LMD mokslo darbai, 55–60
1998, Vilnius

О группах Галуа p-расширений с двумя критическими точками

Г. Маркшайтис (ВУ)

Обозначим через $\mathcal{K}_p(q_1, q_2, \ldots, q_r)$ класс конечных нормальных расширений K поля рациональных чисел $\mathbb{Q}$, степени которых являются степенями простого числа p и дискриминанты которых делятся только на простые числа $q_1, q_2, \ldots, q_r$. Простое число q, делящее дискриминант некоторого конечного расширения K поля рациональных чисел $\mathbb{Q}$, называется точкой ветвления или критической точкой поля K. Обозначим через $K_p(q_1, q_2, \ldots, q_r)$ композит всех полей K, принадлежащих классу $\mathcal{K}_p(q_1, q_2, \ldots, q_r)$. Поле $K_p(q_1, q_2, \ldots, q_r)$ называется максимальным p-расширением поля рациональных чисел $\mathbb{Q}$ с критическими точками (или точками ветвления) $q_1, q_2, \ldots, q_r$.

Группа Галуа $G_p(q_1, q_2, \ldots, q_r)$ поля $K_p(q_1, q_2, \ldots, q_r)$ над полем рациональных чисел $\mathbb{Q}$ определяется как проективный предел

$$G_p(q_1, q_2, \ldots, q_r) = \varprojlim_{K \in \mathcal{K}_p(q_1, q_2, \ldots, q_r)} G(K/\mathbb{Q})$$

групп Галуа $G(K/\mathbb{Q})$ полей $K \in \mathcal{K}_p(q_1, q_2, \ldots, q_r)$. Конечные группы Галуа $G(K/\mathbb{Q})$ полей $K \in \mathcal{K}_p(q_1, q_2, \ldots, q_r)$ наделяются дискретной топологией.

По определению проективного предела, $G_p(q_1, q_2, \ldots, q_r)$ является замкнутой подгруппой прямого произведения

$$\prod_{K \in \mathcal{K}_p(q_1, q_2, \ldots, q_r)} G(K/\mathbb{Q}),$$

и наделяется индуцированной топологией. Группа $G_p(q_1, q_2, \ldots, q_r)$, будучи замкнутой подгруппой компактной топологической группы, – компактна. Так определена группа Галуа $G_p(q_1, q_2, \ldots, q_r)$ поля $K_p(q_1, q_2, \ldots, q_r)$ над полем рациональных чисел $\mathbb{Q}$ является топологической p-группой.

Основная задача о p-расширениях состоит в выяснении строения групп Галуа $G_p(q_1, q_2, \ldots, q_r)$.

Будем пользоваться следующими обозначениями. Для любой группы G индуктивно определим следующие подгруппы:

$$G^{(0)} = G^{(0, p^m)} = G, \quad G^{(n)} = [G, \ G^{(n-1)}], \quad G^{(n, p^m)} = G^{p^m}[G, G^{(n-1, p^m)}], \quad n \geq 1, \quad m \geq 1,$$

где через G^{p^m} обозначена подгруппа группы G, порожденная p^m степенями элементов группы G, $[G, \ H]$ – подгруппа группы G, порожденная коммутаторами $[x, y]$ элементов $x \in G$ и $y \in H$.

Топологические p-группы, как и абстрактные группы, могут быть заданы образующими и соотношениями между образующими. Минимальное число образующих группы Галуа $G_p(q_1, q_2, \ldots, q_r)$ по теореме Бернсайда [см. 10] равно минимальному числу образующих группы

$$G_p(q_1, q_2, \ldots, q_r)/(G_p(q_1, q_2, \ldots, q_r))^{(1,p)}$$

или, иначе говоря, равно числу независимых абелевых полей степени p над полем $\mathbb{Q}$ с критическими точками $q_1, q_2, \ldots, q_r$. По теореме Кронекера–Вебера [см. 9] число таких полей равно числу таких q_j, $1 \leq j \leq r$, которые удовлетворяют одному из условий: $q_j \equiv 1 (\mathrm{mod}\, p)$ или $q_j = p$. Следовательно, если предположим, что критические точки q_j, неравные p, удовлетворяют условию $q_j \equiv 1 (\mathrm{mod}\, p)$, то минимальное число образующих группы Галуа $G_p(q_1, q_2, \ldots, q_r)$ равно r. Минимальное число соотношений между образующими группы $G_p(q_1, q_2, \ldots, q_r)$ по теореме Шафаревича [см. 8] равно r, если p не является точкой ветвления поля $K_p(q_1, q_2, \ldots, q_r)$ и равно $r - 1$, если p является точкой ветвления этого поля.

Группа Галуа $G_p(q_1, q_2, \ldots, q_r)$ полностью определена только в некоторых случаях. Известны группы Галуа p-расширений с одним критическии числом [см. 7]. Из работы Фрелиха [см. 3] известна структура группы

$$G_p(q_1, q_2, \ldots, q_r)/(G_p(q_1, q_2, \ldots, q_r))^{(2)}.$$

Бровкиным доказано [см. 1], что в случае $p > 2$, $q_j \equiv 1 (\mathrm{mod}\, p)$, $q_j \not\equiv 1 (\mathrm{mod}\, p^2)$, $j = 1, 2$, $q_1 \not\equiv x^p (\mathrm{mod}\, q_2)$, группа $G_p(q_1, q_2)$ конечна и определена образующими σ, τ, которые связаны соотношениями: $\sigma^{p^2} = 1$, $\tau^p = 1$, $\tau\sigma = \sigma^{1+p}\tau$. Кохом исследован случай $q_1 \equiv q_2 \equiv 1 (\mathrm{mod}\, p)$, $q_1 \not\equiv 1 (\mathrm{mod}\, p^2)$, $q_2 \not\equiv 1 (\mathrm{mod}\, p^2)$, и каждое из чисел q_1 и q_2 является p-степенью классов вычетов по модулю другого [см. 4, 5]. В зависимости от некоторых параметров им определены группы

$$G_p(q_1, q_2)/(G_p(q_1, q_2))^{(3,p)} \quad \text{и} \quad G_p(q_1, q_2)/(G_p(q_1, q_2))^{(4,p)}.$$

В частности доказана конечность группы $G_3(79, 97)$. Другие примеры можно найти в книге Коха [см. 6].

Самый простой неизвестен случай группы Галуа максимального p-расширения $K_p(p, q)$ с двумя точками ветвления p и q, удовлетворяющими условиям:

$$q \equiv 1 (\mathrm{mod}\, p^2), \quad q \not\equiv 1 (\mathrm{mod}\, p^3).$$

Группа Галуа $G_p(p, q)$ такого расширения порождена двумя образующими σ и τ, которые связаны единственным соотношением. Соотношение между образующими σ и τ известно лишь по модулю $G_p(p, q)^{(2)}$. Оно имеет следующий вид:

$$\sigma^{q-1} = [\tau^p, \sigma] = [\tau, \sigma]^p (\mathrm{mod}\, G_p(p, q)^{(2)}).$$

Окончательный вид соотношения неизвестен. В случае

$$q \equiv 1 (\mathrm{mod}\, p), \quad q \not\equiv 1 (\mathrm{mod}\, p^2)$$

вид соотношения между образующими σ и τ группы $G_p(p, q)$ по модулю группы $G_p(p, q)^{(2)}$ следующий:

$$\sigma^{q-1} = [\tau, \sigma](\mathrm{mod}\, G_p(p, q)^{(2)}).$$

По теореме Демушкина [см. 2], в группе Галуа $G_p(p, q)$ можно выбрать другие образующие (их опять обозначим через σ и τ) так, чтобы соотношение между ними имело вид

$$\sigma^{q-1} = [\tau, \sigma]$$

в групе $G_p(p, q)$.

В этой работе рассмотрим пример, когда $p = 3$, $q = 19$. В этом случае вычислим вид соотношения между образующими τ и σ группы $G_3(3, 19)$ по модулю $G_3(3, 19)^{(3)}$. Полное обоснование проводимых в рассматриваемом примере вычислений будет приведено в статье, которая готовится к печати.

Пусть $p = 3$, $q = 19$. Группу Галуа максимального 3-расширения $\mathbb{Q}_S$ поля рациональных чисел $\mathbb{Q}$ с двумя точками ветвления 3 и 19 обозначим G_S, где $S = \{3, 19\}$.

Подгруппе $G_S^{(1)}$ по основной теореме теории Галуа соответсвует максимальное абелево 3-расширение $\mathbb{Q}_S^{(1)}$ поля рациональных чисел $\mathbb{Q}$ с двумя точками ветвления 3 и 19. По теореме Кронекера-Вебера [см. 9], поле $\mathbb{Q}_S^{(1)}$ является композитом максимального 3-подполя поля $\mathbb{Q}(\mu_{19})$ степени 9 над полем $\mathbb{Q}$, где μ_{19} – первообразный корень 19 степени из единицы, и поля $\cup_{j=1}^{\infty} L_j$, где L_j максимальное 3-подполе поля $\mathbb{Q}(\mu_{3^{j+1}})$, где $\mu_{3^{j+1}}$ – первообразный корень 3^{j+1} степени из единицы. Следовательно, группа Галуа поля $\mathbb{Q}_S^{(1)}$ над полем $\mathbb{Q}$ изоморфна прямому произведению циклической группе 9-ого порядка Z_9 и циклической топологической 3-группе, изоморфной аддитивной группе целых 3-адических чисел $\mathbb{Z}_3$. Пусть $\bar{\tau}$ – образующая группы Z_9, $\bar{\sigma}$ – образующая группы $\mathbb{Z}_3$. Выберем элементы τ и σ группы G_S, которые при естественном гомоморфизме $G_S \to G_S/G_S^{(1)}$ переходят в $\bar{\tau}$ и $\bar{\sigma}$. По теореме Бернсайда, элементы τ и σ порождают группу G_S. Кроме того образующие элементы τ и σ группы G_S по теореме Фрелиха можно выбрать так, чтобы соотношение между ними по модулю $G_S^{(2)}$ виглядлядело следующим образом:

$$\sigma^9 = [\tau, \sigma]^3(\mathrm{mod}\, G_S^{(2)}).$$

На роль группы разложения простого дивизора числа 19 в поле, соответствующем согласно теории Галуа подгруппе $G_S^{(2)}$, претендуют следующие три подгруппы группы G_S по модулю $G_S^{(2)}$:

$$\{\sigma G_S^{(2)}, \tau^3 G_S^{(2)}\}, \quad \{\sigma G_S^{(2)}, \tau^3 z G_S^{(2)}\}, \quad \{\sigma G_S^{(2)}, \tau^3 z^2 G_S^{(2)}\}.$$

Здесь, например, обозначение

$$\{\sigma G_S^{(2)}, \tau^3 G_S^{(2)}\}$$

означает группу, порожденную элементами $\sigma G_S^{(2)}$ и $\tau^3 G_S^{(2)}$ в факторгруппе $G_S/G_S^{(2)}$, $z = [\tau, \sigma]$. Будем пользоваться обозначениями:

$$\tilde{\sigma} = \sigma G_S^{(2)}, \quad \tilde{\tau} = \tau G_S^{(2)}.$$

В группах

$$\{\tilde{\sigma}, \tilde{\tau}^3\}, \quad \{\tilde{\sigma}, \tilde{\tau}^3 z\}, \quad \{\tilde{\sigma}, \tilde{\tau}^3 z^2\}.$$

выберем подгруппы

$$U_0 = \{\tilde{\sigma}^3, \tilde{\tau}^3\}, \quad U_1 = \{\tilde{\sigma}^3, \tilde{\tau}^3 z\}, \quad U_2 = \{\tilde{\sigma}^3, \tilde{\tau}^3 z^2\}.$$

Пусть K_0, K_1, K_2 поля соответствующие согласно теории Галуа подгруппам U_0, U_1, U_2. Группа Галуа $G(K_0/\mathbb{Q})$ поля K_0 над полем рациональных чисел $\mathbb{Q}$ изоморфна группе

$$G_S/U_0, \quad \text{порожденной элементами } \sigma U_0, \quad \text{и } \tau U_0.$$

Если обозначить $\sigma_0 = \sigma U_0$, $\tau_0 = \tau U_0$, то $G(K_0/\mathbb{Q})$ изоморфна группе, порожденной образующими σ_0, τ_0 и соотношениями:

$$\sigma_0^3 = 1, \ \tau_0^3 = 1, \ z_0^3 = 1, \quad \text{где } z_0 = [\tau_0, \ \sigma_0].$$

Группа Галуа $G(K_1/\mathbb{Q})$ поля K_1 над полем рациональных чисел $\mathbb{Q}$ изоморфна группе

$$G_S/U_1, \quad \text{порожденной элементами } \sigma U_1, \quad \text{и } \tau U_1.$$

Если обозначить $\sigma_1 = \sigma U_1$, $\tau_1 = \tau U_1$, то $G(K_1/\mathbb{Q})$ изоморфна группе, порожденной образующими σ_1, τ_1 и соотношениями:

$$\sigma_1^3 = 1, \ \tau_1^9 = 1, \ z_1^2 = \tau_1^3, \quad \text{где } z_1 = [\tau_1, \ \sigma_1].$$

Группа Галуа $G(K_2/\mathbb{Q})$ поля K_2 над полем рациональных чисел $\mathbb{Q}$ изоморфна группе

$$G_S/U_2, \quad \text{порожденной элементами } \sigma U_2, \quad \text{и } \tau U_2.$$

Если обозначить $\sigma_2 = \sigma U_2$, $\tau_2 = \tau U_2$, то $G(K_2/\mathbb{Q})$ изоморфна группе, порожденной образующими σ_2, τ_2 и соотношениями:

$$\sigma_2^3 = 1, \ \tau_2^9 = 1, \ z_2 = \tau_2^3, \quad \text{где } z_2 = [\tau_2, \ \sigma_2].$$

Выясним в каком поле K_j, $0 \leq j \leq 2$, число 19 полностью распадается.

Если 19 распадается в поле K_j, $0 \leq j \leq 2$, то оно распадается и в композите $K_j \cdot \mathbb{Q}(\rho)$, $0 \leq j \leq 2$, где $\rho^3 = 1$.

Покажем, что число 19 не распадается полностью в поле $K_0 \cdot \mathbb{Q}(\rho)$.

Группа Галуа $G(K_0 \cdot \mathbb{Q}(\rho)/\mathbb{Q})$ поля $K_0 \cdot \mathbb{Q}(\rho)$ над полем рациональных чисел $\mathbb{Q}$ изоморфна прямому произведению

$$G(K_0/\mathbb{Q}) \times G(\mathbb{Q}(\rho)/\mathbb{Q})$$

групп $G(K_0/\mathbb{Q})$ и $G(\mathbb{Q}(\rho)/\mathbb{Q})$. Пусть $G(\mathbb{Q}(\rho)/\mathbb{Q}) = \{1, t \mid t^2 = 1\}$. Тогда группа Галуа $G(K_0 \cdot \mathbb{Q}(\rho)/\mathbb{Q})$ поля $K_0 \cdot \mathbb{Q}(\rho)$ над полем рациональных чисел $\mathbb{Q}$ изоморфна группе, порожденной образующими σ_0, τ_0, t и соотношениями

$$\sigma_0^3 = 1,\ \tau_0^3 = 1, t^2 = 1,\ [\sigma_0, t] = [\tau_0, t] = [z_0, t] = z_0^3 = 1,\ \text{где}\ z_0 = [\tau_0,\ \sigma_0].$$

Следовательно, возникла задача погружения: необходимо построить расширение $K_0 \cdot \mathbb{Q}(\rho)$ поля, являющегося композитом максимального 3-подполя поля $\mathbb{Q}(\mu_{19})$ степени 9 над полем $\mathbb{Q}$, где μ_{19} – первообразный корень 19 степени из единицы, и поля $\mathbb{Q}(\zeta)$, где ζ – первообразный корень 27 степени из единицы. Решая эту задачу погружения, получаем:

$$\mathbb{Q} \subset \mathbb{Q}(\rho) \subset \mathbb{Q}\Big(\rho,\ \sqrt[3]{\rho},\ \sqrt[3]{\frac{\alpha}{\alpha'}},\Big) \subset \mathbb{Q}\Big(\rho,\ \sqrt[3]{\rho},\ \sqrt[3]{\frac{\alpha}{\alpha'}},\ \sqrt[3]{\mu}\Big),$$

где

$$\alpha = -2 + 3\rho,\ \ \alpha' = -5 - 3\rho,\ \ \alpha \cdot \alpha' = 19,\ \ \mu = \frac{\mathfrak{p}_2\mathfrak{q}_1}{\mathfrak{q}_3\mathfrak{p}_3},$$

$$\begin{aligned}
\mathfrak{p}_1 &= -2 + (1-\rho)\zeta, & \zeta &\equiv 6 (\mathrm{mod}\, \mathfrak{p}_1),\\
\mathfrak{p}_2 &= -2 + (1+2\rho)\zeta, & \zeta &\equiv 9 (\mathrm{mod}\, \mathfrak{p}_2),\\
\mathfrak{p}_3 &= -2 + (-2-\rho)\zeta, & \zeta &\equiv 4 (\mathrm{mod}\, \mathfrak{p}_3),\\
\mathfrak{q}_1 &= -2 + (2+\rho)\zeta^2, & \zeta &\equiv 5 (\mathrm{mod}\, \mathfrak{q}_1),\\
\mathfrak{q}_2 &= -2 + (1+2\rho)\zeta^2, & \zeta &\equiv -3 (\mathrm{mod}\, \mathfrak{q}_2),\\
\mathfrak{q}_3 &= -2 + (-1-\rho)\zeta^2, & \zeta &\equiv -2 (\mathrm{mod}\, \mathfrak{q}_3),
\end{aligned}$$

$$\alpha = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3, \quad \alpha' = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3.$$

Элементы группы Галуа $G(K_0 \cdot \mathbb{Q}(\rho)/\mathbb{Q})$ действуют следующим оброзом:

$$\begin{array}{llll}
\zeta^t = \zeta^{-1}, & \zeta^{\sigma_0} = \zeta, & \zeta^{\tau_0} = \zeta^4, & \alpha^t = \alpha',\\
\mathfrak{p}_1^t = \mathfrak{q}_2, & \mathfrak{p}_2^t = \mathfrak{q}_3, & \mathfrak{p}_3^t = \mathfrak{q}_1, & \mathfrak{q}_j^{\sigma_0} = \mathfrak{q}_j,\ 1 \le j \le 3,\\
\mathfrak{p}_1^{\tau_0} = \mathfrak{p}_2, & \mathfrak{p}_2^{\tau_0} = \mathfrak{p}_3, & \mathfrak{p}_3^{\tau_0} = \mathfrak{p}_1, & \mathfrak{p}_j^{\sigma_0} = \mathfrak{p}_j,\ 1 \le j \le 3,\\
\mathfrak{p}_1^{\tau_0} = \mathfrak{p}_2, & \mathfrak{p}_2^{\tau_0} = \mathfrak{p}_3, & \mathfrak{p}_3^{\tau_0} = \mathfrak{p}_1, &
\end{array}$$

Заметим, что

$$\mu^{t-2} = \frac{\mathfrak{p}_2^t\mathfrak{q}_1^t}{\mathfrak{q}_3^t\mathfrak{p}_3^t} \cdot \frac{\mathfrak{q}_3^2\mathfrak{p}_3^2}{\mathfrak{p}_2^2\mathfrak{q}_1^2} = \frac{\mathfrak{q}_3^3\mathfrak{p}_3^3}{\mathfrak{q}_1^3\mathfrak{p}_2^3} = \frac{\mathfrak{q}_3\mathfrak{p}_3{}^3}{\mathfrak{q}_1\mathfrak{p}_2}.$$

Пусть $\beta = \frac{\mathfrak{q}_3\mathfrak{p}_3}{\mathfrak{q}_1\mathfrak{p}_2}$.

$$\mu^{\sigma_0} = \mu,\ \ \mu^{\tau_0 - 1} = \frac{\mathfrak{p}_3^3}{\mathfrak{q}_1^3}\frac{\alpha'}{\alpha}.$$

Пусть $\gamma = \frac{\mathfrak{p}_3}{\mathfrak{q}_1}\sqrt[3]{\frac{\alpha'}{\alpha}}$.

Можем записать следующие равенства:

$$\sqrt[3]{\mu}^{\tau_0} = \gamma\sqrt[3]{\mu}, \quad \sqrt[3]{\mu}^{t} = \beta\sqrt[3]{\mu}^{2}.$$

Для того, чтобы поле $\mathbb{Q}(\rho, \sqrt[3]{\rho}, \sqrt[3]{\frac{\alpha}{\alpha'}}, \sqrt[3]{\mu})$ было композитом поля $\mathbb{Q}(\rho)$ и некоторого поля L, необходимо и достаточно, чтобы выполнялось равенство:

$$\gamma^{t}\beta = \beta^{\tau_0}\gamma^{2}.$$

Простая проверка показывает, что это равенство выполняется.

Рассмотрим уравнение $\mu \equiv x^3 (\mathrm{mod}\, \mathfrak{p}_1)$. Так как $\zeta \equiv 6(\mathrm{mod}\, \mathfrak{p}_1)$, $\rho \equiv 7(\mathrm{mod}\, \mathfrak{p}_1)$, то $\mu \equiv 5^2 (\mathrm{mod}\, \mathfrak{p}_1)$. Но 2 является первообразным классом вычетов по mod 19, и так как $5 \equiv 2^5 (\mathrm{mod}\, 19)$, то сравнение $\mu \equiv x^3 (\mathrm{mod}\, \mathfrak{p}_1)$ не разрешимо. Легко убедиться, что $\zeta\mu \not\equiv x^3 (\mathrm{mod}\, \mathfrak{p}_1)$, $\zeta^2\mu \equiv -1 (\mathrm{mod}\, \mathfrak{p}_1)$. Следовательно, группа, порожденная элементами σ и $\tau^3 z$, где $z = [\tau, \sigma]$, является группой разложения простого дивизора числа 19 в поле, соответствующем согласно теории Галуа подгруппе $G(3, 19)^{(2)}$. Таким образом, соотношение между образующими σ и τ группы Галуа G_S по модулю $G_S^{(3)}$ следующее:

$$\sigma^9 = [\tau^3[\tau, \sigma], \sigma] (\mathrm{mod}\, G_S^{(3)}).$$

ЛИТЕРАТУРА

[1] J. Browkin, On generalized class field tower, *Bull. Acad. Polon. Sci., Ser. Math.*, **11** (1963), 143–145.

[2] С.П. Демушкин, Максимальное p-расширение локального поля, *Изв. АН СССР, сер. матем.*, **25** (1961), 329–346.

[3] A. Frohlich, On fields of class two, *Proc. London Math. Soc.*, **3**(4) (1954), 235–256.

[4] H. Koch, l-Erweiterungen mit vorgegebenen Verzweigungsstellen, *J. reine angew. Math.*, **219** (1965), 30–61.

[5] H. Koch, l-Erweiterungen mit zwei Verzweigungsstellen, *Monatsber. DAW*, **7** (1965), 616–623.

[6] H. Koch, *Galoissche Theorie der p-Erweiterungen*, Berlin, 1970.

[7] Г.Н. Маркшайтис, О p-расширениях с одной критической точкой, *Изв. АН СССР, сер. матем.*, **27** (1963), 463–466.

[8] И.Р. Шафаревич, Расширения с заданными точками ветвления, *Publ. Mathem., IHES*, **18** (1964), 71–95.

[9] И.Р. Шафаревич, Новое доказательство теоремы Кронекера-Вебера, *Труды матем. института Ак. наук СССР*, **38** (1951), 382–387.

[10] H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Leipzig, 1937.

p-plėtinių su dviem kritiniais taškais Galua grupės

H. Markšaitis (VU)

Rasta 3-plėtinio su kritiniais taškais 3 ir 19 Galua grupės struktūra pagal trečiąjį apatinės centrinės eilutės narį.