Градуировки расширений Галуа

Д. А. БАДУЛИН
Московский государственный университет им. М. В. Ломоносова
e-mail: dbadulin28@gmail.com

А. Л. КАНУННИКОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: andrew.kanunnikov@gmail.com

УДК 512.623

Ключевые слова: расширения Галуа, куммеровы расширения, градуировки.

Аннотация

В статье исследуются градуировки конечных расширений, в которых все однородные компоненты одномерны. Такие градуировки называются тонкими. Важный класс расширений, допускающих тонкую градуировку, образуют куммеровы расширения. Для них всегда существует стандартная градуировка по группе Галуа. В работе описаны все тонкие градуировки куммеровых расширений, в частности, установлен критерий того, что всякая тонкая градуировка изоморфна стандартной. Исследованы также градуировки более широкого класса расширений Галуа, допускающих тонкие градуировки.

Abstract

D. A. Badulin, A. L. Kanunnikov, Gradings of Galois extensions, Fundamentalnaya i prikladnaya matematika, vol. 24 (2023), no. 4, pp. 11—29.

This paper is devoted to the gradings of finite field extensions in which all homogeneous components are one-dimensional. Such gradings are called fine. Kummer extensions are an important class of extensions that admit fine gradings. There always exists a standard grading of Kummer extension based on the Galois group. The paper describes all fine gradings of Kummer extensions, and, in particular, it establishes a criterion for any fine grading to be isomorphic to the standard one. We also investigate gradings of a wider class of Galois extensions that admit fine gradings.

Введение

Интерес к градуированным структурам возник во второй половине XX века в алгебраической геометрии, теории супералгебр Ли, структурной теории колец и алгебр [5]. Одной из центральных задач теории градуированных алгебр является описание всех градуировок на данной алгебре, и прежде всего на алгебрах, допускающих некоторую естественную градуировку (таковыми, например, являются алгебры многочленов, групповые алгебры, алгебры матриц [4]).

Фундаментальная и прикладная математика, 2023, том 24, № 4, с. 11—29.

Градуировки на алгебре естественным образом возникают при рассмотрении действия на ней группами автоморфизмов.

Например, куммеровы расширения, которые получаются присоединением корней из элементов основного поля, допускают естественную градуировку по группе Галуа, и при этом все однородные компоненты одномерны. Градуировки с таким условием называются тонкими. При этом некоторый класс куммеровых расширений допускает другие тонкие градуировки не по группе Галуа.

В [6, 7] исследованы классы алгебраических расширений (кнезеровские расширения), допускающие естественную градуировку, и развита теория, двойственная теории Галуа, рассмотрены её приложения к арифметическим вопросам теории полей. В [2] авторы нашли все градуировки квадратичных куммеровых расширений. В данной работе мы описываем все возможные градуировки любых куммеровых расширений, а также исследуем множество тонких градуировок расширений Галуа, что также позволяет вычислить их группы Галуа.

1. Свойства градуировок конечных расширений

Всюду G — мультипликативная группа с единицей e.

Определение 1. Кольцо R называется градуированным по группе G (или G-градуированным), если $R = \bigoplus\limits_{g\in G} R_g$, где $\{R_g \mid g \in G\}$ — семейство аддитивных подгрупп кольца R, таких что $R_gR_h \subseteq R_{gh}$ для всех $g, h \in G$. При этом элементы множества $h(R) = \bigcup\limits_{g\in G} R_g$ называются *однородными*; ненулевой элемент $r \in R_g$ называется однородным элементом *степени* g; множество $\operatorname{Supp}(R) = \{g \in G \mid R_g \neq 0\}$ называется *носителем* градуированного кольца R.

Если R — G-градуированное кольцо, то $1 \in R_e$ и для каждого обратимого однородного элемента $r \in R_g$ имеем $r^{-1} \in R_{g^{-1}}$ [5, предложение 1.1.1].

Предложение 1 [2]. *Пусть G-градуированное поле R является конечномерной алгеброй над некоторым полем K, лежащим в R_e. Тогда*

$$\dim_K R = \dim_K R_e \cdot |\operatorname{Supp}(R)|.$$

Определение 2. Конечной невырожденной градуировкой расширения L/K будем называть градуировку поля L как K-алгебры $L = \bigoplus\limits_{g\in G} L_g$ по конечной группе G, называемой градуирующей группой, где все компоненты L_g ненулевые.

Определение 3. Градуировка расширения L/K по группе G называется *тонкой*, если $L_e = K$ и $\operatorname{Supp} L = G$.

Замечание 1. Требование $L_e = K$ равносильно тому, что все подпространства L_g ($g \in G$) над K одномерны.

Определение 4. Огрублением или свёрткой градуировки $L = \bigoplus\limits_{g\in G} L_g$ относительно проекции $G \overset{\pi}{\twoheadrightarrow} H$ назовём градуировку

$$L = \bigoplus_{h\in H} L_h, \quad \text{где} \quad L_h = \bigoplus_{\substack{g\in G \\ \pi(g)=h}} L_g.$$

Отметим, что в англоязычной литературе для тонких градуировок используется название «fine grading», а для огрубления используется термин «coarsening».

Пусть L/K — расширение с тонкой G-градуировкой. Ставя в соответствие каждому ненулевому однородному элементу $\alpha \in h(L)^*$ его степень $g \in G$, получаем сюръективный гомоморфизм групп $h(L)^* \to G$ с ядром K^*. Следовательно, $h(L)^*/K^* \cong G$. При этом данная G-градуировка изоморфна градуировке по группе $h(L)^*/K^*$.

Определение 5. Тонкую градуировку расширения L/K по группе $h(L)^*/K^*$ назовём градуировкой *канонического типа*.

Так как всякая тонкая градуировка изоморфна градуировке канонического типа, то классификация всех тонких градуировок данного расширения сводится к классификации его градуировок канонического типа. Каждая из таких градуировок однозначно определяется множеством $h(L)$ однородных элементов.

Замечание 2. Пусть L/K — расширение степени n с тонкой G-градуировкой. Так как G — конечная группа, то $h(L)^*/K^* \subseteq T_n(L^*/K^*)$. Поэтому если $|T_n(L^*/K^*)| = n$, то последнее включение обращается в равенство и существует ровно одна градуировка канонического типа расширения L/K. Как следствие, группа G определена однозначно с точностью до изоморфизма, $G \cong T_n(L^*/K^*)$.

Предложение 2. *Если L/K — конечное сепарабельное расширение степени n, то тонких градуировок расширения L/K с точностью до изоморфизма конечное число.*

Доказательство. Пусть существует тонкая G-градуировка канонического типа расширения L/K. Тогда L/K — сепарабельное радикальное расширение. Как показано в [10], подгруппа

$$T_n(L^*/K^*) = \{\alpha K^* \in L^*/K^* \mid \alpha^n \in K\}$$

в группе $T(L^*/K^*)$ конечна. При этом данной градуировке соответствует некоторый гомоморфизм $G \to T_n(L^*/K^*)$.

Так как группа $T_n(L^*/K^*)$ конечна и возможных градуирующих групп с точностью до изоморфизма (т. е. конечных абелевых групп порядка n) конечное число, то из наблюдения выше получаем, что тонких градуировок расширения L/K с точностью до изоморфизма конечное число. □

Замечание 3. Из предложения 2 следует, что конечных невырожденных градуировок расширения L/K конечное число, так как промежуточных полей в расширении L/K конечное число.

Замечание 4. Условие сепарабельности в предложении 2 необходимо. Пусть F — бесконечное поле характеристики p. Положим $K = F(T^p)$, $L = K(T)$. Тогда $[L : K] = p$, и для любого $\alpha \in L \setminus K$ верно, что $L = K(\alpha)$, так как $1 \neq [K(\alpha) : K] \mid [L : K]$. Имеется тонкая градуировка

$$L = K \oplus KT \oplus \ldots \oplus KT^{p-1},$$

откуда видно, что $L^p = K$.

Рассмотрим элементы вида $\alpha = 1 + aT$, $a \in K^*$. Так как $\alpha^p \in K$, $\alpha \notin K$ и двучлен $x^p - \alpha^p$ неприводим в $K[x]$, то имеется градуировка

$$L = K \oplus K\alpha \oplus \ldots \oplus K\alpha^{p-1},$$

причём градуировки для α_1 и α_2 не изоморфны при $\alpha_1 \neq \alpha_2$, так как иначе существует изоморфизм, для которого $K\alpha_1 = K\alpha_2^k$ для некоторого k, $0 \leqslant k < p$, что равносильно тому, что $\alpha_1 \in K\alpha_2^k$. Это возможно только при $k = 1$, так как

$$1 + a_1 T \in K\left(\sum_{j=0}^{k} C_k^j a_2^j T^j\right),$$

т. е.

$$1 + a_1 T = b + b a_2 T,$$

что возможно только при $b = 1$ и $a_1 = a_2$, что противоречит предположению $\alpha_1 \neq \alpha_2$.

Тем самым, варьируя значения a, будем получать различные градуировки, попарно неизоморфные между собой, следовательно, количество попарно неизоморфных градуировок бесконечно.

Если L/K — G-градуированное расширение полей, то для $\alpha \in L$ обозначим через $\theta(\alpha)$ наименьшее такое $m \in \mathbb{N}$, что $\alpha^m \in K$, если такое m существует, иначе будем считать, что $\theta(\alpha) = 0$. Очевидно, что для однородного элемента $\alpha \in L_g$ $\theta(\alpha) = O(g)$ — порядок элемента g в группе G.

Лемма 1. *Пусть L/K — G-градуированное расширение полей, $\alpha \in h(L) \setminus K$. Тогда* $\mathrm{tr}(\alpha) = 0$.

Доказательство. Пусть $\alpha \in L_g$, $n = O(g) = \theta(\alpha)$. Так как подпространства $K, K\alpha, \ldots, K\alpha^{n-1}$ состоят из однородных элементов различных степеней $e, g, \ldots, g^{n-1}$, то их сумма прямая. Следовательно, двучлен $x^n - \alpha^n$ неприводим над K, а значит, является минимальным многочленом для элемента α. Так как $\alpha \notin K$, то $n > 1$, откуда вытекает, что $\mathrm{tr}(\alpha) = 0$ ($\mathrm{tr}(\alpha)$ пропорционален коэффициенту при $(n-1)$-й степени минимального многочлена элемента α). □

Лемма 2. *Пусть L/K — G-градуированное расширение полей, $\varepsilon \in L$ — корень из единицы простой степени p. Если ε — однородный элемент, то $\varepsilon \in K$.*

Доказательство. Пусть $\varepsilon \in L_g$ ($g \in G$). Так как $\varepsilon^p = 1$, то $g^p = e$, откуда следует, что либо $g = e$, либо $O(g) = p$. Последний случай невозможен, так как тогда пространства $K = L_e, L_g, \ldots, L_{g^{p-1}}$ должны образовывать прямую сумму, что противоречит равенству $1 + \varepsilon + \ldots + \varepsilon^{p-1} = 0$. □

Теорема 1. *Пусть L/K — конечное расширение полей с тонкой G-градуировкой $(L_e = K)$, причём $\operatorname{char} K \nmid [L : K]$.*

1. *Если $\operatorname{char} K \neq 2$ и $i \in L$, то элемент i однороден.*
2. *Пусть L содержит неоднородный элемент α, $\theta(\alpha) = m$ и $\varepsilon_p \in K$ для каждого простого делителя p числа m. Тогда*
   a) $\operatorname{char} K \neq 2$ *и* $i \in L \setminus K$;
   b) m *или* $\exp G$ *кратно* 4;
   c) *при* $m = 2$ *элемент* $(1 + i)\alpha$ *однороден.*

Доказательство. Начнём с утверждения 2. В разложении $\alpha = \sum\limits_g \alpha_g$ больше одного слагаемого. Пусть $g \in G$ — любой элемент, для которого $\alpha_g \neq 0$. Положим $\beta = \alpha\alpha_g^{-1}$ и $n = \theta(\beta)$ (ясно, что $\beta^s \in K$, где $s = \text{НОК}\big(m, O(g)\big)$). Имеем

$$\beta = 1 + \sum_{h \neq g} \alpha_h \alpha_g^{-1} \notin K.$$

По лемме 1 $\operatorname{tr}(\alpha_h\alpha_g^{-1}) = 0$ для всех $h \neq g$, следовательно, $\operatorname{tr}(\beta) = \operatorname{tr}(1) = [L : K] \neq 0$. Поэтому $n > 1$ и двучлен $x^n - \beta^n$ не является минимальным многочленом для элемента β. Следовательно, этот двучлен приводим над K. По [3, с. 252] это возможно только в одном из следующих двух случаев.

Случай 1: $\beta^n = b^p$ для некоторого $b \in K$ и некоторого простого p, делящего n. Отсюда следует, что $\beta^{n/p} = b\varepsilon$, где $\varepsilon^p = 1$. Если $\varepsilon \in K$, то $\beta^{n/p} \in K$, что противоречит минимальности n. При $p \mid m$ элемент ε лежит в K по условию. Пусть $p \nmid m$. Тогда

$$b^m\varepsilon^m = \beta^{mn/p} = \alpha^{mn/p}\alpha_g^{-mn/p}.$$

Так как $\alpha^m, b^m \in K$ и $\alpha_g^{-mn/p}$ — степень однородного элемента α_g, то ε^m — однородный элемент, откуда по лемме 2 $\varepsilon^m \in K$ и $\varepsilon \in K$, так как $(m, p) = 1$ ($um + vp = 1$ влечёт $\varepsilon = (\varepsilon^m)^u 1^v \in K$). Таким образом, этот случай невозможен.

Случай 2: $n = 4k$ ($k \in \mathbb{N}$), $\operatorname{char} K \neq 2$ и $\beta^{4k} = -4b^4$ для некоторого $b \in K$. Тогда в поле $L(i)$

$$\beta^{2k} = \pm 2ib^2, \tag{1}$$

поэтому $i \in L$. Если $i \in K$, то $\beta^{2k} \in K$, что противоречит минимальности n. Таким образом, $i \in L \setminus K$, и утверждение 2 a) доказано.

Докажем утверждение 2 b). Так как $\beta = \alpha\alpha_g^{-1}$, то

$$4k = n = \theta(\beta) \mid \text{НОК}\big(\theta(\alpha), \theta(\alpha_g^{-1})\big) \mid \text{НОК}(m, \exp G).$$

Докажем утверждения 1 и 2 c). Пусть $m = 2$. Тогда $\alpha^2 \in K$ и $\beta^2 = \alpha^2\alpha_g^{-2}$ — однородный элемент. Следовательно, все чётные степени элемента β однородны. Из (1) получаем, что i — однородный элемент. В частности, предположив, что $\alpha = i$, получаем противоречие. Поэтому утверждение 1 доказано. Следовательно, $\alpha \neq i$, и

$$\beta^k = i^s(1 + i)b, \quad s = 0, 1, 2, 3. \tag{2}$$

Элемент в правой части неоднороден, так как $i \in h(L) \setminus K$ и $1 + i \notin h(L)$. Следовательно, k нечётно, а тогда элемент $\beta^{k+1} = \beta(1+i)i^s b$ однороден, поэтому однородны элементы $\beta(1+i)$ и $\alpha(1+i) = \beta(1+i)\alpha_g$. □

2. Градуировки куммеровых расширений

Пусть L/K — куммерово расширение с группой Галуа $G = \mathrm{Gal}(L/K)$. Обозначим $k = \exp G$. Как известно, $\varepsilon_k \in K$.

Определим подгруппу в L^*/K^*:

$$S = S_{L/K} = \{a \in L^*/K^* \mid a^k = 1\}.$$

Если $\alpha K^* \in S_{L/K}$ и $\alpha K^* \neq K^*$, то $\mathrm{tr}(\alpha) = 0$. Действительно, $\theta(\alpha) > 1$ и двучлен $x^{\theta(\alpha)} - \alpha^{\theta(\alpha)}$ неприводим, так как $\varepsilon_k \in K$ и $\theta(\alpha) \mid k$ по определению группы $S_{L/K}$.

Предложение 3. $S_{L/K} \cong \mathrm{Gal}(L/K)$.

Доказательство. См. [9, «Теория Куммера», замечание 5.30]. □

Замечание 5. Если $r^{ab} \in K$ и $(a, b) = 1$, то $K(r) = K(r^a, r^b)$.

Замечание 6. Если $r^m \in K$, $r, \ldots, r^{m-1} \notin K$, $\varepsilon_m \in K$, то $[K(r) : K] = m$.

Из этих замечаний получаем следующий результат.

Предложение 4. *Пусть $L/K = K(r_1, \ldots, r_n)/K$ — куммерово расширение. Для каждого $j = 1, \ldots, n$ пусть $d_j = 2^{k_j} m_j$ — наименьшее натуральное число со свойством $r_j^{d_j} \in K$, причём $k_j \in \mathbb{N}_0$ и m_j нечётно. Положим*

$$P = K(r_1^{m_1}, \ldots, r_n^{m_n}), \quad Q = K(r_1^{2^{k_1}}, \ldots, r_n^{2^{k_n}}).$$

Тогда P/K и Q/K — куммеровы расширения, $[P : K] \mid m_1 \ldots m_n$ нечётно, $[Q : K] \mid 2^{k_1 + \ldots + k_n}$.

Предложение 5. *Разложение $L = \bigoplus\limits_{sK^* \in S} Ks$ является тонкой градуировкой канонического типа. Такую градуировку куммерова расширения L/K назовём стандартной.*

Доказательство. Выберем в каждом классе $s_i K^*$ по представителю. Эти представители порождают L как векторное пространство над K и линейно независимы по предложению 3. □

Далее L/K — куммерово расширение. Зафиксируем обозначения:

$$L = K(r_1, \ldots, r_n), \quad G = \mathrm{Gal}(L/K), \quad k = \exp G, \quad r_j^k \in K.$$

Теорема 2. *Если выполнено хотя бы одно из условий*

1) *число k нечётно или кратно 4,*
2) $\mathrm{char}\, K \neq 2$, *$i \notin K$ или $i \in L$,*

то всякая тонкая G-градуировка расширения L/K является стандартной.

Доказательство. Для каждого $j \in \{1, \dots, n\}$ определим число $k_j \in \mathbb{N}$ так, что элементы $1, r_1, \dots, r_j^{k_j} - 1$ образуют базис расширения $K(r_1, \dots, r_j)$ над $K(r_1, \dots, r_{j-1})$. Тогда система

$$R = \{r_1^{i_1} \dots r_n^{i_n} \mid 0 \leqslant i_1 < k_1, \dots, 0 \leqslant i_n < k_n\}$$

является базисом в L/K. Из условия следует, что каждый элемент $\alpha \in R$ удовлетворяет условиям теоремы 1, а значит, все элементы из R однородны. С другой стороны, $|R| = |S| = |G|$. Следовательно, данная градуировка изоморфна стандартной. □

Итак, нестандартная градуировка куммерова расширения может существовать, только если k чётно, но не кратно 4, и $i \in L \setminus K$.

Предложение 6. *Пусть P и Q — расширения поля K, имеющие конечные взаимно простые степени, и G — абелева группа порядка $[L : K]$. Тогда*

1) *композит $L = PQ$ является их тензорным произведением $P \otimes Q$;*
2) *в G есть ровно одна подгруппа $G(P)$ порядка $[P : K]$ и ровно одна подгруппа $G(Q)$ порядка $[Q : K]$;*
3) *если L/K — куммерово расширение, то любая его тонкая G-градуировка является произведением тонкой $G(P)$-градуировки расширения P/K и тонкой $G(Q)$-градуировки расширения Q/K.*

Доказательство. Пусть $[P : K] = m$, $[Q : K] = n$.

Докажем утверждение 1). Если $e_1, \dots, e_m$ — базис в P/K и $f_1, \dots, f_n$ — базис в Q/K, то mn произведений $e_i f_j$ ($1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$) порождают композит PQ над K, а значит, составляют его базис, так как по лемме о башне $[PQ : K]$ делится на $[P : K] = m$ и на $[Q : K] = n$, а тогда и на mn в силу условия $(m, n) = 1$.

Утверждение 2) следует из структурной теоремы о конечных абелевых группах.

Утверждение 3) следует из соответствий Галуа: группа $\mathrm{Gal}(PQ/K)$ абелева и имеет порядок mn, поэтому в ней есть ровно одна пара подгрупп порядков m и n, следовательно, им соответствуют подполя Q и P соответственно. Значит, P и Q — единственная пара подполей в PQ степеней m и n над K. □

Расширение L/K представляется в виде тензорного произведения (композита) подполей:

$$L = L^{T_2(G)} \otimes P,$$

здесь $L^{T_2(G)}$ — подполе инвариантов 2-примарной подгруппы $T_2(G)$ группы Галуа G и

$$P = \bigoplus_{sK^* \in T_2(S)} Ks -$$

максимальное квадратичное расширение в L/K. Эти расширения являются куммеровыми, а их степени взаимно просты. Поэтому описание градуировок расширения L сводится к описанию градуировок этих двух расширений.

Так как степень $[L^{T_2(G)} : K]$ нечётна, то все градуировки расширения $L^{T_2(G)}$ стандартны.

Пусть $[P : K] = 2^{m+1}$, $m \geqslant 1$. Выберем квадратные радикалы $r_0 = i$, $r_1, \ldots, r_m \in P$ так, что $P = K(r_0, \ldots, r_m)$. Тогда

$$T_2(S) = \langle r_0 K^* \rangle \times \ldots \times \langle r_m K^* \rangle.$$

Теорема 3. *Для каждого непустого подмножества $J \subseteq \{1, \ldots, m\}$ существует единственная градуировка канонического типа расширения P/K, в которой однородными являются элементы*

$$(1+i)r_j \text{ при } j \in J, \quad r_k \text{ при } k \in \{1, \ldots, m\} \setminus J. \tag{3}$$

Так описываются все нестандартные градуировки канонического типа расширения P/K.

Доказательство. Пусть дана произвольная градуировка расширения P/K. По теореме 1 для каждого $j = 1, \ldots, m$ ровно один из двух элементов r_j, $(1+i)r_j$ однороден. Если все r_j однородны, то градуировка стандартна. Пусть однородны элементы (3) для некоторого непустого подмножества $J \subseteq \{1, \ldots, m\}$. Для простоты обозначений перенумеруем радикалы, считая, что $J = \{1, \ldots, n\}$. На поле $P' = K(i, r_1, \ldots, r_n)$ получаем индуцированную градуировку, в которой однородны 2^{n+1} элементов:

$$1,\ i,\ r_{j_1} \ldots r_{j_{2s}},\ ir_{j_1} \ldots r_{j_{2s}},\ (1 \pm i)r_{j_1} \ldots r_{j_{2t+1}} \quad (s > 0,\ 1 \leqslant j_1 < j_2 < \ldots \leqslant n). \tag{4}$$

Эти элементы образуют базис расширения P'/K, так как получены из базиса всевозможных 2^{n+1} произведений элементов $i, r_1, \ldots, r_n$ преобразованиями вида

$$\{R, iR\} \to \{(1+i)R, (1-i)R\}, \quad R = r_{j_1} \ldots r_{j_{2t+1}}.$$

Градуировка поля P является произведением данной градуировки поля P' и стандартной градуировки поля $P'' = K(r_{n+1}, \ldots, r_m)$.

Таким образом, набор однородных элементов, а значит и градуировка расширения P/K, однозначно определяется подмножеством J.

Умножая элементы (4) на K^*, получаем группу G, которая канонически градуирует расширение P'/K. Отметим, что $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2^{n-1}$, так как G — абелева группа порядка 2^{n+1} и $G^2 = \{K^*, iK^*\} \cong \mathbb{Z}_2$. □

Следствие 1. *Нестандартная градуировка куммерова расширения L/K существует в точности тогда, когда* $\operatorname{char} K \neq 2$, *$i \in L \setminus K$ и существует квадратный радикал $r \in P \setminus (K \cup Ki)$, $r^2 \in K$.*

Доказательство. Поскольку произведение стандартных градуировок является стандартной градуировкой и все градуировки расширения Q/K стандартны, надо доказать, что указанное в теореме условие является критерием существования нестандартной градуировки квадратичного расширения P/K, а это следует из теоремы 3. □

3. Градуировки расширений Галуа

Всюду в этом разделе L/K — расширение Галуа с тонкой G-градуировкой и $\operatorname{char} K \nmid [L:K]$.

Лемма 3. *Для каждого простого делителя p числа $[L:K]$ имеем $\varepsilon_p \in L$. Если q — наименьший простой делитель числа $[L:K]$, то $\varepsilon_q \in K$.*

Доказательство. Пусть $g \in G$ — элемент порядка p. Тогда всякий элемент $\alpha \in L_g \setminus K$ обладает следующими свойствами: $\alpha^p \in K$ и $1, \alpha, \ldots, \alpha^{p-1}$ линейно независимы над K (последнее следует из того, что сумма $L_e \oplus L_g \oplus \ldots \oplus L_{g^{p-1}}$ прямая). Следовательно, двучлен $x^p - \alpha^p$ является минимальным многочленом для α над K. Так как L/K — нормальное и сепарабельное расширение, то этот двучлен имеет в L ровно p различных корней $\alpha\varepsilon_p^j$, $j = 0, \ldots, p-1$. В частности, $\varepsilon_p \in L$.

Далее $[K(\varepsilon_q):K] \leqslant q-1$ и $[K(\varepsilon_q):K] \mid [L:K]$. Отсюда следует, что $[K(\varepsilon_q):K] = 1$, т. е. $\varepsilon_q \in K$. □

3.1. Случай: $|G|$ нечётно

Теорема 4. *Если порядок группы G нечётен, то эта группа определена однозначно.*

Доказательство. Свернём градуировку расширения L/K относительно канонической проекции $G \to T_p(G)$. Эта градуировка является тонкой. Обозначим через F нейтральную компоненту получившейся градуировки, а через H — подгруппу в G, являющуюся носителем поля F в исходной градуировке расширения L/K:

$$F = \bigoplus_{h \in H} K_h, \quad H = \bigoplus_{q \neq p} T_q(G).$$

Так как $[L:F] = [L:K]/[F:K] = |T_p(G)|$, то при соответствии Галуа для расширения L/K подполе F соответствует p-силовской подгруппе в группе $\operatorname{Gal}(L/K)$. Так как p — единственный простой делитель числа $[L/F] = |T_p(G)|$, то по лемме 3 $\varepsilon_p \in F$. По теореме 1 любой такой элемент α, что $\alpha K^* \in \in T_p(L^*/F^*)$, однороден. Ставя в соответствие каждому такому элементу его степень однородности, получаем изоморфизм групп $T_p(L^*/F^*) \cong T_p(G)$.

Пусть существует другая тонкая G'-градуировка расширения L/K. Аналогично рассматривая проекцию $G' \to T_p(G')$ и подполе F', получаем, что $T_p(G') \cong T_p(L^*/F'^*)$. Но подполя F и F' соответствуют силовским p-подгруппам в группе $\operatorname{Gal}(L/K)$. Значит, $F' = \sigma F$ для некоторого $\sigma \in \operatorname{Gal}(L/K)$ и, следовательно, $T_p(L^*/F^*) \cong T_p(L^*/\sigma F^*)$, откуда следует, что $T_p(G) \cong T_p(G')$. Значит, $G \cong G'$. □

Замечание 7. Для данного простого делителя p порядка группы G обозначим через t_p максимальное среди таких $m \geqslant 0$, что $\varepsilon_{t^m} \in L$. Отметим, что

подгруппа $\langle \varepsilon_{p^{t_p}} K^* \rangle$ не всегда выделяется прямым слагаемым в группе G. Действительно, положим $K = \mathbb{Q}(\varepsilon_3)$, $L = \mathbb{Q}(\varepsilon_{27}\sqrt[9]{5})$. Тогда L/K — расширение, полученное присоединением корней двучлена $x^3 - 5\varepsilon_3$. Значит, это расширение Галуа степени 9. Его группа Галуа $\mathrm{Gal}(L/K) \cong \mathbb{Z}_9$, и оно допускает градуировку по группе $\mathbb{Z}_9$:

$$L = \bigoplus_{k=0}^{8} K(\varepsilon_{27}\sqrt[3]{5})^k.$$

3.2. Случай: $|G| = 2^n$

В этом подразделе $|G| = [L : K] = 2^n$, в частности, $\mathrm{char}\, K \neq 2$.

Теорема 5.

1. *Если $i \notin L$, то расширение L/K — квадратичное куммерово расширение, $G \cong \mathrm{Gal}(L/K) \cong \mathbb{Z}_2^n$ и данная G-градуировка определена однозначно с точностью до автоморфизма группы G.*
2. *Если $i \in K$, то данная G-градуировка определена однозначно с точностью до автоморфизма группы G.*

Доказательство. По теореме 1 неоднородный элемент $\alpha \in L$ с $\theta(\alpha) < \infty$ может существовать лишь в случае $i \in L \setminus K$. Следовательно, в каждом из случаев, $i \notin L$ и $i \in K$, $T_2(L^*/K^*) = h(L)^*/K^*$, тем самым градуировка канонического типа расширения L/K единственна. Кроме того, в случае 1 имеем $\exp G = 2$, так как если $\exp G$ кратно 4, то $i = \varepsilon_4 \in L$. Отсюда следует, что $T_2(L^*/K^*) \cong \mathbb{Z}_2^n$ и L/K — квадратичное куммерово расширение. □

Перейдём к случаю $i \in L \setminus K$. Напомним, что элемент i однороден по теореме 1. Порядок группы $T_2(L^*/K^*)$ может быть больше, чем $[L : K]$, поэтому расширение L/K может иметь более одной градуировки канонического типа.

Пример 1. Так как $\varepsilon_8 = (1 + i)/\sqrt{2}$, то $\mathbb{Q}(\varepsilon_8) = \mathbb{Q}(i, \sqrt{2})$. Расширение $\mathbb{Q}(\varepsilon_8)/\mathbb{Q}$ имеет тонкие градуировки по группам $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ и $\mathbb{Z}_4$:

$$\mathbb{Q}(\varepsilon_8) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}i \oplus \mathbb{Q}i\sqrt{2},$$
$$\mathbb{Q}(\varepsilon_8) = \mathbb{Q} \oplus \mathbb{Q}\varepsilon_8 \oplus \mathbb{Q}\varepsilon_8^2 \oplus \mathbb{Q}\varepsilon_8^3.$$

Лемма 4. *При $i \in L \setminus K$ элементы группы $h(L)^*/K^*$ определены с точностью до умножения на элементы группы $T_2(K(i)^*/K^*)$. Иными словами, если α — ненулевой элемент из L, однородный в некоторой тонкой градуировке, то для любой другой тонкой градуировки существует такой элемент $\delta \in K(i)^*$, что $\delta K^* \in T_2(K(i)^*/K^*)$ и элемент $\delta\alpha$ в этой градуировке однороден.*

Доказательство. По пункту 2 теоремы 5 расширение $L/K(i)$ имеет единственную градуировку канонического типа. Пусть даны две тонкие градуировки расширения L/K с множествами однородных элементов $h_1(L)$ и $h_2(L)$, и пусть $\alpha \in h_1(L)^*$. Тогда α будет однородным в единственной градуировке расширения $L/K(i)$. Поэтому найдётся такое $\beta \in h_2(L)^*$, что $K(i)\alpha = K(i)\beta$,

т. е. $\beta = \delta\alpha$, где $\delta \in K(i)^*$. Поскольку $\exp G$ — степень двойки и элемент δK^* имеет конечный порядок, то этот порядок является степенью двойки, т. е. $\delta K^* \in T_2(K(i)^*/K^*)$. □

Обозначим через N наибольшее натуральное число, такое что

$$c_N := \varepsilon_{2^N} + \varepsilon_{2^N}^{-1} \in K,$$

если такое существует. Если все $c_k \in K$, положим $N = \infty$.

Теорема 6 [8]. *Предположим, что* $\operatorname{char} K \neq 2$ *и* $i \notin K$. *Тогда если* $N = \infty$, *то*

$$T_2(K(i)^*/K^*) = \langle \varepsilon_{2^n} K^* \mid n \in \mathbb{N} \rangle;$$

если $N < \infty$, *то*

$$T_2(K(i)^*/K^*) = \langle (1 + \varepsilon_{2^N}) K^* \rangle.$$

Лемма 5. *Пусть* $i \in L \setminus K$ *и* $\alpha \in h(L) \setminus K$, $\theta(\alpha) = 2^k$. *Тогда*

1) *если* $1 < m \leqslant \min(k-1, N)$, *то*

$$\theta((1 + \varepsilon_{2^m})\alpha) = 2^k;$$

2) *если* $K\alpha^{2^{k-1}} \neq Ki$ *и* $1 < k \leqslant N$, *то*

$$\theta\big((1 + \varepsilon_{2^k})\alpha\big) = 2^k \quad \text{и} \quad K\big((1 + \varepsilon_{2^k})\alpha\big)^{2^{k-1}} \neq Ki;$$

3) *если* $K\alpha^{2^{k-1}} = Ki$ *и* $1 < k \leqslant N$, *то*

$$\theta\big((1 + \varepsilon_{2^k})\alpha\big) = 2^{k-1} \quad \text{и} \quad K\big((1 + \varepsilon_{2^k})\alpha\big)^{2^{k-2}} \neq Ki;$$

4) *если* $k \leqslant N - 1$, *то*

$$\theta\big((1 + \varepsilon_{2^{k+1}})\alpha\big) = 2^{k+1} \quad \text{и} \quad K\big((1 + \varepsilon_{2^{k+1}})\alpha\big)^{2^k} = Ki.$$

Доказательство. Пункт 1) следует из того, что

$$K\big((1 + \varepsilon_{2^m})\alpha\big)^{2^{k-1}} = K\alpha^{2^{k-1}} \neq K \quad \text{и} \quad K\big((1 + \varepsilon_{2^m})\alpha\big)^{2^k} = K\alpha^{2^k} = K.$$

Докажем пункт 2). Имеем

$$K\big((1 + \varepsilon_{2^k})\alpha\big)^{2^k} = K\alpha^{2^k} = K \quad \text{и} \quad K\big((1 + \varepsilon_{2^k})\alpha\big)^{2^{k-1}} = Ki\alpha^{2^{k-1}} \neq K, Ki.$$

Докажем пункт 3). Аналогично пункту 2) имеем

$$K\big((1+\varepsilon_{2^k})\alpha\big)^{2^{k-1}} = Ki\alpha^{2^{k-1}} = K \quad \text{и} \quad K\big((1+\varepsilon_{2^k})\alpha\big)^{2^{k-2}} = K(1+i)\alpha^{2^{k-2}} \neq K, Ki,$$

так как иначе элемент $1 + i$ однороден, что невозможно.

Пункт 4) следует из того, что

$$K\big((1 + \varepsilon_{2^{k+1}})\alpha\big)^{2^k} = Ki \quad \text{и} \quad K\big((1 + \varepsilon_{2^{k+1}})\alpha\big)^{2^{k+1}} = K. \qquad \square$$

Лемма 6. *Пусть $i \in L\setminus K$ и $\alpha_1, \ldots, \alpha_t \in h(L)\setminus K$, $\theta(\alpha_j) = 2^{k_j}$, $1 < k_1 \leqslant \ldots \leqslant$ $\leqslant k_{t-1} < k_t$, причём $K\alpha_j^{2^{k_j-1}} \neq Ki$ при $j < t$, $K\alpha_t^{2^{k_t-1}} = Ki$ и $B = \langle\alpha_1 K^*\rangle \times \ldots \times \langle\alpha_t K^*\rangle \subseteq G$. Пусть для каждого $1 \leqslant j < t$ зафиксировано число $r_j \leqslant \min(k_j + 1, N)$. Тогда*

$$\langle\{(1+\varepsilon_{2^{r_j}})\alpha_j K^*\}_{j=1}^{t-1},\ \alpha_t K^*\rangle \cong B.$$

Доказательство. Обозначим $A = \langle\{(1+\varepsilon_{2^{r_j}})\alpha_j K^*\}_{j=1}^{t-1},\ \alpha_t K^*\rangle$. По лемме 5 имеем $\theta\big((1+\varepsilon_{2^{r_j}})\alpha_j\big) = 2^{k_j}$ или 2^{k_j+1}. Следовательно, $\exp A = 2^{k_t}$. Если $r_j = k_j + 1$ для некоторого $j < t$, то

$$\langle(1+\varepsilon_{2^{k_j+1}})\alpha_j K^*, \alpha_t K^*\rangle = \langle(1+\varepsilon_{2^{k_j+1}})\alpha_j\alpha_t^{2^{k_t-k_j-1}} K^*,\ \alpha_t K^*\rangle \cong \mathbb{Z}_{2^{k_j}} \oplus \mathbb{Z}_{2^{k_t}}.$$

Действительно, $\exp\langle(1+\varepsilon_{2^{k_j+1}})\alpha_j K^*,\ \alpha_t K^*\rangle = 2^{k_t}$ и

$$K((1+\varepsilon_{2^{k_j+1}})\alpha_j\alpha_t^{2^{k_t-k_j-1}})^{2^{k_j}} = Ki\cdot i = K,$$

причём $K\big((1+\varepsilon_{2^{k_j+1}})\alpha_j\alpha_t^{k_t-k_j-1}\big)^{2^{k_j-1}} = K(1+i)\alpha_j^{2^{k_j-1}}\alpha_t^{2^{k_t-2}} \neq K, Ki$, так как иначе $K\alpha_j^{2^{k_j-1}} = K(1+i)\alpha_t^{2^{k_t-2}}$ или $K(1-i)\alpha_t^{2^{k_t-2}}$, откуда получаем, что $[K(\alpha_t,\alpha_j) : K(\alpha_t)] \leqslant 2^{k_j-1}$, но из однородности радикалов в градуировке и их независимости имеем $[K(\alpha_t,\alpha_j) : K(\alpha_t)] = 2^{k_j}$ — противоречие.

Если $r_j < k_j + 1$, то из леммы 5 получаем, что $\langle(1+\varepsilon_{2^{r_j}})\alpha_j K^*,\ \alpha_t K^*\rangle \cong$ $\cong \mathbb{Z}_{2^{k_j}} \oplus \mathbb{Z}_{2^{k_t}}$.

Таким образом, получаем, что

$$\begin{aligned} A = \langle&\{(1+\varepsilon_{2^{r_j}})\alpha_j K^* \mid j < t,\ r_j < k_j + 1\},\\ &\{(1+\varepsilon_{2^{k_j+1}})\alpha_j\alpha_t^{2^{k_t-k_j-1}} K^* \mid j < t,\ r_j = k_j + 1\},\ \alpha_t K^*\rangle \cong\\ &\cong \mathbb{Z}_{2^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{2^{k_t}}, \end{aligned}$$

так как $\exp A = 2^{k_t}$ и аналогично рассуждениям выше

$$[K(\alpha_t, \alpha_1, \ldots, \alpha_j) : K(\alpha_t)] = 2^{k_1+\ldots+k_j}$$

для каждого $j < t$ (имеем $K(\alpha_t, \alpha_1, \ldots, \alpha_j) = K(\alpha_t, (1+\varepsilon_{2^{r_1}})\alpha_1, \ldots, (1+\varepsilon_{2^{r_j}})\alpha_j)$). □

Теорема 7. *При $i \in L \setminus K$ существуют такие $\beta_0, \ldots, \beta_s \in h(L)^*$, что*

$$G = \langle\beta_0 K^*\rangle \times \langle\beta_1 K^*\rangle \times \ldots \times \langle\beta_s K^*\rangle, \quad iK^* \in \langle\beta_0 K^*\rangle.$$

Положим $\theta(\beta_j) = 2^{m_j}$, $0 \leqslant j \leqslant s$. Тогда тонкие градуировки канонического типа расширения L/K существуют в точности по следующим группам:

$$G' = \langle iK^*, \{(1+\varepsilon_{2^{r_j}})\beta_j K^*\}_{j=0}^{s}\rangle \tag{5}$$

для некоторых $r_0 = 0, 2, 3, \ldots, \min(m_0, N)$, $r_j = 0, 2, 3, \ldots, \min(m_j + 1, N)$, $j = 1, \ldots, s$.

Существует тонкая градуировка канонического типа, в которой подгруппа iK^* выделяется прямым сомножителем в градуирующей группе, если и только если $m_0 \leqslant N$.

Если $m_0 \leqslant N$, то число групп, по которым существует тонкая градуировка расширения L/K, равно $|\{m_0-1, m_1, \ldots, m_s\} \cap \{1, \ldots, N-1\}|+1$, а при $m_0 > N$ такая группа единственна.

Доказательство. Группа G раскладывается в прямое произведение 2-групп, причём это разложение можно выбрать так, чтобы в одном из прямых сомножителей лежал наперёд заданный элемент группы, в данном случае элемент iK^*. Из теоремы 5 получаем, что существует единственная градуировка расширения $L/K(i)$. Следовательно, по лемме 4 *любая* градуировка расширения L/K получается из данной в условии путём умножения каждой из компонент на элемент из группы $T_2(K(i)^*/K^*)$. С учётом описания этой группы из теоремы 6 компоненту $\beta_j K^*$ можно умножить только на $(1+\varepsilon_{2^{r_j}})$, где $1 \neq r_j \leqslant N$ (при $r_j = 1$ получили бы $1+\varepsilon_{2^{r_j}} = 0$; $r_j = 0$ допустимо — тогда компонента остаётся прежней). Кроме того, есть ещё одно ограничение на r_j, связанное с тем, что элемент $1+i$ не может быть однородным (так как $i \notin K$). Именно: при $j \in \{0, \ldots, s\}$ и $r_j \in \{m_j+2, \ldots, N\}$ имеем

$$\big(\beta_j(1+\varepsilon_{2^{r_j}})\big)^{2^{r_j-2}} K^* = (1+i)K^*,$$

поэтому должно быть $r_j \leqslant m_j + 1$ при $j \in \{0, \ldots, s\}$. Кроме того, если $r_0 = m_0 + 1$, то

$$\big(\beta_0(1+\varepsilon_{2^{r_0}})\big)^{2^{r_0-2}} K^* = \beta_0^{2^{m_0-1}}(1+i)K^* = i(1+i)K^*,$$

поэтому должно быть $r_0 \leqslant m_0$.

Мы доказали, что градуировка канонического типа может быть только по группе (5). Обратно, пусть дана любая такая группа.

Если $r_j \leqslant m_j$ для некоторого $j > 0$, то по лемме 5 можем изначально полагать, что $\beta_j' = (1+\varepsilon_{2^{r_j}})\beta_j$ — один из порождающих радикалов. В этом случае градуирующая группа с точностью до изоморфизма не меняется. Таким образом, если $r_j \leqslant m_j$, то без ограничения общности положим $r_j = 0$.

Если $m_0 \leqslant N$, то по лемме 5 верно, что

$$\langle iK^*, (1+\varepsilon_{2^{m_0}})\beta_0 K^* \rangle = \langle iK^* \rangle \times \langle (1+\varepsilon_{2^{m_0}})\beta_0 K^* \rangle$$

(при $m_0 = 1$ будем полагать, что обе части равны $\langle iK^* \rangle$), т. е. в этом случае существует тонкая градуировка канонического типа, где $\langle iK^* \rangle$ выделяется прямым сомножителем в градуирующей группе. Поэтому если $r_j = 0$ для каждого $j > 0$ и $r_0 = m_0$, то $|G'| = |G|$. Если $r_j = 0$ для каждого $j > 0$ и $r_0 < m_0$, то $G' \cong G$. Если $r_0 < m_0$ и для каждого $j > 0$ такого, что $r_j = m_j + 1$, верно, что $m_0 > m_j$, то по лемме 6 имеем $G' \cong G$. Если же существует такой $j > 0$, что $r_j = m_j + 1$ и $m_0 \leqslant m_j$, то выберем j так, чтобы m_j было максимально. Без ограничения общности будем полагать, что $j = 1$. Рассмотрим группу

$$H = \langle (1+\varepsilon_{2^{m_0}})\beta_0 K^* \rangle \times \langle (1+\varepsilon_{2^{m_1+1}})\beta_1 K^* \rangle \times \langle \beta_2 K^* \rangle \times \ldots \times \langle \beta_s K^* \rangle \subset L^*/K^*.$$

Последнее включение следует из того, что

$$K(\beta_0, \beta_1) = K\big((1+\varepsilon_{2^{m_0}})\beta_0,\ (1+\varepsilon_{2^{m_1+1}})\beta_1\big)$$

и

$$\langle(1+\varepsilon_{2^{m_0}})\beta_0K^*,\,(1+\varepsilon_{2^{m_1+1}})\beta_1K^*\rangle=\langle(1+\varepsilon_{2^{m_0}})\beta_0K^*\rangle\times\langle(1+\varepsilon_{2^{m_1+1}})\beta_1K^*\rangle.$$

Следовательно, группе H соответствует тонкая градуировка расширения L/K, откуда вытекает, что $|H|=|G|$. Из леммы 6 следует, что $G'\cong H$. Из этих рассуждений также получаем, что количество градуирующих групп с точностью до изоморфизма равно $|\{m_0-1,m_1,\ldots,m_s\}\cap\{1,\ldots,N-1\}|+1$.

Если $m_0>N$, то для любого j, $0\leqslant j\leqslant s$, верно, что $r_j\leqslant N<m_0$, и, в частности, из пункта 1) леммы 5 получаем, что $\langle iK^*\rangle$ не выделяется прямым слагаемым ни в какой градуирующей группе никакой тонкой градуировки канонического типа. Поэтому по лемме 6 получаем, что $G'\cong G$, т. е. в этом случае градуирующая группа с точностью до изоморфизма единственна.

Во всех случаях получили, что $|G'|=|G|$. Тогда из того, что

$$K(i,\beta_0,\beta_1,\ldots,\beta_s)=K(i,(1+\varepsilon_{2^{r_0}})\beta_0,(1+\varepsilon_{2^{r_1}})\beta_1,\ldots,(1+\varepsilon_{2^{r_s}})\beta_s),$$

получаем, что G' задаёт тонкую градуировку. □

Пример 2. Рассмотрим расширение $L/K=\mathbb{Q}(i,\sqrt[4]{3})/\mathbb{Q}$. Тогда по теореме 7 существует две неизоморфные тонкие градуировки канонического типа с градуирующими группами, изоморфными группе $\mathbb{Z}_2\oplus\mathbb{Z}_4$, а именно:

$$L=\mathbb{Q}(i)\otimes\mathbb{Q}(\sqrt[4]{3}),$$
$$L=\mathbb{Q}(i)\otimes\mathbb{Q}\big((1+i)\sqrt[4]{3}\big).$$

Предложение 7. *Обозначим* $\alpha=(1+\varepsilon_{2^N})^{2^{N-2}-1}\varepsilon_{2^{N+1}}$.

1. *Верны формулы*

$$K\alpha=K(1+i)\sqrt{\varepsilon_{2^N}+\varepsilon_{2^N}^{-1}+2},$$
$$K(1+i)\alpha\ =Ki\sqrt{\varepsilon_{2^N}+\varepsilon_{2^N}^{-1}+2}.$$

2. *Пусть* $i\in L\setminus K$, $\sqrt{2}\in K$ *и* $N<\infty$. *Тогда* $\varepsilon_{2^{N+2}}\notin L$. *Если* $\varepsilon_{2^{N+1}}\in L$, *то* $\alpha\in L$, *и однороден либо элемент* α, *либо элемент* $(1+i)\alpha$.

Доказательство. Обозначим $m=\max\{k\mid\varepsilon_{2^k}\in L\}$ и предположим, что $m>N$. По теореме 5 существует единственная градуировка расширения $L/K(i)$, в которой элемент ε_{2^m} однороден по теореме 1. Следовательно, в данной градуировке расширения L/K однороден элемент $(1+\varepsilon_{2^N})^r\varepsilon_{2^m}$ для некоторого $0\leqslant r<2^N$. При этом $[K(\varepsilon_{2^m}):K]=[K(\varepsilon_{2^m}):K(i)]\cdot[K(i):K]=2^{m-N+1}$. Следовательно, необходимо, чтобы $K\big((1+\varepsilon_{2^N})^r\varepsilon_{2^m}\big)^{2^{m-N+1}}=K$. Но

$$K\big((1+\varepsilon_{2^N})^r\varepsilon_{2^m}\big)^{2^{m-N+1}}=K\big((\varepsilon_{2^{N+1}}+\varepsilon_{2^{N+1}}^{-1})^r\varepsilon_{2^{N+1}}^r\varepsilon_{2^m}\big)^{2^{m-N+1}}=$$
$$=K\big(\varepsilon_{2^m}^{r\cdot2^{m-N-1}}\varepsilon_{2^m}\big)^{2^{m-N+1}}=K\varepsilon_{2^{N-1}}^{r\cdot2^{m-N-1}+1},$$

откуда получаем, что либо $N = 2$, либо $m - N - 1 = 0$ и $2^{N-2} \mid r + 1$, т. е. $r = t \cdot 2^{N-2} - 1$, $t = 1, \ldots, 4$. Осталось заметить, что

$$(1 + \varepsilon_{2^N})^{3 \cdot 2^{N-2}-1} \varepsilon_{2^{N+1}} K^* \in \langle \alpha K^*, iK^* \rangle$$

и

$$(1 + \varepsilon_{2^N})^{4 \cdot 2^{N-2}-1} \varepsilon_{2^{N+1}} K^* \in \big\langle (1 + \varepsilon_{2^N})^{2 \cdot 2^{N-2}-1} \varepsilon_{2^{N+1}} K^*, iK^* \big\rangle,$$

причём $K(1 + \varepsilon_{2^N})^{2 \cdot 2^{N-2}-1} \varepsilon_{2^{N+1}} = K(1 + i)(1 + \varepsilon_{2^N})^{2^{N-2}-1} \varepsilon_{2^{N+1}}$. □

Пример 3. Расширение $L/\mathbb{Q} = \mathbb{Q}\big(\sqrt[4]{3}\varepsilon_{16}, \varepsilon_8\big)/\mathbb{Q}$ степени 16 имеет ровно 4 неизоморфные тонкие градуировки — все по группе $\mathbb{Z}_8 \oplus \mathbb{Z}_2$:

$$L = \mathbb{Q}\big(\sqrt[4]{3}\varepsilon_{16}\big) \otimes \mathbb{Q}(\sqrt{3}) = \mathbb{Q}\big((1 + i)\sqrt[4]{3}\varepsilon_{16}\big) \otimes \mathbb{Q}(\sqrt{3}) = \\ = \mathbb{Q}\big(\sqrt[4]{3}\varepsilon_{16}\big) \otimes \mathbb{Q}(\sqrt{2}) = \mathbb{Q}\big((1 + i)\sqrt[4]{3}\varepsilon_{16}\big) \otimes \mathbb{Q}(\sqrt{2}).$$

По теореме 7 других градуировок нет, в частности, не существует градуировки канонического типа расширения по группе, в которой подгруппа $\langle i\mathbb{Q}^* \rangle$ выделяется прямым сомножителем.

Пример 4. Рассмотрим расширение $L/K = \mathbb{Q}(\varepsilon_{16}, \sqrt[8]{7}\varepsilon_{32}, \sqrt[4]{3})/\mathbb{Q}(\sqrt{2})$. Оно имеет ровно 27 неизоморфных тонких градуировок — все по группе $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{16}$, при этом по предложению 7 либо элемент $\alpha = (1 + \varepsilon_8)\varepsilon_{16} = (1 + i)\sqrt{2 + \sqrt{2}}$ однороден, либо элемент $(1 + i)\alpha = 2i\sqrt{2 + \sqrt{2}}$ однороден. Две неизоморфные градуировки могут иметь вид

$$L = K\Big(\sqrt{7(2 + \sqrt{2})}\Big) \otimes K\big(\sqrt[4]{3}\big) \otimes K\big(\sqrt[8]{7}\varepsilon_{32}\big),$$
$$L = K\Big(\sqrt{7(2 + \sqrt{2})}\Big) \otimes K\big(\sqrt[4]{21}\big) \otimes K\big(\sqrt[8]{7}\varepsilon_{32}\big),$$

причём

$$\alpha = \sqrt{2}i \cdot \frac{\sqrt{7(2 + \sqrt{2})}}{\big(\sqrt[8]{7}\varepsilon_{32}\big)^4}$$

однороден в обеих градуировках.

3.3. Общий случай

Для каждого нечётного простого делителя p числа $[L : K]$ определим число $t_p = \max\{n \colon \varepsilon_{p^n} \in L\}$.

Замечание 8. Если $\varepsilon_p \in K$, то условие $t_p = \infty$ влечёт, что $\varepsilon_{p^r} \in K$ для любого r. Действительно, по [3, с. 252] степень расширения $[K(\varepsilon_{p^{r+1}}) : K(\varepsilon_{p^r})]$ равна 1 или p, причём если $[K(\varepsilon_{p^{r+1}}) : K(\varepsilon_{p^r})] = p$, то для любого $r' \geqslant r$ будем иметь $[K(\varepsilon_{p^{r'+1}}) : K(\varepsilon_{p^{r'}})] = p$, что противоречит конечности расширения L/K.

Теорема 8. *Пусть L/K — расширение Галуа степени $[L : K] = 2^n \cdot m$, $2 \nmid m$, с тонкой G-градуировкой. Тогда*

1) *существует единственное подрасширение* P/K *степени* $[P:K]=2^n$ *и оно является расширением Галуа*;
2) *группа* $T_m(G)$ *определена однозначно*;
3) *если* p *— простой делитель* m*, то при* $\varepsilon_p \in K$ *компоненты, соответствующие элементам* $T_p(G)$*, определены однозначно, иначе они определены с точностью до умножения на* ε_{p^r} *для некоторых* $r \leqslant t_p$;
4) *если* p *— простой делитель* m*, такой что* $\varepsilon_p \notin K$*, то*

$$\varepsilon_{p^r} \in K\Big(\{L_g\}_{g\in \bigoplus\limits_{q<p} T_q(G)}\Big)$$

для каждого конечного $r \leqslant t_p$.

Доказательство. Докажем пункт 1). Если $i \notin L$, то любой квадратный радикал $r \in L \setminus K$ однороден, поэтому $P = K(\{r \in L \setminus K \mid r^2 \in K\})$ — единственное подполе степени 2^n. Если $i \in K$, то единственность следует из того, что по теореме 1 любой элемент α, такой что $\alpha K^* \in T_2(L^*/K^*)$, однороден.

Пусть $i \in L \setminus K$. Тогда i однороден по теореме 1 и тонкая градуировка расширения $L/K(i)$ единственна по теореме 5. Отсюда следует, что подполе $P = K(\{L_g\}_{g\in T_2(G)})$ определено однозначно (т. е. P не зависит от выбора тонкой градуировки расширения L/K). Так как применение автоморфизма переводит тонкие градуировки в себя, то из вышесказанного следует, что $\sigma P = P$ для любого $\sigma \in \mathrm{Gal}(L/K)$, откуда вытекает, что P/K — расширение Галуа.

Единственность подполя такой степени следует из того, что $P = K(\alpha_1,\ldots,\alpha_t)$, $[P:K] = \theta(\alpha_1)\cdot\ldots\cdot\theta(\alpha_r)$, так как существует тонкая градуировка расширения L/K. Действительно, пусть P' — другое подполе, такое что $[P':K]=2^n$. Отметим, что $i \in P'$, иначе $[P'(i):P']=2$, что невозможно. Тогда для всякого j, $1 \leqslant j \leqslant t$, имеем $[P'(\alpha_j):P'] \mid \theta(\alpha_j)$, так как по критерию приводимости двучлена [3, с. 252] имеем либо $\alpha_j^{\theta(\alpha_j)} \in K^2$, либо $\alpha_j^{\theta(\alpha_j)} \in -4K^4$, и в обоих случаях приходим к двучлену такого же вида. Следовательно, так как $\theta(\alpha_j) \mid 2^n$, имеем $[P'(\alpha_j):P']=1$, т. е. $\alpha_j \in P'$. Отсюда следует, что $P \subseteq P'$, а так как $[P:K]=[P':K]$, то $P'=P$.

Докажем пункт 2). Из единственности подполя P из пункта 1) следует, что $T_m(G)$ изоморфна градуирующей группе тонкой градуировки расширения L/P, а из теоремы 4 следует единственность этой градуирующей группы.

Докажем пункт 3). Если $\varepsilon_p \in K$, то по теореме 1 любой элемент α, такой что $\alpha K^* \in T_p(L^*/K^*)$, однороден. Если $\varepsilon_p \notin K$, то после свёртки градуировки относительно проекции $G \to \bigoplus\limits_{q\geqslant p} T_q(G)$ по лемме 3 имеем $\varepsilon_p \in F = K\Big(\{L_g\}_{g\in \bigoplus\limits_{q<p} T_q(G)}\Big)$, и тогда компоненты в получившейся градуировке, соответствующие элементам из $T_p(G)$, определены однозначно, поэтому компоненты в исходной градуировке, соответствующие элементам из $T_p(G)$, определены с точностью до умножения на элемент из группы $T_p(F^*/K^*)$, которая по [8, следствие 1.4] порождена $\varepsilon_{p^r}K^*$ для таких r, что $\varepsilon_{p^r} \in L$.

Докажем пункт 4). Неоднородность ε_p следует из леммы 2. Аналогично пункту 3) рассмотрим свёртку градуировки относительно проекции $G \to \bigoplus\limits_{q\geqslant p} T_q(G)$ и обозначим $F = K\Big(\{L_g\}_{g\in \bigoplus\limits_{q<p} T_q(G)}\Big)$. Тогда по пункту 3) $\varepsilon_p \in F$ и ε_{p^r} однороден в градуировке расширения L/F для любого конечного $r \leqslant t_p$. Если $t_p = \infty$, то $\varepsilon_{p^r} \in F$ ввиду конечности расширения L/F и замечания 8.

Предположим, что $t_p < \infty$ и $\varepsilon_{p^{t_p}} \notin F$. Так как рассматриваемая градуировка расширения L/F есть свёртка градуировки расширения L/K, то из однородности компоненты $F\varepsilon_{p^{t_p}}$, не равной F, следует однородность компоненты $K\alpha\varepsilon_{p^{t_p}}$, не равной K, для некоторого $\alpha \in T_p(F^*/K^*)$ (аналогично лемме 6 с учётом того, что элемент $\varepsilon_{p^{t_p}}$ однороден в любой градуировке расширения L/F). Из этого следует, что $\big([F:K], \theta(\alpha)\big) = 1$, откуда получаем по [8, следствие 1.4], что α — корень из единицы степени $\theta(\alpha)$. Следовательно, $\alpha\varepsilon_{p^{t_p}} = \varepsilon_{p^{t_p}}^k$, $0 \leqslant k < p^{t_p}$. Так как $\alpha\varepsilon_{p^{t_p}} \notin K$, то $k \neq 0$, и значит, ε_p однороден, что противоречит его неоднородности. □

Замечание 9. Доказанная теорема позволяет описать градуировки куммерова расширения, что было сделано выше непосредственно.

Пример 5. Положим

$$K = \mathbb{Q}\Bigg(\varepsilon_5,\ \varepsilon_{11} + \varepsilon_{11}^4 + \varepsilon_{11}^9 + \varepsilon_{11}^5 + \varepsilon_{11}^3 = \frac{1+\sqrt{-11}}{2},\ \frac{\varepsilon_{11} + \varepsilon_5^{-1}\varepsilon_{11}^4 + \varepsilon_5^{-2}\varepsilon_{11}^5 + \varepsilon_5^{-3}\varepsilon_{11}^9 + \varepsilon_5^{-4}\varepsilon_{11}^3}{\varepsilon_{25}}\Bigg).$$

1. Пусть $L = K(\varepsilon_{25})$. Тогда $[L:K] = 5$, $\varepsilon_{11} \notin K$, $\varepsilon_{11} \in L$, откуда следует, что $K(\varepsilon_{25}) = K(\varepsilon_{11}) = L$.

В этом случае по теореме 2 существует единственная нетривиальная градуировка расширения L/K, которая имеет вид

$$L = K \oplus K\varepsilon_{25} \oplus K\varepsilon_{25}^2 \oplus K\varepsilon_{25}^3 \oplus K\varepsilon_{25}^4,$$

а элемент ε_{11} не является однородным.

2. Пусть $L' = K(\varepsilon_{25},\ \sqrt[11]{7})$. Тогда одиннадцать градуировок

$$L' = \bigoplus_{j=0}^{4}\bigoplus_{k=0}^{10} K\varepsilon_{25}^j(\sqrt[11]{7}\varepsilon_{11}^l)^k, \quad l = 0, 1, \ldots, 10,$$

попарно неизоморфны. Отметим, что $\mathrm{Gal}(L'/K) \cong \mathbb{Z}_{11} \leftthreetimes \mathbb{Z}_5$.

Если для расширения Галуа L/K существует тонкая G-градуировка, то в таком случае можно описать группу Галуа $\mathrm{Gal}(L/K)$ этого расширения.

Замечание 10. Если $P = K(\alpha_1, \ldots, \alpha_s)$ — промежуточное поле, порождённое однородными радикалами $\alpha_1, \ldots, \alpha_s \in h(L)$, то P/K — расширение Галуа в точности тогда, когда $\varepsilon_{\theta(\alpha_j)} \in P$ для всех $j = 1, \ldots, s$.

Обозначим для $p \mid [L:K]$

$$L_{(p)} = \bigoplus_{g \in T_p(G)} L_g, \quad L^{(p)} = \bigoplus_{g \in \bigoplus\limits_{q \leqslant p} T_q(G)} L_g.$$

Пусть также множество простых делителей $\{p_1, \ldots, p_k\}$ степени $[L:K]$ упорядочено по возрастанию. Отметим, что $L^{(p)}/K$ — расширение Галуа для каждого p, что следует из теоремы 8 и замечания 10.

Предложение 8. *Пусть L/K — расширение Галуа с тонкой G-градуировкой. Тогда для $j = 1, \ldots, k-1$*

1) *если $\varepsilon_{p_{j+1}} \in K$, то $L_{(p_{j+1})}/K$ — расширение Галуа и*

$$\operatorname{Gal}\bigl(L^{(p_{j+1})}/K\bigr) \cong \operatorname{Gal}\bigl(L^{(p_j)}/K\bigr) \oplus \operatorname{Gal}\bigl(L_{(p_{j+1})}/K\bigr);$$

2) *если $\varepsilon_{p_j} \notin K$, то*

$$\operatorname{Gal}\bigl(L^{(p_{j+1})}/K\bigr) \cong T_{p_{j+1}}(G) \leftthreetimes \operatorname{Gal}\bigl(L^{(p_j)}/K\bigr).$$

Доказательство. Докажем пункт 1). Так как по теореме 8 элемент $\varepsilon_{p_{j+1}^r}$ однороден для всякого конечного $r \leqslant t_p$, то $\varepsilon_{p_{j+1}^r} \in L_{(p_{j+1})}$, поэтому по замечанию 10 $L_{(p_{j+1})}/K$ — расширение Галуа. Кроме того, $L_{(p_{j+1})} \cap L^{(p_j)} = K$, так как степени соответствующих расширений взаимно просты. Следовательно,

$$\operatorname{Gal}\bigl(L^{(p_{j+1})}/K\bigr) \cong \operatorname{Gal}\bigl(L^{(p_j)}/K\bigr) \oplus \operatorname{Gal}\bigl(L_{(p_{j+1})}/K\bigr).$$

Докажем пункт 2). Из теоремы 8 следует, что

$$T_{p_{j+1}}(G) \cong T_{p_{j+1}}\bigl(L^{(p_{j+1})}/L^{(p_j)}\bigr)$$

и $\varepsilon_{p^r} \in L^{(p_j)}$ для любого конечного $r \leqslant t_{p_j}$, т. е. $L^{(p_{j+1})}/L^{(p_j)}$ — куммерово расширение с абелевой p_{j+1}-группой Галуа. Так как его степень нечётна, то по предложениям 3 и 5 имеем

$$T_{p_{j+1}}(G) \cong \operatorname{Gal}\bigl(L^{(p_{j+1})}/L^{(p_j)}\bigr).$$

Более того, расширение $L^{(p_{j+1})}/L^{(p_j)}$ порождается некоторыми однородными радикалами $\alpha_1, \ldots, \alpha_s$ из $L_{(p_{j+1})}$, их степени взаимно просты со степенью $[L^{(p_j)}:K]$, поэтому по теореме о побочных иррациональностях

$$\operatorname{Gal}\bigl(L^{(p_j)}/K\bigr) \cong \operatorname{Gal}\bigl(L^{(p_{j+1})}/K(\alpha_1, \ldots, \alpha_s)\bigr).$$

Отсюда, учитывая, что $L^{(p_j)}/K$ — расширение Галуа и

$$\operatorname{Gal}\bigl(L^{(p_{j+1})}/L^{(p_j)}\bigr) \lhd \operatorname{Gal}\bigl(L^{(p_{j+1})}/K\bigr),$$

причём порядки групп $\operatorname{Gal}\bigl(L^{(p_{j+1})}/K(\alpha_1, \ldots, \alpha_s)\bigr)$ взаимно просты и в произведении дают $\bigl|\operatorname{Gal}\bigl(L^{(p_{j+1})}/K\bigr)\bigr|$, имеем

$$\operatorname{Gal}\bigl(L^{(p_{j+1})}/K\bigr) = \operatorname{Gal}\bigl(L^{(p_{j+1})}/L^{(p_j)}\bigr) \leftthreetimes \operatorname{Gal}\bigl(L^{(p_{j+1})}/K(\alpha_1, \ldots, \alpha_s)\bigr).$$

С учётом двух последних изоморфизмов получаем пункт 2) теоремы. □

Пример 6. Рассмотрим расширение Галуа $L/\mathbb{Q}$, где $L = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{7})$, с группой Галуа $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_3 \leftthreetimes (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$. Отметим, что $\varepsilon_3 \in \mathbb{Q}(i, \sqrt{3})$. У расширения $L/\mathbb{Q}$ существуют неизоморфные тонкие градуировки по группам $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ и $\mathbb{Z}_4 \oplus \mathbb{Z}_3$, например:

$$L = \mathbb{Q}(i) \otimes \mathbb{Q}(\sqrt{3}) \otimes \mathbb{Q}(\sqrt[3]{7}),$$
$$L = \mathbb{Q}(i) \otimes \mathbb{Q}(\sqrt{3}) \otimes \mathbb{Q}(\varepsilon_3 \sqrt[3]{7}),$$
$$L = \mathbb{Q}((1+i)\sqrt{3}) \otimes \mathbb{Q}(\sqrt[3]{7}).$$

Литература

[1] Артин Э. Теория Галуа. — М.: МЦНМО, 2008.

[2] Бадулин Д. А., Канунников А. Л. Градуировки куммеровых квадратичных расширений // Вестн. Моск. ун-та. Сер. 1. Матем., мех. — 2022. — № 2. — С. 67—71.

[3] Ленг С. Алгебра. — Мир, 1968.

[4] Bahturin Yu. A., Zaicev M. V., Sehgal S. K. Group gradings on associative algebras // J. Algebra. — 2001. — Vol. 241. — P. 677—698.

[5] Nästäsescu C., Van Oystaeyen F. Graded Ring Theory. — Amsterdam: North-Holland, 2004.

[6] Albu T. Cogalois Theory. — CRC Press, 2003. — (Pure Appl. Math.).

[7] Albu T. Applications of cogalois theory to elementary field arithmetic // Advances in Ring Theory / D. Van Huynth and S. R. López-Permouth, eds. — Birkhäuser, 2010. — P. 1—17.

[8] Gay D., Velez W. Y. The torsion group of a radical extension // Pacific J. Math. — 1981. — Vol. 92, no. 2. — P. 317—327.

[9] Milne J. S. Fields and Galois Theory. — 2012.

[10] De Orozco M. A., Velez W. Y. The torsion group of a field defined by radicals // J. Number Theory. — 1984. — Vol. 19, no. 2. — P. 283—294.