Математические заметки

Том 117 выпуск 1 январь 2025

УДК 512.623

Поля алгебраических чисел, мультипликативные группы которых свободны по модулю группы единиц

К. Н. Пономарев

Показано, что мультипликативная группа поля алгебраических чисел оказывается свободной по модулю группы единиц, если группа значений любого неархимедова нормирования этого поля образует свободную группу.

Библиография: 7 названий.

Ключевые слова: поле, поле алгебраических чисел, нормирование поля, неархимедово нормирование, группа единиц поля алгебраических чисел, свободная группа.

DOI: https://doi.org/10.4213/mzm14263

Изучаем строение мультипликативной группы поля *алгебраических чисел*, полученного добавлением к полю рациональных чисел алгебраических элементов.

Мультипликативное строение такого поля K конечной степени хорошо известно, оно было установлено Сколемом в 1947 г. Мультипликативная группа поля K образует свободную группу по модулю подгруппы кручения. А в 1972 г. Мэй указал пример поля K бесконечной степени, мультипликативная группа которого по модулю кручения не является свободной [1].

Возникает проблема выделения классов полей алгебраических чисел бесконечной степени, мультипликативные группы которых образуют свободные группы по модулю подгруппы кручения (см. [2], [3; гл. 4, § 16]). Находим подходы к решению этой задачи.

Больший класс полей образуют поля алгебраических чисел K, мультипликативные группы которых свободны по модулю группы единиц $\mathscr{O}_K^*$ кольца целых чисел $\mathscr{O}_K$ этого поля. В статье определяем широкий класс полей, обладающих этим свойством.

Теорема 1. *Рассмотрим любое поле алгебраических чисел K. Если для любого неархимедова нормирования v поля K группа его значений $v(K^*)$ образует свободную группу, то фактор его мультипликативной группы $K^*/\mathscr{O}_K^*$ является свободной группой.*

Группы значений неархимедовых нормирований поля алгебраических чисел – абелевы группы без кручения унитарного ранга. Каждая такая группа оказывается свободной тогда и только тогда, когда она получается пополнением бесконечной циклической группы элементом конечной высоты (см. [4; гл. 8, § 30]). Это означает конечность индекса ветвления нормирования в расширении $K/\mathbb{Q}$. Поэтому условие свободы группы значений неархимедова нормирования w поля K естественно трактовать как конечную разветвленность этого нормирования.

Поле алгебраических чисел K будем называть *всюду конечно разветвленным*, если любое его неархимедово нормирование конечно разветвлено над полем рациональных чисел. Подчеркнем: при этом не требуется, чтобы индексы ветвления всех неархимедовых нормирований поля K имели общую верхнюю границу, чтобы они были ограничены в совокупности.

Утверждение теоремы 1 можно сформулировать в такой эквивалентной форме.

Следствие 1. *Если поле K является всюду конечно разветвленным расширением поля рациональных чисел, тогда фактор мультипликативной группы поля алгебраических чисел K по группе единиц $K^*/\mathscr{O}_K^*$ образует свободную группу.*

Поле K конечной степени представляет всюду конечно разветвленное поле, для такого поля утверждение вытекает из теоремы Сколема. Поэтому в статье предполагаем поле алгебраических чисел K бесконечной степени.

В течение статьи любое поле предполагается полем алгебраических чисел. *Числовым полем* называем поле алгебраических чисел конечной степени.

Все необходимые для понимания работы понятия и факты изложены в книгах [3], [5].

1. Предварительные замечания. Предположим K полем алгебраических чисел. Рассматриваем неархимедовы аддитивные нормирования w (показатели) этого поля – такие отображения $w\colon K^* \to w(K^*)$ в абелеву упорядоченную группу значений $w(K^*)$, которые удовлетворяют тождествам при любых $x, y \in K^*$:

1) $w(xy) = w(x) + w(y)$;
2) $w(x+y) \geqslant \min\{w(x), w(y)\}$.

Лемма 1 (о факторах). *Рассмотрим расширение поля алгебраических чисел K до поля алгебраических чисел L. Обозначим $\mathscr{O}_L$ кольцо целых чисел поля L, общая часть $\mathscr{O}_L \cap K$ образует кольцо целых чисел поля K: $\mathscr{O}_K = \mathscr{O}_L \cap K$. Утверждается, что группа единиц $\mathscr{O}_K^*$, (обратимых элементов кольца $\mathscr{O}_K$) также совпадает с общей частью $\mathscr{O}_K^* = \mathscr{O}_L^* \cap K$.*

В частности, композиция вложения и факторморфизма $K^* \hookrightarrow L^* \rightarrowtail L^*/\mathscr{O}_L^*$ пропускается через фактор $K^*/\mathscr{O}_K^*$. Так определяется вложение факторгрупп

$$K^*/\mathscr{O}_K^* \hookrightarrow L^*/\mathscr{O}_L^*. \tag{1}$$

Таким же образом получается вложение факторов по периодической части:

$$K^*/t(k^*) \hookrightarrow L^*/t(L^*). \tag{2}$$

В самом деле, это следует из того факта, что группа единиц $\mathscr{O}_K^*$ – общее ядро всех неархимедовых нормирований поля K (см. [3; гл. 3, § 6, следствие 6.2]). А все такие нормирования получаются ограничениями неархимедовых нормирований поля L.

Вложение факторов по периодической части получается, если в рассуждении использовать все нормирования, включая архимедовы. Это объясняет утверждение.

Будем использовать эту лемму, считать фактор $K^*/\mathscr{O}_K^*$ вложенным в фактор $L^*/\mathscr{O}_L^*$, а фактор $K^*/t(K)$ вложенным в $L^*/t(L)$.

2. Теорема Понтрягина и группы унитарного ранга. Будем рассматривать группы без кручения. Соответственно под рангом группы понимаем ее ранг без кручения.

Лемма 2. *Рассмотрим свободную группу F конечного ранга $n > 1$, а в ней максимальную подгруппу H ранга $m < n$. Утверждается, что любая максимальная подгруппа G ранга $n-m$, которая удовлетворяет условию $G \cap H = 0$, прямо дополняет H до F, т.е. выполняется равенство $F = G \oplus H$.*

Доказательство. Действительно, максимальная подгруппа H ранга m группы F *изолированная*: для любого $x \in F$ и натурального n, если $nx \in H$, то и $x \in H$.

В силу этого свойства из структуры подгрупп свободной группы, установленной в лемме 15.4 [6], следует, что одну часть базиса группы F можно выбрать из базисных элементов подгруппы H.

В силу условия $G \cap H = 0$ другую дополнительную часть базиса можно выбрать из базиса максимальной группы G ранга $n - m$. Это доказывает лемму.

Будем применять это утверждение при $m = 1$ в случае максимальных подгрупп унитарного ранга.

В силу теоремы Понтрягина [6; гл. 3, § 19] счетная абелева группа A, которая не имеет кручения, является свободной тогда и только тогда, когда каждая ее подгруппа конечного ранга свободна. Это эквивалентно условию максимальности для возрастающих цепей подгрупп ограниченного ранга.

Теорема 2. *Рассмотрим группу A, которая представляется объединением башни свободных абелевых групп счетного ранга*:

$$A_1 \leqslant A_2 \leqslant \cdots, \qquad A = \bigcup A_i. \tag{3}$$

Утверждается, что группа A образует свободную группу тогда и только тогда, когда все ее подгруппы унитарного ранга являются свободными группами. Иными словами, условие теоремы Понтрягина для такой группы – условие максимальности – достаточно проверять только для подгрупп ранга один.

Доказательство. В самом деле, *необходимость* условия следует из теоремы Понтрягина. Будем проверять *достаточность*, используем теорему Понтрягина, установим условие максимальности для подгрупп ранга n индукцией по n.

База индукции при $n = 1$ обеспечена условием теоремы. Поэтому рассмотрим подгруппу B ранга $n > 1$. Будем предполагать, что для групп меньшего ранга условие максимальности выполнено. Будем этим пользоваться. Установим, что группа B является свободной группой.

В группе B определим башню свободных групп:

$$B_1 \leqslant B_2 \leqslant \cdots, \quad B_i = B \cap A_i, \qquad i \in \mathbb{N}. \tag{4}$$

Ранг каждого этажа B_i не превосходит n. Заметим, что число тех этажей башни, ранг которых строго меньше n, конечное. Отбросим из башни (4) эти члены, пронумеруем заново, и считаем далее, что для каждого натурального i выполняется включение $B_i \subseteq A_i$. При этом каждая группа B_i (как подгруппа свободной группы A_i) образует свободную группу ранга $n > 1$.

Выберем в группе B_1 какую-нибудь максимальную подгруппу унитарного ранга $\mathscr{A}_1$. Далее для каждого $i = 2, 3, \ldots$ продолжаем эту подгруппу до максимальной подгруппы унитарного ранга $\mathscr{A}_2, \mathscr{A}_3, \ldots$ соответственно в группе $B_2, B_3, \ldots$. Получается неубывающая последовательность подгрупп группы B унитарного ранга. По условию теоремы эта последовательность на некотором конечном шаге стабилизируется. Отбросим все предыдущие члены ряда (4), и считаем, что сразу $\mathscr{A}_1 = \mathscr{A}_2 = \cdots = \mathscr{A}$.

Используем лемму 2 и дополним $\mathscr{A}$ до прямого слагаемого в группе B_1: $B_1 = \mathscr{A} \oplus \mathscr{B}_1$. При этом $\mathscr{B}_1$ образует максимальную подгруппу в группе B_1 ранга $n-1$ для нее выполняется условие $\mathscr{A} \cap \mathscr{B}_1 = 0$.

Далее продолжаем $\mathscr{B}_1$ до максимальной подгруппы $\mathscr{B}_2$ в группе B_2 ранга $n-1$. $\mathscr{B}_1$ – существенная подгруппа в $\mathscr{B}_2$, эти группы не имеют кручения, поэтому также будет выполняться условие $\mathscr{B}_2 \cap \mathscr{A} = 0$. Значит $B_2 = \mathscr{A} \oplus \mathscr{B}_2$.

Продолжаем, и получаем неубывающую последовательность $\mathscr{B}_1 \subseteq \mathscr{B}_2 \subseteq \cdots$ подгрупп ранга $n-1$, для которой при любом i выполняется равенство: $B_i = \mathscr{A} \oplus \mathscr{B}_i$. По предположению индукции она стабилизируется. Значит стабилизируется сама последовательность (4). Группа B оказывается свободной.

Тогда в силу теоремы Понтрягина свободной будет сама группа A. Теорема доказана.

3. Высота элементов в группах без кручения. Будем изучать абелевы группы без кручения.

Группа без кручения унитарного ранга является рациональной группой, она составляется из делителей (корней) нетривиального элемента. Распознать такую свободную группу можно по *высотным последовательностям* элементов (см. [7; гл. 13, § 85]). Будем использовать эквивалентное этому понятие.

Рассмотрим аддитивную абелеву группу без кручения A, а в ней элемент $a \in A$. *Порядками делителей* элемента a в группе A называем множество натуральных чисел:

$$S_A(a) = \{n \in \mathbb{N} \mid \text{ для которых } a \in nA\}.$$

В случае мультипликативной группы A *порядки корней* элемента определяются через степени:

$$S_A(a) = \{n \in \mathbb{N} \mid \text{ для которых } a \in A^n\}.$$

Будем говорить, что элемент *a ограниченный в группе A*, если порядки его делителей (соответственно его корней) образуют конечное множество натуральных чисел, $|S_A(a)| < \infty$. Понятно, что такой элемент должен быть ненулевым (соответственно, неединичным) элементом группы.

Замечание 1 (свобода и ограниченность). В силу строения групп унитарного ранга (см. [4; гл. 8, § 30], также [7; гл. 13, § 85]) группа без кручения унитарного ранга является свободной группой тогда и только тогда, когда любой ее ненулевой элемент будет ограниченным в ней.

В группах без кручения ограниченные элементы обладают простой структурой порядков делителей в силу следующей леммы, которая выводится из упражнения 1 в [7] из того же раздела на с. 133.

Лемма 3. *Для аддитивной группы A без кручения и ее ненулевого элемента $a \in A$, $a \neq 0$, частично упорядоченное множество порядков делителей $S(a)$ с отношением делимости образует решетку. В этой решетке для любых $n, m \in S(a)$ получается $n \wedge m = (n, m)$ – наибольший общий делитель, а $n \vee m = [n, m]$ – наименьшее общее кратное.*

Значит, если элемент a ограниченный в группе A, $S_A(a)$ образует конечное множество, то оно образует полную решетку: найдется натуральное число $h_A(a) \in \mathbb{N}$, для которого $S_A(a)$ составлено из его делителей:

$$S_A(a) = \{m \in \mathbb{N}\colon m \mid h_A(a)\}.$$

Это число $h_A(a)$ называем *высотой* этого элемента в группе. Таким образом, высота определяется соотношением $h_A(a) = \max S(a)$. Здесь используем отношение частичного порядка на $S(a)$, отвечающего делимости элементов. Ограниченные элементы группы также будем называть элементами *конечной высоты*.

Равенство $h(a) = 1$ означает, что элемент a в группе A порождает максимальную подгруппу унитарного ранга – свободную группу ранга 1. В общем случае элемент выражается как $a = h(a)c$ через порождающий c максимальной подгруппы A унитарного ранга, которая включает a. Значит высота совпадает с индексом подгруппы, порожденной элементом a: $h(a) = |A : \langle a \rangle|$.

Замечание 2 (консервативность высоты). Рассмотрим расширение групп без кручения $A \hookrightarrow B$, в котором подгруппа A образует максимальную подгруппу B ранга n. Такая подгруппа изолированная: для $b \in B$ и натурального m если выполняется включение $mb \in A$; тогда должно быть $b \in A$. Отсюда заключаем, что для любого элемента $a \in A$ его высота в подгруппе A совпадает с высотой в группе B, $h_A(a) = h_B(a)$.

В частности, при $n = 1$ получается, что порядки делителей $S_B(a)$ и высота элемента $h_B(a)$ группы B определяются его порядками делителей и высотой в максимальной подгруппе $A \leqslant B$ унитарного ранга, содержащей элемент a: $S_A(a) = S_B(a)$, $h_A(x) = h_B(x)$. Поэтому в свободной группе высота каждого ненулевого элемента ограниченная. Значит, ненулевые элементы свободной группы ограниченные в ней.

Лемма 4. *Рассмотрим абелеву группу без кручения A, а в ней изолированную (сервантную) подгруппу $B \leqslant A$. Факторгруппа A/B также не имеет кручения. Рассматриваем канонический эпиморфизм $^-\colon A \to A/B$, определенный по правилу $x \to \overline{x} = x + B$. Утверждается, что для любого элемента $x \in A$ выполняется включение: $S_A(x) \subseteq S_{A/B}(\overline{x})$.*

В частности, если элемент x ограниченный в факторгруппе A/B (множество $S_{A/B}(\overline{x})$ конечное), то элемент будет ограниченным и в самой группе A.

Доказательство. В самом деле. Включение $S_A(x) \subseteq S_{A/B}(\overline{x})$ очевидно. Ведь если $x \in nA$, то $\overline{x} \in n\overline{A}$. Это доказывает лемму.

В заключение раздела напомним, что высотная последовательность элемента x абелевой группы: $\chi(x) = (h_2(x), h_3(x), \dots)$ составляется из значения p – высоты элемента x в этой группе для различных простых $2, 3, \dots, p \dots$. Она образована степенями примарного разложения его высоты $h(x) = 2^{h_2(x)} 3^{h_3(x)} \cdots p^{h_p(x)} \cdots$. Значит ограниченные элементы абелевой группы без кручения – это такие элементы, p – высота которых при любом простом p оказывается конечной, причем почти всегда (за исключением конечного множества простых p) она оказывается унитарной.

4. Когда фактор мультипликативной группы поля свободный.

Теорема 3 (критерий). *Рассмотрим поле алгебраических чисел K бесконечной степени, его мультипликативную группу K^*, и подгруппу в ней $N < K^*$. Предположим, что для любого подполя $L < K$ конечной степени над $\mathbb{Q}$ мультипликативная группа L^* по модулю подгруппы $L^* \cap N$ образует свободную группу счетного ранга. Утверждается, что вся группа K^* является свободной по модулю подгруппы N тогда и только тогда, когда высота каждого нееденичного элемента факторгруппы K^*/N конечная.*

Для доказательства представим поле K объединением башни расширений поля $\mathbb{Q}$ конечной степени: $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots$, $K = \bigcup K_i$. Тогда мультипликативная группа K^* представляется объединением башни мультипликативных групп конечной степени – $K^* = \bigcup K_i^*$. Факторгруппа K^*/N представляется объединением башни факторгрупп $K_i^*/(K_i^* \cap N)$, по условию теоремы – свободных групп счетного ранга.

В силу утверждения теоремы 2 такая группа является свободной тогда и только тогда, когда свободными являются все подгруппы K^*/N ранга один. А это означает ограниченность каждого нетривиального элемента факторгруппы. Это доказывает теорему.

Будем применять эту теорему в случае абелевой группы без кручения K^*/N для $N = \mathscr{O}_K^*$, либо в случае $N = t(K^*)$. Хорошо известно, что если $L < K$ подполе конечной степени, то фактор $L/L \cap \mathscr{O}_K^* = L/\mathscr{O}_L^*$ образует свободную группу счетного ранга (см. [7; гл. 18, § 127, раздел 2]). Из теоремы Сколема следует, что фактор $L^*/t(L^*)$ также образует свободную группу счетного ранга. Поэтому начальные условия теоремы для таких значений N оказываются выполненными. Остается проверять только заключительное утверждение о конечности высоты нетривиальных элементов.

Лемма 5. *Рассмотрим поле алгебраических чисел K. Утверждается, что если фактор $K^*/t(K)$ образует свободную группу, то и фактор $K^*/\mathscr{O}_K^*$ является свободной группой.*

В самом деле, абелева группа $K^*/\mathscr{O}_K^*$ не имеет кручения. Она изоморфна факторгруппе группы $K^*/t(K)$ по подгруппе $\mathscr{O}_K^*/t(K)$.

Если факторгруппа $K^*/t(K)$ свободная группа, то все ее нетривиальные элементы ограниченные в силу теоремы 3. В силу леммы 4 все нетривиальные элементы фактора $K^*/\mathscr{O}_K^*$ также оказываются ограниченными. В силу теоремы 3 факторгруппа $K^*/\mathscr{O}_K^*$ является свободной группой. Это доказывает утверждение.

Лемма 6. *Рассмотрим любое поле алгебраических чисел K, обозначим V – множество неархимедовых нормирований этого поля. Пусть $N = \mathscr{O}_K^* = \bigcap_{v \in V} \ker v$.*

Утверждается, что для произвольного $x \in K^*/N$, $x \neq N$ *и любого* $v \in V$ *в факторгруппе* K^*/N *выполняется включение* $S(x) \subseteq S(v(x))$.

В частности, если элемент $v(x)$ *ограниченный в группе значений* $v(K^*)$, *то и сам элемент* x *является ограниченным в факторе* K^*/N, *причем выполняется неравенство* $h(x) \leqslant h(v(x))$.

Доказательство. В самом деле, если $v(x) = 1$, то утверждение выполняется, поскольку $S(v(x)) = S(1) = \mathbb{N}$. А в случае $v(x) \neq 1$ утверждение следует из мультипликативности нормирования v. Ведь если $n \in S(x)$, то найдется $y \in K^*$, для которого $xN = y^n N$. Значит $v(x) = v(y)^n$, и $n \in S(v(x))$. Это доказывает лемму.

Выведем утверждение теоремы 1. Рассмотрим любое поле алгебраических чисел K, обозначим V – множество неархимедовых нормирований этого поля.

Докажем теорему. Пусть для любого неархимедова нормирования $v \in V$ поля K группа его значений $v(K^*)$ образует свободную группу. Значит высота каждого значения $v(x)$, $x \in K^*$, ограничена в группе значений, $h(v(x)) < \infty$. Проверим, что фактор мультипликативной группы $K^*/\mathscr{O}_K^*$ является свободной группой. Для этого используем теорему 3 при $N = \mathscr{O}_K^*$.

Рассмотрим произвольный $x \in K^*/N$, $x \neq N$. В силу леммы 6 он является ограниченным, $h(x) < \infty$. Заключение следует из теоремы 3. Это доказывает теорему 1.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] W. May, "Multiplicative groups of fields", *Proc. London Math. Soc.* (3), **24** (1972), 295–306.

[2] W. May, "Fields with free multiplicative groups modulo torsion", *Rocky Mountain J. Math.*, **10**:3 (1980), 599–604.

[3] G. Karpilovsky, *Field Theory. Classical Foundations and Multiplicative Groups*, Monogr. Textbooks Pure Appl. Math., **120**, Marcel Dekker, New York, 1988.

[4] А. Г. Курош, *Теория групп*, Наука, М., 1967.

[5] О. Зарисский, П. Самюэль, *Коммутативная алгебра*, т. 1, ИЛ, М., 1963.

[6] Л. Фукс, *Абелевы группы*, т. 1, Мир, М., 1974.

[7] Л. Фукс, *Абелевы группы*, т. 2, Мир, М., 1977.

К. Н. Пономарев
Новосибирский государственный технический университет
E-mail: linalgebra@mail.ru

Поступило
14.02.2024
Принято к публикации
10.04.2024