючи на це, праця В. П. Єрмакова має неперехідне наукове значення, тим більше, що ряд цікавих ідей, які в ній висвітлено, так і не дістали продовження в подальших працях фахівців із теорії Ґалуа. На жаль, пройшла ця праця практично не поміченою. Систематичні дослідження з теорії Ґалуа розпочато в Київському університеті на десятиліття пізніше в школі професора Д. Граве. На свого попередника представники цієї школи не посилалися. Єдине цитування праці В. П. Єрмакова з дуже побіжним оглядом її змісту автори знайшли у великому історичному огляді розвитку алгебраїчних досліджень у Росії професора А. К. Сушкевича [21].

§ 5. Деякі висновки

Праця В. П. Єрмакова «Алгебраїчні рівняння, що розв'язуються в радикалах» є цілісним науковим дослідженням, в якому запропоновано нові підходи до побудови теорії Ґалуа. Підходи В. П. Єрмакова вигідно вирізняються своєю елементарністю й економністю в сеансі запроваджуваних понять. Їх особливістю є також цілком алгоритмізований підхід до викладення теорії: значну увагу автор звертає на характеризацію редукційних процедур, на основі яких порівняно легко можуть бути укладені відповідні алгоритми. Так, у праці докладно описано процедуру зведення процесу розв'язування (в радикалах) алгебраїчних рівнянь з імпримітивною групою Ґалуа до примітивних рівнянь. Менш докладно, але досить змістовно охарактеризовано також процедуру зведення рівнянь довільного степеня до розгляду рівнянь прімарних степенів. Описано також схему побудови загального рівняння довільного степеня, яке розв'язується в радикалах. В такому рівнянні існує велика кількість залежностей між його коефіцієнтами, і побудова рівняння зводиться до характеризації таких залежностей. У праці воно повністю реалізоване для рівнянь п'ятого степеня: виписано загальний вигляд такого рівняння, наведений нами вище. Таким чином, праця В. П. Єрмакова виявилася значною мірою скерованою в напрямі, який нині розвинувся у велику самостійну галузь досліджень, що дістала назву алгоритмічної теорії Ґалуа.

1. *Добровольский В. А.* Василий Петрович Ермаков, 1845–1922.– М.: Наука, 1981.– 165 с.
2. *Ермаков В. П.* Дифференциальные уравнения второго порядка. Условия интегрируемости в конечном виде // Университетские известия.– 1880.– № 9.– С. 1–25.
3. *Ермаков В. П.* Алгебраические уравнения, решаемые в радикалах // Университетские известия.– 1901.– № 5.– С. 1–65.
4. *Ермаков В. П.* Алгебраические уравнения, решаемые в радикалах // Университетские известия.– 1901.– № 6.– С. 65–101.
5. *Ермаков В. П.* Общая форма радикального выражения имеющего 3, 4, 5, 6, 7, 8 и 9 решений // Университетские известия.– 1901.– № 10.– С. 1–36.
6. *Айгнер М.* Комбинаторная теория.– М.: Мир, 1982.– 556 с.
7. *Pöschel R., Kaluzhnin L.* Functionen- und Relationenalgebren // Deutscher Verlag d.Wiss. Berlin und Birkhauser Verlag Basel und Stuttgart (Math. Reihe Bd. 67).– 256 s.
8. *Артин Е.* Теорія Галуа.– К.: Радянська школа, 1963.– 98 с.
9. *Дрозд Ю.* Теорія Галуа.– К.: РВЦ «Київського університету», 1997.– 35 с.
10. *Ван дер Варден Б. Л.* Алгебра.– М.: Наука, 1979.– 624 с.
11. *Чеботарев Н. Г.* Основы теории Галуа.– М.: ОНТИ и ГТТИ, 1934.– Т. 1.– 219 с.
12. *Шатуновский С.О.* Алгебра как учение о сравнениях по функциональным модулям.– Одесса: Изд-во Новороссийского ун-та, 1917.
13. *Mertens P* . Ein Beweis des Galois'schen Fundamentalsatzes. Sitzber. Wiener Akad., 111 (1902).
14. *Jürgencen H.* Calculation with the elements of finite groups given by generators and defining relations in Computational Problems in Abstract Algebra, Pergamon Press, 1970, pp. 47–57. Переклад російською в кн.: Вычисления в алгебре и теории чисел / Під редакцією Б. Б. Генкова и О. К. Фадеєва.– М.: Мир, 1976.– С. 32–46.
15. *Weber H.* Algebra, Bd I, II, III.– Braunschweig, 1898–1903.
16. *Netto E.* Algebra, Bd. I, II.– Leipzig: Teubner, 1898, 1900.
17. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп.– 3-е изд.– М.: Наука, 1982.– 288 с.
18. *Ващенко-Захарченко М. Е.* Высшая алгебра.– К.: Изд-во Киевского университета, 1890.
19. *Jordan C.* Commentaire sur Galois // Math. Ann., 1 (1869), pp. 141–160.
20. *Pierpoint J.* Galois theory of algebraic equations // Ann. of Math. 1 (1899/1900).– № 1–4.– PP. 113–143.

O. Bezushchak, O. Ryabukho, V. Sushchanskii

GALOIS THEORY IN MONOGRAPH OF PROFESSOR V. P. ERMAKOV «ALGEBRAIC EQUATIONS, WHICH IS PROVED IN RADICALS»

One of the first papers of Galois theory in Ukraine, the monograph on decision of algebraic equations in radicals by Vasil Ermakov, professor of Kiev St. Vladimir University, is analyzed. We also perform the comparison this monograph with others papers of that time famous mathematicians which is devoted Galois theory.