A. L. Smirnov, On explicit units in Kummer's tower,
Zap. Nauchn. Sem. POMI, 2020, Volume 490, 109–123

https://www.mathnet.ru/eng/znsl6932

Записки научных
семинаров ПОМИ
Том 490, 2020 г.

А. Л. Смирнов

О ЯВНЫХ ЕДИНИЦАХ В КУММЕРОВОЙ БАШНЕ

§1. Введение

Важым арифметическим инвариантом числового поля K является группа единиц $\mathcal{O}_K^*$, где $\mathcal{O}_K$ – кольцо целых элементов K. Кручение этой группы обычно найти несложно, а ранг легко определяется с помощью теоремы Дирихле. Однако явное нахождение единиц считается трудным делом. Например, пусть $K = \mathbb{Q}(\alpha)$, где $\alpha^3 = a$ и a – рациональное число, из которого в $\mathbb{Q}$ не извлекается кубический корень. Тогда $\mathcal{O}_K^* \simeq \{\pm 1\} \times \mathbb{Z}$. Таким образом, в этом случае имеется ровно 4 элемента $\mathcal{O}_K$, переходящих в образующую группы $\mathcal{O}_K^*/\{\pm 1\}$ при факторизации. Поэтому для полного описания группы единиц достаточно предъявить один из них. В [1] приведена таблица таких элементов для небольших целых чисел a. В частности, для $a = 239$ соответствующий элемент выписан в виде $c_0 + c_1\alpha + c_2\alpha^2$, где c_0, c_1, c_2 – целые числа. Несмотря на относительно небольшое значения a, длина десятичной записи коэффициентов c_0, c_1 и c_2 поражает воображение. А именно, запись каждого из коэффициентов содержит 188 цифр.

Однако имеется относительно небольшой набор ситуаций, где единицы можно указать явно. Самый известный пример такого рода – круговые единицы (см. [2]). В этом случае имеется серия полей $K_n = \mathbb{Q}(\zeta_n)$, где $n = 1, 2, \ldots$, а ζ_n – примитивный корень степени n из 1. При $n > 1$ и d взаимно простом с n элемент

$$\frac{\zeta_n^d - 1}{\zeta_n - 1}.$$

является единицей кольца $\mathbb{Z}[\zeta_n]$. Более сложный пример связан с комплексным умножением для эллиптических кривых (см. [3]).

В работе [4] объяснена желательность изучения ζ-функций и L-рядов, связанных с башней Куммера

$$K_n = \mathbb{Q}(\sqrt[n]{a}),$$

Ключевые слова: куммерова башня, явные единицы, круговые единицы, эллиптические единицы.

Работа выполнена при поддержке РФФИ (грант 19-01-00513).)

где a – фиксированное рациональное число, а $n = 1, 2, \ldots$ В частности, для изучения поведения L-рядов при $s = 1$ полезно иметь информацию о единицах кольца $\mathcal{O}_n$, то есть кольца целых элементов поля K_n. В данной работе указано несколько серий единиц в кольцах $\mathcal{O}_n$ для $a = 2$ и $a = 3$.

§2. Построение единиц

Ниже a – целое число. При этом мы ограничиваемся случаем общего положения, то есть считаем, что $a \neq 0, \pm 1$ и a бесквадратно. В кольце $\mathcal{O}_n$ выделим подкольцо

$$A_n = \mathbb{Z}[\alpha_n], \text{ где } \alpha_n = \sqrt[n]{a}.$$

Если n ясно из контекста, то пишем α_n вместо α. Символ norm используется для обозначения нормы из K_n в $\mathbb{Q}$.

2.1. Серия 1 для $a = 2$. Положим

$$\eta_1 = 1 - \alpha.$$

Покажем, что $\eta_1 \in \mathcal{O}_n^*$ для всех $n \geqslant 1$. В самом деле, $\operatorname{norm}(\eta_1) = 1 - \alpha^n = -1$ (см. 4.1.3). Другое, более явное рассуждение, показывает, что $\eta_1 \in A_n^*$. А именно, $(1-\alpha)(1+\alpha+\cdots+\alpha^{n-1}) = 1-\alpha^n = -1$.

2.2. Серия 2 для $a = 2$. Для $n = 1, 2, \ldots$ положим

$$\eta_2 = 1 + \alpha + \alpha^3 + \alpha^5 + \cdots + \alpha^{n-2} = -\frac{1-\alpha+\alpha^2}{1-\alpha^2}.$$

Не при всех n элемент η_2 является единицей. Например, η_2^{-1} не является целым при $n = 2$. При $n = 3$ получаем единицу, но при $n = 9$ не получаем. Проверим, что если n взаимно простом с 6, то $\eta_2 \in \mathcal{O}_n^*$. В самом деле, положим $u = 1 - \alpha + \alpha^2$, $v = 1 - \alpha^2$. Тогда (см. 4.1.3) $\operatorname{norm} u = 1 - a + a^2 = 3$, $\operatorname{norm} v = 1 - a^2 = -3$. Предложение 4.1.4 показывает, что η_2 – единица.

Другое, более явное, рассуждение показывает, что при n взаимно простом с 6 элемент η_2 лежит в $\mathbb{Z}[\alpha]^*$, а не только в $\mathcal{O}_n^*$. А именно, положим

$$\theta = 1 + \alpha + \alpha^2 - \alpha^4 - \alpha^5 + \alpha^7 + \alpha^8 - \cdots + \alpha^{n-5} - \alpha^{n-3} - \alpha^{n-2}$$

для $n = 1 \pmod 6$, и

$$\theta = 1 - \alpha - \alpha^2 + \alpha^4 + \alpha^5 - \cdots - \alpha^{n-4} - \alpha^{n-3} + \alpha^{n-1}$$

для $n = -1 \pmod 6$. В обоих случаях суммирование геометрической прогрессии показывает, что $\eta_2\theta = -1$.

2.3. Серия 3 для $a = 2$**.** При нечетном n положим

$$\eta_3 = \begin{cases} 1 + \alpha - \alpha^{\frac{n+1}{2}}, & \text{для } n = \pm 1 \pmod 8; \\ 1 + \alpha + \alpha^{\frac{n+1}{2}}, & \text{для } n = \pm 3 \pmod 8). \end{cases}$$

Проверим, что $\eta_3 \in A_n^*$ для всех нечетных n. Для этого предъявим такой элемент $\theta \in A_n$, что $\eta_3\theta = 1$. Проверим это соотношения только для $n = 1 \pmod 8$. В остальных случаях проверка аналогична.

2.3.1. Для $n = 1 \pmod 8$ положим

$$\theta = \sum_{r=0}^{\frac{n-1}{2}} (-\alpha^2)^r - \alpha \sum_{r=0}^{\frac{n-5}{4}} (-\alpha^2)^r = \frac{1 + \alpha^{n+1}}{1 + \alpha^2} - \alpha \frac{1 - \alpha^{\frac{n-1}{2}}}{1 + \alpha^2} = \frac{1 - \alpha + \alpha^{\frac{n+1}{2}} + \alpha^{n+1}}{1 + \alpha^2}.$$

Пока мы работали в полиномах и не использовали специфику случая $a = 2$. Воспользовавшись равенством $\alpha^n = 2$, получим

$$\theta = \frac{1 + \alpha + \alpha^{\frac{n+1}{2}}}{1 + \alpha^2}.$$

Поэтому

$$\eta_3\theta = \frac{(1 + \alpha)^2 - \alpha^{n+1}}{1 + \alpha^2} = 1.$$

2.3.2. Для $n = 3 \pmod 8$ положим

$$\theta = \sum_{r=0}^{\frac{n-3}{4}} (-\alpha^2)^r - \alpha \sum_{r=0}^{\frac{n-3}{2}} (-\alpha^2)^r = \frac{1 - \alpha + \alpha^{\frac{n+1}{2}} - \alpha^n}{1 + \alpha^2}.$$

2.3.3. Для $n = 5 \pmod 8$ положим

$$\theta = \sum_{r=0}^{\frac{n-1}{2}} (-\alpha^2)^r - \alpha \sum_{r=0}^{\frac{n-5}{4}} (-\alpha^2)^r = \frac{1 - \alpha + \alpha^{\frac{n+1}{2}} + \alpha^{n+1}}{1 + \alpha^2}.$$

2.3.4. Для $n = 7 \pmod 8$ положим

$$\theta = \sum_{r=0}^{\frac{n-3}{4}} (-\alpha^2)^r - \alpha \sum_{r=0}^{\frac{n-3}{2}} (-\alpha^2)^r = \frac{1 - \alpha - \alpha^{\frac{n+1}{2}} - \alpha^n}{1 + \alpha^2}.$$

2.3.5. Существование третьей серии связано с несколькими фактами. Во-первых, для нечетного n имеется факторизация

$$(1+\alpha)^2 - \alpha^{n+1} = u_+ u_-,$$

где

$$u_+ = 1 + \alpha + \alpha^{\frac{n+1}{2}};$$
$$u_- = 1 + \alpha - \alpha^{\frac{n+1}{2}}.$$

Используя равенство $\alpha^n = 2$, получаем отсюда, что

$$u_+ u_- = (1+\alpha)^2 - 2\alpha = 1 + \alpha^2. \tag{1}$$

Второй факт, имеющий значение для существования серии, состоит в том, что в (1) получили круговой полином Φ_4 от α. Поэтому (см. 4.1.3) норма этого элемента не зависит от n. Более того, для данного конкретного полинома Φ_4 и данного конкретного $a = 2$ видим, что

$$\operatorname{norm}(u_+) \operatorname{norm}(u_-) = \Phi_4(2) = 5.$$

Третий факт, имеющий значение для существования серии, состоит в том, что получили простое число.

Таким образом, для всякого нечетного n один из этих двух элементов u_+ и u_- обратим, а норма второго равна 5. Утверждается, что единицей является

$$u = \begin{cases} u_-, & \text{если } n = \pm 1 \pmod 8; \\ u_+, & \text{если } n = \pm 3 \pmod 8). \end{cases}$$

Это вытекает из формул для обратного элемента θ, предъявленных в 2.3.1, 2.3.2, 2.3.3, 2.3.4.

2.4. Серия 4 для $a = 2$**.** При нечетном n положим

$$\eta_4 = \begin{cases} 1 + \alpha + \alpha^2 - \alpha^{\frac{n+1}{2}} - \alpha^{\frac{n+3}{2}} & \text{для } n = \pm 1, \pm 3, \pm 7 \pmod{24}; \\ 1 + \alpha + \alpha^2 + \alpha^{\frac{n+1}{2}} + \alpha^{\frac{n+3}{2}} & \text{для } n = \pm 5, \pm 9, \pm 11 \pmod{24}. \end{cases} \tag{2}$$

Утверждается, что $\eta_4 \in A_n^*$ для всех нечетных n. Для проверки предъявим такой элемент $\theta \in A_n$, что $\eta_4 \theta = 1$. Для построения θ удобно положить

$$\sigma = \sum_{i=0}^{m-1} (-1)^i \alpha^{6i} = \frac{1 - (-1)^m \alpha^{6m}}{1 + \alpha^6}, \tag{3}$$

где $m = (n-r)/12$, а $r = n \pmod{24}$ и $0 \leqslant r < 24$. Представление σ в виде суммы показывает, что $\sigma \in A_n$.

2.4.1. Для $n = 1 \pmod{24}$ положим

$$\theta = 1-\alpha(1+2\alpha+3\alpha^2+3\alpha^3+2\alpha^4+\alpha^5)\sigma-\alpha^{\frac{n+1}{2}}\left(\alpha(1+2\alpha+2\alpha^2+2\alpha^3+\alpha^4)\sigma\right).$$

Для $n = 3 \pmod{24}$ положим

$$\theta = 1+\alpha-(\alpha^3+\alpha^4+2\alpha^5+\alpha^6+\alpha^7)\sigma+\alpha^{\frac{n+1}{2}}\left(1-(\alpha^3+\alpha^4+\alpha^5+\alpha^6)\sigma\right).$$

Для $n = 5 \pmod{24}$ положим

$$\theta = -1+(\alpha+\alpha^3+\alpha^4+\alpha^6)\sigma-\alpha^{\frac{n+5}{2}}(1+\alpha^2)\sigma.$$

Для $n = 7 \pmod{24}$ положим

$$\theta = 1+(\alpha+\alpha^3-\alpha^4-\alpha^6)\sigma+\alpha^{\frac{n-5}{2}}+\alpha^{\frac{n-1}{2}}-\alpha^{\frac{n+3}{2}}\left(1-(\alpha^4+\alpha^6)\sigma\right).$$

Для $n = 9 \pmod{24}$ положим

$$\begin{aligned}\theta = &-1-\alpha+(\alpha^3+\alpha^4+2\alpha^5+\alpha^6+\alpha^7)\sigma \\ &+\alpha^{\frac{n+1}{2}}\left(1-(\alpha^3+\alpha^4+\alpha^5+\alpha^6)\sigma+\alpha^{\frac{n-3}{2}}\right).\end{aligned}$$

Для $n = 11 \pmod{24}$ положим

$$\begin{aligned}\theta = &-3-3\alpha-2\alpha^2-\alpha^3+(\alpha^4+2\alpha^5+4\alpha^6+3\alpha^7+2\alpha^8+\alpha^9)\sigma+\dots \\ &+2\alpha^{\frac{n-1}{2}}+\alpha^{\frac{n+1}{2}}(2+2\alpha+\alpha^2-\alpha^4)\sigma.\end{aligned}$$

Для $n = 13 \pmod{24}$ положим

$$\begin{aligned}\theta = 1+\big(&-(\alpha+2\alpha^2+3\alpha^3+3\alpha^4+2\alpha^5+\alpha^6) \\ &+\alpha^{\frac{n+3}{2}}(1+2\alpha+2\alpha^2+2\alpha^3+\alpha^4)\big)\sigma.\end{aligned}$$

Для $n = 15 \pmod{24}$ положим

$$\theta = 1+\alpha-\alpha^2(\alpha+\alpha^2+2\alpha^3+\alpha^4+\alpha^5)\sigma-\alpha^{\frac{n+1}{2}}\left(1-(\alpha^3+\alpha^4+\alpha^5+\alpha^6)\sigma\right).$$

Для $n = 17 \pmod{24}$ положим

$$\theta = -1+(\alpha+\alpha^3+\alpha^4+\alpha^6)\sigma-\alpha^{\frac{n-3}{2}}+\alpha^{\frac{n+1}{2}}\left((\alpha^2+\alpha^4)\sigma\right).$$

Для $n = 19 \pmod{24}$ положим

$$\theta = 1+\alpha+\alpha^3-\alpha^4(\alpha+\alpha^2+\alpha^3+\alpha^5)\sigma-\alpha^{\frac{n+1}{2}}\alpha^3\left((\alpha^2+\alpha^4)\sigma\right).$$

Для $n = 21 \pmod{24}$ положим

$$\begin{aligned}\theta = &-1-\alpha+\alpha^2(\alpha+\alpha^2+2\alpha^3+\alpha^4+\alpha^5)\sigma-\alpha^{\frac{n-3}{2}}-\alpha^{\frac{n-1}{2}}\\ &-\alpha^{\frac{n+1}{2}}\left(1-\alpha^2(\alpha+\alpha^2+\alpha^3+\alpha^4)\sigma-\alpha^{\frac{n-3}{2}}\right).\end{aligned}$$

Для $n = 23 \pmod{24}$ положим

$$\begin{aligned}\theta = &-3-3\alpha-2\alpha^2-\alpha^3+\alpha^4(1+2\alpha+3\alpha^2+3\alpha^3+2\alpha^4+\alpha^5)-\alpha^{\frac{n-3}{2}}-2\alpha^{\frac{n-1}{2}}\\ &+\alpha^{\frac{n+1}{2}}\left(-2-2\alpha-\alpha^2+\alpha^4(1+2\alpha+2\alpha^2+2\alpha^3+2\alpha^4+\alpha^5)\sigma-\alpha^{\frac{n-3}{2}}\right).\end{aligned}$$

2.4.2. Проверим соотношение $\eta_4\theta = 1$ для $n = 1 \pmod{24}$. В остальных случаях проверка аналогична. Воспользовавшись (3), видим, что

$$\sigma = \frac{1-\alpha^{(n-1)/2}}{1+\alpha^6}$$

и

$$\theta = \frac{1+\alpha+2\alpha^2+\alpha^3+\alpha^4+\alpha^{(n+1)/2}\left(1+\alpha+\alpha^2+\alpha^3\right)}{1+\alpha^6}.$$

Поэтому

$$\theta\eta_4 = \frac{1+2\alpha+4\alpha^2+4\alpha^3+4\alpha^4+2\alpha^5+\alpha^6-\alpha^{n+1}\left(1+2\alpha+2\alpha^2+2\alpha^3+\alpha^4\right)}{1+\alpha^6}.$$

Воспользовавшись равенством $\alpha^n = 2$, получим $\theta\eta_4 = 1$.

2.4.3. Существование четвертой серии связано с несколькими обстоятельствами. Во-первых, для нечетного $n \geqslant 5$ имеется факторизация

$$u_+u_- = \Phi_6(\alpha^2), \tag{4}$$

где

$$\begin{aligned}u_+ &= 1+\alpha+\alpha^2+\alpha^{\frac{n+1}{2}}+\alpha^{\frac{n+3}{2}};\\ u_- &= 1+\alpha+\alpha^2-\alpha^{\frac{n+1}{2}}-\alpha^{\frac{n+3}{2}}.\end{aligned}$$

Действительно, $u_+u_- = (1+\alpha+\alpha^2)^2-\alpha^{n+1}(1+\alpha)^2$. Заменяя α^n на 2, получим (4).

Заметим (см. 4.1.3), что

$$\operatorname{norm}(\Phi_6(\alpha^2)) = \begin{cases}13, & \text{если } n \neq 0 \pmod{3};\\ 25, & \text{если } n = 0 \pmod{3}.\end{cases} \tag{5}$$

Из (4) и (5) получаем, что

$$\operatorname{norm}(u_+)\operatorname{norm}(u_-) = \begin{cases} 13, & \text{если } n \neq 0 \pmod 3; \\ 25, & \text{если } n = 0 \pmod 3. \end{cases}$$

Так как 13 простое, а $\operatorname{norm}(u_+)$ и $\operatorname{norm}(u_-)$ целые, то одна из этих норм равна ± 1, а другая ± 13. Выбор между u_+ и u_- зависит от n и содержится в формуле (2).

Для $n = 0 \pmod 3$ a priori возможна ситуация, когда

$$\operatorname{norm}(u_+) = \pm 5 \text{ и } \operatorname{norm}(u_-) = \pm 5.$$

В этом случае ни u_+, ни u_+ не являются обратимыми. Однако вышеприведенные формулы для обратного элемента показывают, что эта ситуация не реализуется.

2.5. Серия 5 для $a = 2$. Пусть $n \geqslant 7$ взаимно просто и с 2, и с 5. Для описания серии удобно ввести

$$\sigma = \sum_{i=0}^{m-1} (-1)^i \alpha^{2i} = \frac{1 - (-1)^m \alpha^{2m}}{1 + \alpha^2}, \tag{6}$$

где

$$m = \begin{cases} (n-r)/4, & \text{если } n = \pm 1 \pmod 8; \\ (n-r)/4 - 1, & \text{если } n = 3 \pmod 8; \\ (n-r)/4 + 1, & \text{если } n = 5 \pmod 8; \end{cases}$$

а $r = n \pmod 8$ и $0 \leqslant r < 8$. Представление σ в виде суммы показывает, что $\sigma \in A_n$. Положим

$$\eta_5 = \begin{cases} -1 + \alpha + \alpha^4\sigma - \alpha^{(n+1)/2}\sigma, & \text{если } n = 1 \pmod 8; \\ -1 + \alpha + \alpha^4\sigma + \alpha^{(n+7)/2}\sigma, & \text{если } n = 3 \pmod 8; \\ -1 + \alpha + \alpha^4\sigma + \alpha^{(n+1)/2}\sigma, & \text{если } n = 5 \pmod 8; \\ -1 + \alpha + \alpha^4\sigma - \alpha^{(n+7)/2}\sigma, & \text{если } n = 7 \pmod 8. \end{cases}$$

Утверждается, что $\eta_5 \in A_n^*$ для всех n взаимно простых как с 2, так и с 5. Для доказательства можно было бы предъявить такой элемент $\theta \in A_n$, что $\eta_5\theta = 1$. Однако вид θ зависит от $n \pmod{40}$ и явные формулы займут слишком много места.

2.6. Независимость серий. Вопрос о независимости построенных серий единиц остается невыясненным. Отметим только, что при $n < 11$ они не могут быть независимы по теореме Дирихле о ранге группы единиц. Пусть Θ – группа единиц, порожденная $\eta_1, \eta_2, \eta_3, \eta_4, \eta_5$. Вычисление показывает, что единицы $\operatorname{rk}\Theta = 5$ при $n = 11$. Можно предположить, что $\operatorname{rk}\Theta = 5$ при всех $n \geqslant 11$.

Положим
$$\widetilde{\Theta} = (\Theta \otimes \mathbb{Q}) \cap (\mathcal{O}_n^*/T),$$
где T – кручение, а пересечение рассматривается в группе $\mathcal{O}_n^* \otimes \mathbb{Q}$. Весьма интересный вопрос об индексе Θ в группе $\widetilde{\Theta}$ также остается невыясненным.

§3. Конструктивные единицы для $a = 3$

3.1. Серия 1 для $a = 3$. Для нечетного n положим
$$\eta_1 = \frac{1 + \alpha + \alpha^2 - \alpha^{n+1}}{1 + \alpha}. \tag{7}$$
Так как, $1 + x + x^2 - x^{n+1} = 0$ при $x = 1$, то числитель η_1 делится на знаменатель и, следовательно, $\eta_1 \in A_n$. Проверим, что для $\eta_1 \in A_n^*$. Положим
$$\theta = \sum_{i=0}^{n-1} (m - i)\alpha^i, \text{ где } m = \frac{3n-1}{2}.$$

Несложно проверить, что $\eta_1\theta = 1$.

3.1.1. Существование первой серии для $a = 3$ связано с соотношением
$$\Phi_1(a)^2 = \Phi_2(a). \tag{8}$$
Действительно, подставив $\alpha^n = 3$ в (7), увидим, что
$$\eta_1 = \frac{(1-\alpha)^2}{1+\alpha} = \frac{\Phi_1(\alpha)^2}{\Phi_2(\alpha)}.$$
Поэтому из соотношения (8) вытекает (см. 4.1.3), что $\operatorname{norm}\eta_1 = 1$.

3.2. Серия 2 для $a = 3$. Для n взаимно простого с 12 положим
$$\eta_2 = \begin{cases} 1 + \alpha - \alpha^{(n+1)/2} & \text{если } n = \pm 1 \pmod{12}; \\ 1 + \alpha + \alpha^{(n+1)/2} & \text{если } n = \pm 5 \pmod{12}. \end{cases} \tag{9}$$

Покажем, что $\eta_2 \in A_n^*$. Для проверки предъявим такой элемент $\theta \in A_n$, что $\eta_2\theta = 1$.

3.2.1. Для построения θ удобно взять

$$\sigma(s) = \sum_{i=0}^{s-1} (-1)^i \alpha^{3i} = \frac{1-(-1)^s\alpha^{3s}}{1+\alpha^3}. \tag{10}$$

Представление σ в виде суммы показывает, что $\sigma(s) \in A_n$. Положим

$$\theta = \begin{cases} 1-(1+\alpha)^2\sigma(\frac{n-1}{6}) - \alpha^{\frac{n+3}{2}}(1+\alpha^2)\sigma(\frac{n-1}{6}), & \text{если } n = 1 \pmod{12}; \\ -2-\alpha+(1+\alpha)^2\sigma(\frac{n-5}{6}) + \alpha^{\frac{n-1}{2}}(1+\alpha^2)\sigma(\frac{n+1}{6}), & \text{если } n = 5 \pmod{12}; \\ 1-(1+\alpha)^2\sigma(\frac{n-1}{6}) + \alpha^{\frac{n+3}{2}}(1+\alpha^2)\sigma(\frac{n-1}{6}), & \text{если } n = 7 \pmod{12}; \\ -2-\alpha+(1+\alpha)^2\sigma(\frac{n-5}{6}) - \alpha^{\frac{n-1}{2}}(1+\alpha^2)\sigma(\frac{n+1}{6}), & \text{если } n = 11 \pmod{12}. \end{cases}$$

Несложно проверить, что $\eta_2\theta = 1$.

3.2.2. Существование второй серии для $a = 3$ связано с тем фактом, что

$$\Phi_6(a) \text{ – простое число}$$

и с существованием факторизации

$$\Phi_6(\alpha) = u_+u_-, \text{ где } u_+ = 1+\alpha+\alpha^{\frac{n+1}{2}}, u_- = 1+\alpha-\alpha^{\frac{n+1}{2}},$$

Для n взаимно простого с 6 отсюда вытекает (см. 4.1.3), что

$$\operatorname{norm}(u_+)\operatorname{norm}(u_-) \text{ – простое число.}$$

Поэтому один из элементов u_+ и u_- лежит в $\mathcal{O}_n^*$. Какой именно из элементов u_+ и u_- обратим, указано в (9).

3.3. Независимость серий. Вопрос о независимости построенных серий единиц пока отложим. Отметим только, что при $n < 4$ они не могут быть независимы по теореме Дирихле. Пусть Θ – группа единиц, порожденная η_1, η_2. При $n = 4$ единицы η_1 и η_2 не определены. Вычисление показывает, что $\operatorname{rk}\Theta = 2$ при $n = 5$.

Весьма интересный вопрос об индексе Θ в группе $(\Theta \otimes \mathbb{Q}) \cap \mathcal{O}_n^*/T$, где T – кручение, не изучен.

§4. Некоторые наблюдения

Как понятие серии, так и причины существования таких серий не вполне ясны. Ниже предпринимается попытка пролить свет на эти сущности.

4.1. Происхождение серий. Первая серия для $a = 2$ бросается в глаза. Другие серии обнаружены с помощью компьютера. А именно, были вычислены фундаментальные единицы для небольших n, причем в ответах для разных n было замечено некоторое сходство. Анализ этого сходства и выявил серии.

Между круговыми полиномами нет нетривиальных мультипликативных соотношений. Однако между их значениями такие соотношения могут быть. Похоже, что это явление может рассматриваться как причина существования серий. Круговой полином, связанный с примитивными корнями степени d, обозначаем Φ_d. Таким образом, $\Phi_1 = x$, $\Phi_2 = x + 1$, $\Phi_3 = x^2 + x + 1$ и т.д.

Покажем сначала, как можно вычислять нормы в куммеровой башне для элементов специального вида. Пусть E – некоторое поле, $a \in E$. Для $n = 1, 2, \dots$ положим

$$E_n = E[x]/(x^n - a), \quad \alpha \text{ – образ } x \text{ в } E_n.$$

Элемент $m \in E_n$ назовем мономом, если этот элемент E-пропорционален хотя бы одной из степеней α и $m \neq 0$. Весом монома m назовем элемент $d(m) \in \mathbb{Z}/n\mathbb{Z}$, определенный формулой

$$d(m) = d \pmod n,$$

где m пропорционален α^d.

4.1.1. Лемма. *Пусть σ_1, σ_2 перестановки множества $\mathbb{Z}/n\mathbb{Z}$, заданные формулами*

$$\sigma_1(i) = i + d_1, \sigma_2(i) = i + d_2,$$

где разность $d_1 - d_2$ обратима в $\mathbb{Z}/n\mathbb{Z}$. Пусть ρ перестановка множества $\mathbb{Z}/n\mathbb{Z}$, причем для всякого i либо $\rho(i) = \sigma_1(i)$, либо $\rho(i) = \sigma_2(i)$. Тогда

$$\rho = \sigma_1 \text{ *или* } \rho = \sigma_2.$$

Доказательство. Рассмотрим диаграмму

$$\begin{tikzcd}
0 \arrow[dr, "\sigma_1"'] & & d \arrow[dl, "\sigma_2"] \arrow[dr, "\sigma_1"'] & & 2d \arrow[dl, "\sigma_2"] \arrow[dr, "\sigma_1"'] & \\
& d_1 & & d + d_1 & & \dots
\end{tikzcd},$$

где $d = d_1 - d_2$. Ввиду равноправности σ_1 и σ_2 можно считать, что $\rho(0) = \sigma_1(0)$. Но тогда $\rho(d) \neq d_1 = \sigma_2(d)$. Поэтому $\rho(d) = \sigma_1(d)$. Продолжая этот процесс, увидим, что $\rho(j) = \sigma_1(j)$ для каждого элемента j

из верхней строки. Так как d обратимо, то в верхней строке до повторения 0 встретятся все элементы по одному разу. $\square$

Для $u \in E_n$ по определению

$$\operatorname{norm}(u) = \det(u) \in E,$$

где имеется в виду детерминант E-линейного оператора $E_n \to E_n$, заданного умножением на u и обозначаемого тем же символом. Например, несложно увидеть, что

$$\operatorname{norm}(\alpha) = a. \tag{11}$$

4.1.2. Предложение. *Если m_1, m_2 мономы в E_n и разность $d(m_1) - d(m_2)$ обратима в $\mathbb{Z}/n\mathbb{Z}$, то*

$$\det(m_1 + m_2) = \det(m_1) + \det(m_2).$$

Доказательство. Воспользуемся стандартной формулой:

$$\det(m_1 + m_2) = \sum_\rho \pi(\rho), \text{ где } \pi(\rho) = (-1)^{\operatorname{sign}\rho} \prod_i m_{i,\rho(i)}, \tag{12}$$

где $m_{i,j}$ – матричный элемент оператора умножения на $m = m_1 + m_2$. Если $m_{i,j} \neq 0$, то $m_{i,j} = (m_1)_{i,j}$ или $m_{i,j} = (m_2)_{i,j}$. Это вытекает из мономиальности m_1, m_2 и обратимости $d_1 - d_2$. Пусть σ_1 – перестановка $i \mapsto i + d_1$, а σ_2 – перестановка $i \mapsto i + d_2$. Таким образом, в сумме из (12) $\pi(\rho) \neq 0$ только для тех ρ, для которых выполнено условие леммы 4.1.1. По заключению этой леммы ρ совпадает либо с σ_1, либо с σ_2. Поэтому $\det(m_1 + m_2) = \pi(\sigma_1) + \pi(\sigma_1) = \det(m_1) + \det(m_2)$. $\square$

Для построения серий единиц полезны серии целых элементов с ограниченной нормой. Такие серии легко строить с помощью следующего утверждения, показывающего, что любой круговой полином Φ_m и натуральное r дают серию конструктивных элементов $\Phi_m(\alpha^r)$ с ограниченной нормой.

4.1.3. Предложение. *Пусть $a \in \mathbb{Q}$ и из a в поле $\mathbb{Q}$ не извлекается никакой корень степени больше единицы, $n, m, r \in \{1, 2, \dots\}$. Тогда*

(1) $\operatorname{norm}(\alpha^r) = a^r$;
(2) *если r взаимно просто с n, то* $\operatorname{norm}(\alpha^r - 1) = a^r - 1$;
(3) *если m взаимно просто с n, то* $\operatorname{norm} \Phi_m(\alpha) = \Phi_m(\operatorname{norm}(\alpha))$;
(4) *в общем случае* $\operatorname{norm}(\alpha^r - 1) = (a^{r/d} - 1)^d$, *где* $d = \gcd(r, n)$;

(5) *в общем случае*

$$\operatorname{norm}\Phi_m(\alpha^r) = \prod_{e|m}(a^{re/d} - 1)^{d\mu(m/e)},$$

где $d = \gcd(n, re)$.

Доказательство. Первое утверждение очевидно. Второе утверждение немедленно вытекает из 4.1.2. Третье утверждение вытекает из второго, так как

$$\Phi_m = \prod_{e|m}(x^e - 1)^{\mu(n/e)},$$

где μ – функция Мебиуса.

Для проверки четвертого утверждения заметим, что $K \supset K_m$, где $m = n/d$, так как $\alpha_m = \alpha^d$. Поэтому

$$\operatorname{norm}(\alpha^r - 1) = \operatorname{norm}_m \operatorname{norm}_{K/K_m}(\alpha_m^s - 1) = \operatorname{norm}_{K/K_m}(\alpha_m^s - 1)^d = (a^s - 1)^d,$$

где $s = r/d$. Последнее равенство вытекает из второго пункта, так как m взаимно просто с s.

Пятое утверждение вытекает из формулы

$$\Phi_m(\alpha^r) = \prod_{e|m}\Phi_1(\alpha^{er})^{\mu(m/e)}$$

с учетом уже проверенного в четвертом пункте случая $m = 1$. □

Предложение 4.1.2 позволяет считать нормы и других элементов, а не только указанных в 4.1.3. Но, видимо, это обстоятельство не слишком полезно для образования серий. Например, если $f(x) = (x - \lambda_1)\cdots(x - \lambda_k) \in E[x]$, то $\operatorname{norm} f(\alpha) = (a - \lambda_1^n)\cdots(a - \lambda_k^n)$. Чтобы ограничить эти нормы равномерно по n, корни f должны быть расположены внутри единичного круга. Однако это требование наряду с условием целости корней приводит к тому, что нули f – корни из единицы.

Следующее утверждение окажется полезным при образовании серий.

4.1.4. Предложение. *Предположим, что* $u, v \in \mathcal{O}_n$, *причем* $\operatorname{norm}(u) = \operatorname{norm}(v) = p^r$, *где* p *– простое число, не делящее* a. *Предположим также, что* n *взаимно просто с* p *и* $(p-1)$. *Если, кроме того,*

$$r < d(p, q) \tag{13}$$

для всякого простого q, делящего n, то $u/v \in \mathcal{O}_n^*$. Здесь $d(p,q)$ – порядок $p \pmod q$ в группе $(\mathbb{Z}/q\mathbb{Z})^*$.

Доказательство. Так как p взаимно просто с a и с n, то $\mathcal{O}_n$ неразветвлено над p и разложение идеала (p) в кольце $\mathcal{O}_n$ имеет вид $(p) = P_1 \cdots P_m$, где все простые идеалы P_i различны. Утверждается, что

$$\text{существует, причем единственный, индекс } i, \text{ для которого} \quad \operatorname{norm}(P_i) \leqslant p^r. \tag{14}$$

В самом деле, так как n взаимно просто с p, то полином $x^n - \bar{a}$, где $\bar{a} = a \pmod p$, сепарабелен над $\mathbb{F}_p$. Поэтому набор проекций индуцирует изоморфизм колец

$$\mathbb{F}_p[x]/(x^n - \bar{a}) \to F_1 \times \cdots \times F_m,$$

где F_i – поле вычетов кольца $\mathcal{O}_n$ в простом идеале P_i. Покажем, что

$$[F_i : \mathbb{F}_p] > r \quad \text{для всех } i \in \{1, \ldots, m\} \text{ кроме одного.} \tag{15}$$

Так как n взаимно просто с $p-1$, то в $\mathbb{F}_p$ имеется единственное решение уравнения $x^n = \bar{a}$. Обозначим это решение x_0 и положим $t = x/x_0$. Эта замена устанавливает изоморфизм

$$\mathbb{F}_p[x]/(x^n - \bar{a}) \simeq \mathbb{F}_p[t]/(t^n - 1).$$

и биекцию между множеством $\{P_i\}$ и множеством $\mathcal{P}$, состоящим из всех неприводимых $\mathbb{F}_p$-полиномов, делящих $t^n - 1$ и имеющих старший коэффициент 1. При этом $[F_i : \mathbb{F}_p]$ равна степени соответствующего полинома. Среди элементов $\mathcal{P}$ имеется один, а именно $t-1$, степени 1. Покажем, что степень любого другого $P \in \mathcal{P}$ больше r. Так как

$$t^n - 1 = \prod_{d|n} \Phi_d(t),$$

то P делитель $\Phi_d(t)$, где $d > 1$. Пусть ζ – образ t в $\mathbb{F}_p[t]/(P)$ и e – наименьшее положительное число, для которого $\zeta^e = 1$. Тогда $e = d$, так как Φ_d и Φ_e взаимно просты над $\mathbb{F}_p$ для разных d и e, взаимно простых с p. Поэтому $p^{\deg P} = 1 \pmod d$ и, таким образом, (15) доказано. Из (15) тотчас вытекает (14).

Единственный из идеалов P_i, имеющий степень 1, обозначим $\widetilde{p}$. Из неравенства (13) вытекает, что нормы всех P_i кроме $\widetilde{p}$ имеют p-порядок, больший r. Так как $u \in \mathcal{O}_n$ и $\operatorname{norm}(u) = (p)$, то $(u) = \widetilde{p}^r$. Аналогично для (v). Таким образом, u/v имеет тривиальное разложение на дробные идеалы и поэтому $u/v \in \mathcal{O}_n^*$. □

4.1.5. Существование части серий можно объяснить наличием спорадических соотношений между значениями круговых полиномов вместе со следствием 4.1.3. Это объясняет серию 1 для $a = 2$, так как $\Phi_1(2) = 1$.

Существование второй серии для $a = 2$ связано с тем фактом, что в этом случае

$$\Phi_1(a^2) = \Phi_6(a).$$

Существование первой серии для $a = 3$ связано с тем фактом, что в этом случае

$$\Phi_1(a)^2 = \Phi_2(a).$$

Существование третьей и четвертой серий для $a = 2$ пояснено в 2.3.5 и 2.4.3. Таким образом, объяснены пять серий из семи найденных. Причины существования остальных серий остаются неясными.

Более концептуальный подход к построению конструктивных единиц в куммеровой башне состоит в использовании того обстоятельства, что поле $\mathbb{Q}(\zeta_n, \alpha_n)$ является абелевым расширением кругового поля $\mathbb{Q}(\zeta_n)$. Круговое поле является полем CM-типа (см. [5]) и вполне вероятно, что $\mathbb{Q}(\zeta_n, \alpha_n)$ содержится в поле, связанном с соответствующим абелевым многообразием. По аналогии с эллиптическими единицами должна существовать теория единиц в таких полях. Их нормы со значениями в K_n могут дать интересное описание единиц в куммеровой башне для произвольного a.

4.2. О понятии серии. При построении серии мы не определили это понятие, а пользовались чисто интуитивным его восприятием. Воможно, что определение понятия серии может быть связано с концепцией эйлеровых систем (см. [2]).

Список литературы

1. H. Wada, *A Table of Fundamental Units of Purely Cubic Fields.* — Proc. Japan Acad. **46**, No. 10 (1970), 1135–1140.
2. J. Coates, R. Sujatha, *Cyclotomic Fields and Zeta Values*, Monographs in Mathematics, Springer (2006).
3. G. Robert, *Unités elliptiques et formules pour le nombre de classes des extensions abéliennnes d'un corps quadratic imaginaire*, Bull. Soc. Math., France, 1973, **36**, 5–77.
4. А. Л. Смирнов, *Куммерова башня и большие дзета-функции.* — Зап. научн. сем. ПОМИ **469** (2018), 151–159.
5. G. Shimura, Yu. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Math. Soc. of Japan, 1961.

Smirnov A. L. On explicit units in Kummer's tower.

We consider Kummer's tower, i. e. a family of number fields obtained by means of extracting all possible radicals from a rational base. We construct a few series of units in the tower where the base is equal to two and three.

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
набережная реки Фонтанки 27,
191023, Санкт-Петербург, Россия
E-mail: smirnov@pdmi.ras.ru

Поступило 21 августа 2020 г.