Национальная академия наук Беларуси
Труды Института математики НАН Беларуси. 2025. Том 33. № 1. С. 20–27

УДК 511.2

НЕРАЗВЕТВЛЕННЫЕ РАСШИРЕНИЯ ГАЛУА И ПОДГРУППЫ GL_n

Д. А. Малинин

Институт математики НАН Беларуси, Минск, Беларусь
e-mail: dmalinin@gmail.com

Поступила: 14.01.2025 **Исправлена:** 27.01.2025 **Принята:** 23.05.2025

Ключевые слова: неразветвленные расширения Галуа, действие Галуа, конечные устойчивые подгруппы GL_n.

Аннотация. Мы рассматриваем естественное действие групп Галуа неразветвленных расширений Галуа числовых полей на конечных устойчивых при действии группы Галуа подгруппах GL_n.

UNRAMIFIED GALOIS EXTENSIONS AND SUBGROUPS OF GL_n

D. A. Malinin

Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus
e-mail: dmalinin@gmail.com

Received: 14.01.2025 **Revised:** 27.01.2025 **Accepted:** 23.05.2025

Keywords: unramified Galois extensions, Galois action, Galois stable finite subgroups of GL_n.

Abstract. We consider the natural action of Galois groups of unramified Galois extensions of number fields on finite Galois stable subgroups of GL_n.

1. Введение

Существование глобальных полей с заданной группой Галуа для разных классов групп, а также с предписанными локальными свойствами для ветвления возникает в связи с различными вопросами теории чисел. В связи с этим можно отметить, к примеру, работы [1] и [2].

В этой статье мы рассматриваем некоторое неразветвленное расширение Галуа E/F конечной степени d с группой Галуа Γ для числовых полей E и F, и конечной абелевой подгруппой $G \subset \subset GL_n(E)$ заданной экспоненты t, где мы предполагаем, что G устойчива относительно естественного коэффициентного Γ-действия.

В данной работе O_K обозначает максимальный порядок числового поля K, а $F(G)$ обозначает поле, которое получается присоединением к F всех матричных коэффициентов всех матриц $g \in G$.

Основная цель данной статьи – доказать существование абелевых Γ-устойчивых подгрупп $G \subset \subset GL_n(R)$ для заданного n и заданного показателя t группы G (R обозначает некоторые дедекиндовы подкольца E, но наиболее интересным случаем является $R = O_E$) таких, что $F(G) = E$ обеспечивает некоторые разумные ограничения для фиксированного нормального расширения E/F и целые числа n, t, d остаются верными. Установлена нижняя граница для возможных степеней n представлений G: $n \geqslant C = C(E,F,d,t,h)$ такая, что $\phi_E(t)d \leqslant C \leqslant \phi_E(t)dh$, где h – показатель группы классов поля F; $\phi_E(t) = [E(\zeta_t) : E]$ – обобщенная функция Эйлера для поля E (ζ_t обозначает примитивный t-корень из 1). Также доказано, что в некоторых случаях верхняя граница улучшаема (теорема 1, части 1), 3), 4)), хотя нижняя граница $C = \phi_E(t)d \leqslant n$ не может быть улучшена (предложение 2).

Эти результаты имеют некоторые приложения к конечным арифметическим группам, их когомологиям и положительно определенным квадратичным решеткам над кольцами целых чисел в полях вполне вещественных чисел (см. [3–5]), например, обобщенный «принцип Хассе»: для арифметических групп G определенного типа ($G_{\mathbb{R}}$ является компактной), вполне вещественного $K/\mathbb{Q}$ и $Gal(K/\mathbb{Q})$-устойчивой подгруппы G_{O_K} из $GL_n(O_K)$ ядро естественного отображения когомологий $H^1(Gal(K/\mathbb{Q}), G_{O_K}) \to \prod_v H^1(Gal(K_v/\mathbb{Q}_v), G_v)$ тривиально. Некоторые результаты, связанные с устойчивостью Галуа для порядков в конечномерных алгебрах, можно найти в [6]. Явная конструкция вполне вещественных неразветвленных расширений полей полезна в этой ситуации. Некоторые интересные конструкции неразветвленных и вполне вещественных (а также мнимых)

числовых полей получены в статьях [7–10], см. также [11]; некоторые компьютерные вычисления с использованием KANT и PARI могут быть полезны для этой цели (см., например, [8; 10]). Другая конструкция вполне вещественных неразветвленных расширений, имеющих заданную группу Галуа, приведена в теореме 3.

Статья организована следующим образом. Формулировки результатов приведены в разделе 2, разделы 3, 4, 5 посвящены их доказательствам.

Большинство символов и обозначений, которые мы используем в этой статье, являются традиционными. $\mathbb{Q}$ и $\mathbb{Q}_p$ обозначают поле рациональных чисел и p-адических рациональных чисел. $\mathbb{Z}$ и $\mathbb{N}$ обозначают кольцо рациональных целых чисел и натуральных чисел, $\mathbb{R}$ и $\mathbb{C}$ обозначают поля действительных и комплексных чисел. $GL_n(R)$ обозначает общую линейную группу над R. Мы пишем $[E:F]$ для степени расширения поля E/F. Максимальный порядок числового поля K обозначается O_K. В этой статье мы пишем Γ для групп Галуа, $\sigma, \gamma \in \Gamma$ для элементов Γ. Мы пишем ζ_t для примитивного t-корня из 1, $\phi_K(t) = [K(\zeta_t) : K]$ обозначает обобщенную функцию Эйлера для поля K, I_m обозначает единичную $(m \times m)$-матрицу, $\det M$ является определителем матрицы M. Если G – конечная линейная группа, $F(G)$ обозначает поле, полученное присоединением к F всех матричных коэффициентов всех матриц $g \in G$. Для Γ, действующего на G, и любых $\sigma \in \Gamma$ и $g \in G$ мы пишем g^σ для образа g под действием σ. K^Γ обозначает подполе Γ-устойчивых элементов поля K, $\dim_K A$ обозначает размерность K-алгебры A над полем K, $M_n(R)$ – полную матричную алгебру над R.

2. Результаты

Пусть E обозначает конечное расширение поля алгебраических чисел F, отличное от F. Пусть O'_E обозначает пересечение колец нормирования всех разветвленных простых идеалов в кольце O_E, и пусть $O'_F = F \cap O'_E$.

Поскольку кольца O'_E и O'_F полулокальны, известно, что они являются областями главных идеалов.

Теорема 1. *Пусть $d > 1, t > 1$ будут заданы рациональные целые числа, и пусть E/F будет нормальным неразветвленным расширением полей алгебраических чисел степени d с группой Галуа* Γ.

1) *Если $n \geqslant \phi_E(t)d$, существует конечная абелева* Γ*-устойчивая подгруппа $G \subset GL_n(O'_E)$ экспоненты t такая, что $E = F(G)$.*

2) *Если $n \geqslant \phi_E(t)dh$ и h – показатель группы классов группы F, существует конечная абелева* Γ*-устойчивая подгруппа $G \subset GL_n(O_E)$ показателя t такая, что $E = F(G)$.*

3) *Если $n \geqslant \phi_E(t)d$ и h взаимно просты с n, то G, указанная в* 1)*, сопряжена в $GL_n(F)$ с подгруппой группы $GL_n(O_E)$.*

4) *Если d нечетно, то G, заданная в* 1)*, сопряжена в $GL_n(F)$ с подгруппой в $GL_n(O_E)$.*

Во всех приведенных выше случаях G может быть построена как группа, порожденная матрицами $g^\gamma, \gamma \in \Gamma$ для некоторого $g \in GL_n(E)$.

Результаты, связанные с устойчивостью Галуа конечных групп в ситуациях, подобных нашей, возникают в теории определенных квадратичных решеток, арифметических групп и когомологий Галуа. Точнее, пусть E – вполне вещественное числовое поле, H – алгебраическая подгруппа в $GL_n(\mathbb{C})$, определенная над подполем F в E. Если H определена в следующем смысле: вещественная группа Ли $H(\mathbb{R})$, подгруппа $\mathbb{R}$-точек, компактна, то подгруппа $H(O_E)$ O_E-точек H является конечной Γ-устойчивой подгруппой, и последнее условие имеет некоторые интересные следствия ([3; 4; 12], см. также [13]). Эти результаты также тесно связаны с некоторыми аспектами целочисленных представлений конечных групп, см. [4; 14; 15]. В нашем контексте мы изучаем, можно ли реализовать заданное поле E, нормальное над F, как поле $E = F(G)$ в обоих случаях $G \subset GL_n(O'_E)$ и $G \subset GL_n(O_E)$, и если это так, каковы возможные порядки n матричных реализаций и структура G.

Теорема 1 дает положительный ответ на вопрос: можно ли реализовать любое нормальное неразветвленное расширение числового поля E/F как $E = F(G)$ для некоторого $G \subset GL_n(O_E)$ при условии $n \geqslant \phi_E(t)dh$. Мы доказываем, что любое конечное нормальное расширение поля E/F может быть получено как $F(G)/F$, если $n \geqslant \phi_E(t)d$ для некоторого $G \subset GL_n(E)$. Фактически, мы строим некоторые алгебры Галуа в смысле [16] и устанавливаем нижние границы для их возможных размерностей n. В предложении 2 доказано, что ограничения для заданных целых чисел n, t и d в теореме 1 не могут быть улучшены.

Предложение 2. *Пусть E/F – заданное нормальное расширение полей алгебраических чисел с группой Галуа Γ, $[E:F]=d$, и пусть $G\subset GL_n(E)$ – конечная абелева Γ-устойчивая подгруппа экспоненты t такая, что $E=F(G)$ и n – минимально возможное. Тогда $n=d\phi_E(t)$ и G неприводима относительно сопряжения в $GL_n(F)$. Более того, если G имеет минимально возможный порядок, то G – группа типа $(t,t,...,t)$ и порядка t^m для некоторого положительного целого числа $m\leqslant d$.*

Условия следующей теоремы рассматривались Л. Море-Байи [7] в более общей ситуации. В общем случае существование глобальных полей с заданной группой Галуа и предписанными локальными свойствами для ветвления является довольно тонким вопросом. Л. Море-Байи доказал существование относительных расширений числовых полей с заданной локальной структурой ветвления над заданным множеством простых делителей и неразветвленных в других местах. Однако наша конструкция в теореме 3 дает вполне вещественные неразветвленные расширения более явным и простым способом.

Теорема 3. *Для данной конечной группы Γ существует бесконечно много нормальных неразветвленных расширений вполне вещественных полей E/F, имеющих группу Галуа Γ.*

3. Доказательство теоремы 1

Доказательство теоремы 1. Для любого расширения числового поля L/L_1 оба кольца O'_L и O'_{L_1} являются полулокальными, поэтому они являются кольцами главных идеалов, и O'_L имеет базис над O'_{L_1}. Начнем с доказательства 1). Для заданного базиса $w_1,w_2,...,w_n$ из O'_E над O'_F мы намерены построить матрицу $g=[g_{ij}]_{i,j}=\sum_{i=1}^d B_iw_i$ и попарно коммутирующие матрицы B_i таким образом, чтобы нормальное замыкание поля $F(g_{11},g_{12},...,g_{nn})$ над F совпадало с E и, таким образом, группа G, порожденная $g^\sigma,\sigma\in\Gamma$, является абелевой Γ-устойчивой группой экспоненты t. Во-первых, мы определяем собственные значения, которые должны иметь матрицы B_i, если g имеет заданный набор собственных значений. Собирая заданные собственные значения попарно коммутирующих полупростых матриц и используя регулярное представление, мы строим Γ-устойчивую абелеву группу G для целых параметров, указанных в предложении.

Доказательство 1) используется в доказательстве остальной части теоремы. Фактически, некоторые результаты из теории представлений порядков в полупростых алгебрах (см. [17, § 75]) применяются к порядку $D=O_F[B_1,B_2,\dots,B_d]\subset A$ внутри F-алгебры $A=F[B_1,B_2,\dots,B_d]$. Утверждения 2), 3) и 4) заключаются в том, что конструкция представления G, заданная в 1), может быть реализована над O_E без использования целочисленного базиса O'_E над O'_F (в общем случае кольцу O_E не требуется базис над O_F). Этого можно достичь, используя теорему Штейница–Шевалле для модулей над кольцами Дедекинда, которая применяется к порядку D или прямой сумме его копий, а также один результат Шура для 3) и результат, доказанный Фрелихом [18] для 4).

Доказательство 1). В нашем доказательстве мы рассматриваем два разных случая.

Случай 1. Мы предполагаем, что $F(\zeta_t)$ и E линейно не пересекаются над F и $[E:F]=d$. В этом случае $\phi_E(t)=\phi_F(t)$. Пусть $w_1=1,w_2,...,w_d$ будет базисом O'_E над O'_F, и пусть Γ будет группой Галуа $E(\zeta_t)$ над $F(\zeta_t)$. Пусть g будет полупростой $(d\times d)$-матрицей с собственными значениями $\zeta_t,1,...,1$. Используя разложение $g=B_1+w_2B_2+...+w_dB_d$, мы можем построить матрицы $B_i,i=1,2,...,d$, и мы можем доказать, что группа G, порожденная $g^\gamma,\gamma\in\Gamma$, является абелевой Γ-устойчивой группой экспоненты t. Рассмотрим матрицу $W=[w_i^{\sigma_j}]_{i,j}$ для $\{\sigma_1=1,\sigma_2,...,\sigma_d\}=\Gamma$. Поскольку E/F неразветвлен, $\det W$ является единицей O'_E. Обозначим через W_i матрицу W, i-й столбец которой заменен на d выбранных собственных значений $\zeta_t,1,...,1$ g. Мы можем вычислить

$$\lambda_i=\frac{\det W_i}{\det W}$$

и построить матрицы B_i как регулярное представление $B_i=R(\lambda_i)$ $\lambda_i\in O'_E[\zeta_t]$ в базисе $w_1,w_2,\dots,w_d$ расширения кольца $O'_E[\zeta_t]\supset O'_F[\zeta_t]$, которое получается путем присоединения ζ_t к основному кольцу. Пусть α_{ij} будут коэффициентами обратной матрицы $W^{-1}=[\alpha_{ij}]_{i,j}$. Тогда $\alpha_{i1}^{\sigma_j}=\alpha_{ij}$ и $\lambda_i=(\zeta_t-1)\alpha_{i1}$ для $i\neq1$, и $\lambda_1=1+(\zeta_t-1)\alpha_{11}$. Так что $\lambda_i^{\sigma_j}=(\zeta_t-1)\alpha_{i1}^{\sigma_j}=(\zeta_t-1)\alpha_{ij}$ для $i\neq1$, и $\lambda_1^{\sigma_j}=(\zeta_t-1)\alpha_{11}^{\sigma_j}+1=(\zeta_t-1)\alpha_{1j}+1$. Поскольку любое линейное отношение

$$k_1(\lambda_1-1)+\sum_{i=2}^d k_i\lambda_i=0,\quad k_i\in F(\zeta_t),\quad i=1,2,...,d$$

подразумевает линейное отношение

$$k_1(\lambda_1^{\sigma_j}-1)+\sum_{i=2}^{d}k_i\lambda_i^{\sigma_j}=0,\quad k_i\in F(\zeta_t),\quad i=1,2,...,d$$

для всех $\sigma_j\in\Gamma$, это также означало бы $\det W^{-1}=0$, что невозможно. Следовательно, λ_1-1, $\lambda_2,...,\lambda_d$ генерируют поле $E(\zeta_t)$ над $F(\zeta_t)$, и поэтому $B_1-I_d,B_2,...,B_d$ генерируют $F(\zeta_t)$-диапазон $F(\zeta_t)[B_1,...,B_d]$ над $F(\zeta_t)$.

Обратите внимание, что B_i можно выразить как линейную комбинацию g^{σ_i}, $i=1,2,...,d$, с коэффициентами в E: $B_i=\sum_{j=1}^{d}\alpha_{ij}g^{\sigma_j}$. Это можно получить из системы матричных уравнений

$$g^{\sigma_j}=\sum_{i=1}^{d}w_i^{\sigma_j}B_i,\quad j=1,2,...,d,$$

если рассматривать B_i как неопределенности. Поскольку G имеет показатель t, $F(\zeta_t)$ является полем расщепления для G, группы, порожденной всеми $g^{\sigma},\sigma\in\Gamma$. Следовательно, размерность $E(\zeta_t)$-пространства $E(\zeta_t)G=E(\zeta_t)\otimes_{F(\zeta_t)}F(\zeta_t)G$ над $E(\zeta_t)$ равна d, и поэтому размерность $F(\zeta_t)$-пространства $F(\zeta_t)G$ также равна d.

Обозначим через E' образ $E(\zeta_t)$ при регулярном представлении $E(\zeta_t)$ над $F(\zeta_t)$ в базисе $w_1,\dots,w_d$. Тогда $A=E(\zeta_t)G=E(\zeta_t)\otimes_{F(\zeta_t)}F(\zeta_t)G$, $E(\zeta_t)$-оболочка G является E'-алгеброй Галуа в смысле [16], т. е. это ассоциативная и коммутативная отделимая E'-алгебра, имеющая нормальный базис. Мы можем выбрать идемпотенты

$$\varepsilon_i=\frac{1}{\zeta_t-1}(g^{\sigma_j}-I_d),\quad j=1,2,...,d,$$

как нормальный базис A над E', так что $\varepsilon_j=\varepsilon_1^{\sigma_j}$.

У нас есть $F(\zeta_t)G=F(\zeta_t)[<g^{\sigma_1},...,g^{\sigma_d}>]=F(\zeta_t)[(g-I_d)^{\sigma_1},...,(g-I_d)^{\sigma_d}]$, и $\dim_{F(\zeta_t)}F(\zeta_t)G=$ $=d$. Поскольку длина орбиты $M=[m_{ij}]=(g-I_d)$ под действием Γ равна d, мы можем использовать коэффициенты матриц $M^{\sigma_i},i=1,2,...,d$, чтобы построить элемент $\theta=\sum_{i,j}k_{ij}m_{ij},k_{ij}\in F(\zeta_t)$, который генерирует нормальный базис $E(\zeta_t)/F(\zeta_t)$. Следовательно, для любого заданного $\alpha\in E(\zeta_t)$ мы имеем $\alpha=\sum_i k_i\theta^{\sigma_i}$ для некоторого $k_i\in F(\zeta_t)$.

Следовательно, наш выбор собственных значений подразумевает, что $F(\zeta_t)(G)=E(\zeta_t)$.

Теперь мы можем применить регулярное представление R_F матрицы $O'_F[\zeta_t]$ над O'_F к матрицам $M=[m_{ij}]_{i,j}$, $m_{ij}\in O'_F[\zeta_t]$ следующим образом: $R_F(M)=[R_F(m_{ij})]_{i,j}$. Таким образом, используя R_F для всех компонентов матриц $B_i\in M_n(F(\zeta_t))$, мы можем получить абелеву подгруппу $G\subset$ $\subset GL_{n_1}(E),n_1=[F(\zeta_t):F]d$ экспоненты t, которая Γ-устойчива, если мы определим изоморфные группы Галуа расширений E/F и $E(\zeta_t)/F(\zeta_t)$. Мы снова имеем $\dim_F FG=\dim_E EG$, E снова является алгеброй Галуа, и $F(G)=E$. Теперь, используя естественное вложение G в $GL_n(E),n\geqslant n_1$, мы завершаем доказательство теоремы 1 в случае 1).

Случай 2. В силу случая 1 мы можем рассмотреть случай, когда пересечение $F_0=E\cap F(\zeta_t)\neq$ $\neq F$. Мы можем использовать регулярное представление R O'_E над O'_F. Пусть $\Gamma_0=\{\sigma'_1,\sigma'_2,...,\sigma'_d\}$ будет множеством некоторых расширений элементов $\Gamma=\{\sigma_1,\sigma_2,...,\sigma_d\}$ до $E(\zeta_t)/F$, и пусть $w_1=$ $=1,w_2,...w_d$ будет базисом O'_E над O'_F. Итак, мы можем использовать наши предыдущие обозначения и применить аналогичный аргумент, как в случае 1 доказательства, для построения $g=\sum_{i=1}^{d}B_iw_i$ и матриц B_i как регулярных представлений R_0 собственных значений

$$\lambda_i=\frac{\det W_i}{\det W}=\sum_{j=1}^{\phi_E(t)}\lambda_{ij}\zeta^j,\quad i=1,2,...,d,$$

следующим образом: мы рассматриваем

$$B_i=R_0(\lambda_i)=\sum_{j=1}^{\phi_E(t)}R(\lambda_{ij})\zeta^j,$$

где R – регулярное представление O'_E над O'_F. Мы также имеем $\lambda_1^{\sigma'_j}=\alpha_{1j}+1,\lambda_i^{\sigma'_j}=\alpha_{ij}$ для $j=2,...,d$. Теперь, если у нас есть какая-либо линейная связь между строками матрицы $[\alpha_{ij}(\zeta_t^{\sigma'_j}-1)]_{i,j}$, это

будет означать линейную связь между ее столбцами, и поэтому столбцы $W^{-1} = [\alpha_{ij}]$ линейно зависимы, и $\det W^{-1} = 0$, что является противоречием. Итак, снова получаем, что $\lambda_1 - 1, \lambda_2, ..., \lambda_d$ линейно независимы над F, поэтому $\dim_F FG' = \dim_F F[B_1 - I_d, B_2, ..., B_d] = \dim_E EG' = d$ для G', порожденного $g^{\sigma'_i}, i = 1, 2, ..., d$. Как и ранее, мы можем рассмотреть регулярное представление $R_E(B_i)$ для коэффициентов матриц B_i в расширении кольца $O'_E[\zeta_t] \supset O'_E$. Итак, получаем $g_0 = \sum_{i=1}^{d} R_E(B_i) w_i$, и можем взять группу G, порожденную всеми $g_0^{\sigma_i}, i = 1, 2, ..., d$. Так как $[E(\zeta_t) : F] = [E(\zeta_t) : E][E : F] = \phi_E(t)d$, то порядок $n = \phi_E(t)d$ совпадает с целым числом, требуемым в формулировке теоремы 1. Таким образом, мы можем построить Г-стабильную группу G, удовлетворяющую условиям 1) в теореме 1.

Доказательство 2). Рассмотрим O_F-порядок $D = O_F[B_1, B_2, \ldots, B_d] \subset A$ в полупростой F-алгебре $A = F[B_1, B_2, \ldots, B_d]$, где B_i – это $(n' \times n')$-матрицы, взятые из 1). Используя нашу конструкцию B_i, мы можем предположить $n' = \phi_E(t)d$. Пусть M будет соответствующим модулем представления в n'-мерном F-векторном пространстве V. Мы утверждаем, что матрицы B_i из 1) могут быть реализованы над O_F путем взятия прямой суммы h копий O_F-модуля M. Мы можем использовать теорему Штейница–Шевалле (см., например, [17]) для M, чтобы получить разложение: $M = v_1\mathfrak{O}_\mathfrak{F} + \mathfrak{v}_2\mathfrak{O}_\mathfrak{F} + \cdots + \mathfrak{v}_{n'-1}\mathfrak{O}_\mathfrak{F} + \mathfrak{v}_{n'}\mathfrak{a}O_F$ для некоторых элементов $v_1, v_2, \ldots, v_{n'} \in V$ и некоторого дробного идеала $\mathfrak{a}$ множества O_F. Взяв прямую сумму $M_1 = \oplus M$ h копий M, мы заключаем, что класс Штейница M_1 равен $\mathfrak{a}^h$, поэтому он тривиален, и M_1 становится свободным O_F-модулем: $M_1 = c_1O_F + c_2O_F + \cdots + c_{hn'}O_F$ для некоторых элементов $c_1, c_2, \ldots, c_{hn'} \in FM_1$. Следовательно, матрицы $B'_1 = \oplus_1^h B_1, B'_2 = \oplus_1^h B_2, \ldots, B'_d = \oplus_1^h B_d$ (h копий B_i) $GL_n(F)$-сопряжены к матрицам, содержащимся в $GL_{hn'}(O_F)$ (мы можем рассмотреть $n = hd\phi_E(t)$ на мгновение, а затем распространить результат на любые $n \geqslant hd\phi_E(t)$, взяв прямые суммы). Мы можем заключить, что все матрицы $g^\sigma, \sigma \in \in \Gamma$ также сопряжены в $GL_n(F)$ с матрицами, содержащимися в $GL_n(O_E)$. Поскольку G порождается этими матрицами, мы получаем утверждение 3) для матриц порядка $hd\phi_E(t)$. Для распространения этого результата на произвольные $n \geqslant hd\phi_E(t)$ мы можем зафиксировать положительные целые числа k и r с $n = khd\phi_E(t) + r, r < hd\phi_E(t)$ и взять прямую сумму k копий построенной реализации G и r копий единичных представлений. Это завершает доказательство 2).

Доказательство 3). Это следует из утверждения (75.5) в [17], примененного к порядку $D = O_F[B_1, B_2, \ldots, B_d] \subset A$ в F-алгебре $A = F[B_1, B_2, \ldots, B_d]$. Так как все матрицы $B_i, i = 1, 2, \ldots, d$, сопряжены в $GL_n(F)$ с матрицами, содержащимися в $GL_n(O_F)$ (здесь можно рассмотреть $n = d\phi_E(t)$), то мы заключаем, что все матрицы $g^\sigma, \sigma \in \Gamma$, также сопряжены в $GL_n(F)$ с матрицами из $GL_n(O_E)$. Так как G порождается этими матрицами, то получаем утверждение 3).

Доказательство 4). По [18], теореме 4.3, в любом нормальном неразветвленном расширении числовых полей нечетной степени кольцо целых чисел имеет свободный базис. В нашем случае $O_E = w_1O_F + w_2O_F + \cdots + w_dO_F$ для некоторых $w_1, w_2, \ldots, w_d$. Поэтому матрицы B_i, $i = 1, 2, \ldots, d$, сопряжены в $GL_n(F)$ матрицам из $GL_n(O_F)$, и наш аргумент 1) может быть непосредственно применен к кольцам O_E и O_F вместо O'_E и O'_F. Это означает, что G сопряжена в $GL_n(F)$ подгруппе $GL_n(O_E)$, как и утверждалось.

Это завершает доказательство теоремы 1.

4. Доказательство предложения 2

Доказательство предложения 2. Мы можем использовать доказательство теоремы 1.

Пусть $G \subset GL_n(E)$ – группа, заданная в формулировке предложения 2, и пусть n – минимально возможное. Тогда мы имеем следующее разложение E-оболочки $A = EG$:

$$A = \varepsilon_1 A + \varepsilon_2 A + ... + \varepsilon_k A$$

для некоторых примитивных идемпотентов $\varepsilon_1, ..., \varepsilon_k$ группы A. ε_i сопряжены под действием группы Галуа $\Gamma = \{\sigma_1, ..., \sigma_d\}$. Ибо если сумма $\varepsilon_i^{\sigma_j}, j = 1, 2, ..., d$, не равна I_n, то $I_n = e_1 + e_2$ для $e_1 = \varepsilon_1^{\sigma_1} + \\ + ... + \varepsilon_1^{\sigma_d}$ и $e_2 = I_n - e_1$, и e_1, e_2 фиксируются Γ, так что e_1, e_2 сопряжены в $GL_n(F)$ до диагональной формы. Поскольку любой из 2 компонентов e_iG имеет ранг меньше n, существует матричная группа, удовлетворяющая условиям предложения 2 степени меньше n.

Следовательно, $\varepsilon_i = \varepsilon_1^{\sigma_i}$, $k = d$ и идемпотенты $\varepsilon_1, ..., \varepsilon_d$ образуют нормальный базис A. Но ранг матрицы ε_i не меньше, чем $\phi_E(t)$. Действительно, ε_iG содержит элемент $\varepsilon_i g$, для некоторого

$g \in G$ порядка t такого, что $(\varepsilon_i g)^t = \varepsilon_i$, но $(\varepsilon_i g)^k \neq \varepsilon_i$ для $k < t$. Мы можем найти $g \in G$ следующим образом. Так как $I_n = \varepsilon_1 + ... + \varepsilon_k$ для любого $h \in G$ порядка t существует ε_j такой, что $(\varepsilon_j h)^t = \varepsilon_j$, но $(\varepsilon_j h)^k \neq \varepsilon_j$ для $k < t$, и то же свойство выполняется для $\varepsilon_j h$ с любым $\sigma \in \Gamma$. Тогда, используя свойство нормального базиса $\varepsilon_k = \varepsilon_1^{\sigma_k}$, мы можем взять $g = h^{\sigma_j^{-1}\sigma_i}$.

Таким образом, неприводимая компонента $\varepsilon_i G$ определяет точное неприводимое представление циклической группы, порожденной g. Но если $T : C \to GL_r(E)$ является точным неприводимым представлением циклической группы C, порожденной элементом g порядка t, то его степень r равна $\phi_E(t)$. Из этого следует, что ранг матриц ε_i равен $\phi_E(t)$. Таким образом, размерность A над E равна $\phi_E(t)d$.

Если G порождается g^γ, $\gamma \in \Gamma$, и его порядок минимален, Γ-устойчивость подразумевает, что g имеет d сопряженных относительно Γ-действия, и поэтому G является абелевой группой экспоненты t и порядка t^m для некоторого положительного целого числа $m \leqslant d$. Это завершает доказательство предложения 2.

5. Доказательство теоремы 3

Доказательство теоремы 3. Во-первых, будет построено вполне вещественное расширение $L/\mathbb{Q}$ степени n. Для этой цели мы можем зафиксировать простые числа q_1, q_2, q_3 таким образом, что q_1 и a являются взаимно простыми, и выбрать многочлен $H(x) = (x - a_1 q_1)(x - a_2 q_2)\dots(x - - a_n q_n) + aq_1$, группа которого имеет транспозицию и один или 2 множителя нечетной степени по модулю q_2, $(n-1)$-цикл по модулю q_3 для целых чисел a_i, достаточно больших по сравнению с $|q_1 a|$ и малых по сравнению с $|a_i - a_j|, i \neq j$, таких, что все корни $H(x)$ являются действительными. Поле расщепления $H(x)$ вполне действительно, а его группа Галуа является симметрической группой S_n. Следовательно, L имеет подполе L степени n над $\mathbb{Q}$.

Зафиксируем множество R всех простых чисел, разветвленных в $L/\mathbb{Q}$.

Рассмотрим следующие условия:

1) $F(x) = (x - b_1 p_1)(x - b_2 p_1)\dots(x - b_n p_1) + p_1 b$;

2) $b_1, b_2, \dots, b_n \in \mathbb{Z}$ различны, и p_1 не делит b; $2bn < (\prod_{j=1(j\neq i)}^n |b_i - b_j|) p_1^{n-2}$ для $i = 1, \dots, n$;

3) $F(x)$ имеет транспозицию и 1 или 2 множителя нечетной степени по модулю p_2;

4) $F(x)$ имеет $(n-1)$-цикл по модулю p_3;

5) p_1, p_2, p_3 – простые числа, не содержащиеся в $R \cup q$, а $q \notin R$ – простое число, сравнимое с 1 по модулю n.

Условия 1) и 2) гарантируют неприводимость $F(x)$, поскольку $F(x)$ – многочлен Эйзенштейна, а также все корни $F(x)$ действительны. Действительно, коэффициент при x^{n-1} в $x^n F(1/x + b_i p_1)$ равен $\prod_{j=1(j\neq i)}^n (b_i p_1 - b_j p_1)$. Следовательно, для корней $x_1, x_2, \dots, x_n$ уравнения $F(x)$ справедливо следующее равенство:

$$\left| \frac{1}{x_1 - b_i p_1} + \frac{1}{x_2 - b_i p_1} + \dots \frac{1}{x_n - b_i p_1} \right| = \left| \frac{\prod_{j=1(j\neq i)}^n |b_i p_1 - b_j p_1|}{b p_1} \right|,$$

и поэтому

$$|x_{k_i} - b_i p_1| \leqslant \frac{nbp_1}{\prod_{j=1(j\neq i)}^n |b_i p_1 - b_j p_1|}$$

при условии $|x_{k_i} - b_i p_1| \leqslant |x_j - b_i p_1|$ для всех $j \neq k_i$.

Теперь, если $2nbp_1 < \prod_{j=1(j\neq i)}^n |b_i p_1 - b_j p_1|$, то $|x_{k_i} - b_j p_1| \leqslant \frac{1}{2}$, и все корни x_{k_i} содержатся в окружностях радиуса $\frac{1}{2}$ с различными центрами $b_j p_1$, поэтому среди x_{k_i} нет комплексно сопряженных.

Условия 3) и 4) подразумевают совпадение группы Галуа $F(x)$ и симметрической группы S_n.

Из теоремы плотности Фробениуса ([19], см. также [20], теорема 42) следует, что заданный многочлен имеет ту же факторизацию, соответствующую перестановке заданного типа цикла по модулю бесконечного числа простых чисел. Следовательно, существует целое число M, не делящееся на p_1, p_2, p_3, q и простые числа из R, такое, что сравнение

6) $f(x) \equiv F(x) (\mathrm{mod} M)$ влечет, что группа Галуа $f(x)$ равна S_n.

Пусть K будет полем разложения $f(x)$. Тогда q-круговое поле $\mathbb{Q}(\zeta_q)$ имеет подполе степени n над $\mathbb{Q}$, которое может быть определено как поле разложения целочисленного многочлена $k(x)$. По лемме Краснера существует $t_1 \in \mathbb{N}$ такое, что сравнения

7) $f(x) \equiv H(x)(\mathrm{mod} p^{t_1})$ для всех $p \in R$ подразумевают совпадение локализаций: $L\mathbb{Q}_p = K\mathbb{Q}_p$ для $p \in R$. Если максимальное абелево подполе K_{ab} поля K не является $\mathbb{Q}$, то $K_{ab} = \mathbb{Q}(\sqrt{r})$ для некоторого $r \in \mathbb{Z}$, и для достаточно большого целого числа t_2 сравнение

8) $f(x) \equiv k(x)(\mathrm{mod} q^{t_2})$ подразумевает $K \cap L = \mathbb{Q}$, рассматривая разветвление в q. Но составной KL не разветвлен над K, потому что $L\mathbb{Q}_p = K\mathbb{Q}_p$ для всех простых чисел p, разветвленных в L.

Мы можем найти многочлен $f(x)$, удовлетворяющий условиям 1)–8), так что его корни действительны, согласно 2). Действительно, используя теорему о слабой аппроксимации (или китайскую теорему о напоминании), мы можем удовлетворить 1) и 3)–8), и в факторизации $f(x) = (x-c_1)(x-c_2)\dots(x-c_n)+c_0\ c_i$ можно увеличить, добавив несколько кратных модулей сравнений 3)–8), чтобы сделать $c_i, i = 1, \dots, n$, достаточно большим по сравнению с c_0 и малым по сравнению с $|c_i - c_j|, i \neq j\ (i, j \neq 0)$. Следовательно, поля $E = LK$ и K вполне вещественны, а расширение E/K неразветвлено, нормально, и его группа Галуа равна S_n. По теории Галуа, для заданной конечной группы $\Gamma \subset S_n$ (для подходящего n) существует нормальное подрасширение E/F, где $F = E^{\Gamma}$ является подполем Γ-неподвижных элементов E, которое также неразветвлено и имеет Γ в качестве группы Галуа. Это замечание завершает доказательство теоремы 3.

Автор благодарен рецензенту за полезные замечания, которые способствовали улучшению работы.

Работа поддержана Институтом математики НАН Беларуси в рамках задания 1.1.01 государственной программы научных исследований «Конвергенция–2025».

Литература

1. *Harbater D.* Galois groups with prescribed ramification // Contemporary Math. 1994. Vol. 174. P. 35–60.

2. *Ozaki Manabu.* Construction of maximal unramified p-extensions with prescribed Galois groups // Invent math. 2011. Vol. 183. P. 649–680.

3. *Bartels H.-J.* Zur Galoiskohomologie definiter arithmetischer Gruppen // J. reine angew. Math. 1978. Vol. 298. P. 89–97.

4. *Малинин Д. А.* Целочисленные представления конечных групп, устойчивые при действии группы Галуа // Алгебра и анализ. 2000. Т. 12, № 3. С. 106–145.

5. *Малинин Д. А.* Целочисленные представления конечных групп с действием Галуа // Докл. РАН. 1996. Т. 349, № 3. С. 303–305.

6. *Ritter J., Weiss A.* Galois action on integral representations // J. London Math. Soc. (2). 1992. Vol. 46. P. 411–431.

7. *Moret-Bailly L.* Extensions de corps globaux a ramification et groupe de Galois donnes // C. R. Acad. Sci. Paris, Serie 1. 1990. Vol. 311. P. 273–276.

8. *Maire Ch.* On infinite unramified extensions // Pacific J. Math. 2000. Vol. 192, N 1. P. 135–142.

9. *Kondo T.* Algebraic number fields with the discriminant equal to that of quadratic number field // J. Math. Soc. Japan. 1995. Vol. 47, N 1. P. 31–36.

10. *Yamamura K.* Maximal unramified extensions of imaginary quadratic fields of small conductors // Journal de Theorie des Nombres de Bordeaux. 1997. Vol. 9. P. 405–448.

11. *Pohst M.* Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper // J. Reine angew. Math. 1975. Vol. 278/279. P. 278–300.

12. *Bartels H.-J., Kitaoka Y.* Endliche arithmetische Untergruppen der GL_n // J. reine angew. Math. 1980. Vol. 313. P. 151–156.

13. *Rohlfs J.* Arithmetische definierte Gruppen mit Galois-operation // Invent. Math. 1978. Vol. 48. P. 185–205.

14. *Малинин Д. А.* О целочисленных представлениях p-групп над локальными полями // Докл. АН СССР. 1989. Т. 309, № 5. С. 1060–1063.

15. *Малинин Д. А.* Целочисленные представления p-групп заданного класса нильпотентности над локальными полями // Алгебра и анализ. 1998. Т. 10, № 1. С. 58–67.

16. *Ишханов В. В., Лурье Б. Б., Фаддеев Д. К.* Задача погружения в теории Галуа. М.: Наука, Гл. ред. физ.-мат. лит., 1990.

17. *Curtis C. W., Reiner I.* Representation theory of finite groups and associative algebras. New York: Interscience, 1962.

18. *Fröhlich A.* Discriminants of algebraic number fields // Math Zeitschr. 1960. Vol. 74. P. 18–28.

19. *Frobenius G.* Über Beziehungen zwischen den Primidealen eines algebraischen Zahlkörpers und den Substitutionen seiner Gruppe. Sitzber: Preussen Akad. Wiss., 1896. S. 689–705.

20. *Чеботарев Н. Г.* Основы теории Галуа. Ч. 2. ОГИЗ: Ленинград–Москва, 1937.

References

1. Harbater D. Galois groups with prescribed ramification. *Contemporary Math.*, 1994, vol. 174, pp. 35–60.

2. Ozaki Manabu. Construction of maximal unramified p-extensions with prescribed Galois groups. *Invent math.*, 2011, vol. 183, pp. 649–680.

3. Bartels H.-J. Zur Galoiskohomologie definiter arithmetischer Gruppen. *J. reine angew. Math.*, 1978, vol. 298, pp. 89–97.

4. Malinin D. A. Galois stability for integral representations of finite groups *St. Petersburg Math. J.*, 2000, vol. 12, no. 3, pp. 106–145.

5. Malinin D. A. Integral representations of finite groups with Galois action. *Dokl. Russ. Akad. Nauk*, 1996, vol. 349, no. 3, pp. 303–305.

6. Ritter J.,Weiss A. Galois action on integral representations. *J. London Math. Soc. (2)*, 1992, vol. 46, pp. 411–431.

7. Moret-Bailly L. Extensions de corps globaux a ramification et groupe de Galois donnes. *C. R. Acad. Sci. Paris, Serie 1*, 1990, vol. 311, pp. 273–276.

8. Maire Ch. On infinite unramified extensions. *Pacific J. Math.*, 2000, vol. 192, no. 1, pp. 135–142.

9. Kondo T. Algebraic number fields with the discriminant equal to that of quadratic number field. *J. Math. Soc. Japan*, 1995, vol. 47, no. 1, pp. 31–36.

10. Yamamura K. Maximal unramified extensions of imaginary quadratic fields of small conductors. *Journal de Theorie des Nombres de Bordeaux*, 1997, vol. 9, pp. 405–448.

11. Pohst M. Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper. *J. Reine angew. Math.*, 1975, vol. 278/279, pp. 278–300.

12. Bartels H.-J., Kitaoka Y. Endliche arithmetische Untergruppen der GL_n. *J. reine angew. Math.*, 1980, vol. 313, pp. 151–156.

13. Rohlfs J. Arithmetische definierte Gruppen mit Galois-operation. *Invent. Math.*, 1978, vol. 48, pp. 185–205.

14. Malinin D. A. Integral representations of p-groups over local fields. *Sov. Math. Dokl.*, 1990, vol. 40, no. 3, pp. 619–622.

15. Malinin D. A. Integral representations over local fields for p-groups of a given class of nilpotency. *St. Petersburg Math. J.*, 1998, vol. 10, no. 1, pp. 58–67.

16. Ishkhanov V. V., Lur'e B. B., Faddeev D. K. *The embedding problem in Galois theory*. Moscow, Nauka, 1990.

17. Curtis C. W., Reiner I. *Representation theory of finite groups and associative algebras*. New York, Interscience, 1962.

18. Fröhlich A. Discriminants of algebraic number fields. *Math Zeitschr.*, 1960, vol. 74, pp. 18–28.

19. Frobenius G. *Über Beziehungen zwischen den Primidealen eines algebraischen Zahlkörpers und den Substitutionen seiner Gruppe*. Sitzber, Preussen Akad. Wiss., 1896, s. 689–705.

20. Chebotarev N. G. *Foundations of Galois theory, Part II.* Noordhoff, 1950 (in German).