УДК 511:681.3.14

К ОПРЕДЕЛЕНИЮ СИСТЕМЫ ОСНОВНЫХ ЕДИНИЦ

АВАНЕСОВ Э.Т., ГУСЕВ В.А., кандидаты физ.- мат. наук

Приводится сравнительный анализ различных методов решения задачи определения системы основных единиц и алгоритм их поиска.

Предметом исследования является сравнительный анализ в определенном историческом контексте различных методов определения системы основных единиц для простейшего, но очень важного и интересного специального класса кубических полей отрицательного дискриминанта. А именно, для чисто кубических полей $K\left(\sqrt[3]{m}\right)$, где $m>0$ и не равно полному кубу.

Теория единиц явилась важнейшим шагом на пути построения арифметики алгебраических чисел. В случае кубических полей она впервые была рассмотрена Ф.Эйзенштейном (1823-1852), для полей деления круга – Л.Кронекером (1823-1891). В общем случае близко подошел к построению теории Ш.Эрмит (1822-1901), но лишь Густав Петер Лежен-Дирихле (1805-1859) завершил конструкцию единиц произвольного алгебраического числового поля [5].

Известно, что структура множества всех единиц описывается следующим утверждением.

Теорема 1 (Дирихле). В произвольном кольце $O(\lambda)$ поля алгебраических чисел $K(\lambda)$ порядка $n=n_1+2n_2$, где $\lambda-$ корень уравнения

$$\lambda^n+a_1\lambda^{n-1}+\ldots+a_n=0,\ a_i\in Z; \qquad (1)$$

n_1 – число действительных корней уравнения (1),

n_2 – число пар комплексных корней,

существуют такие единицы $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_r$ $(r=n_1+n_2-1)$, что каждая единица $\varepsilon\in O(\lambda)$ однозначно представляется в виде

$$\varepsilon=\pm\sigma\varepsilon_1^{\alpha_1}\varepsilon_2^{\alpha_2}\ldots\varepsilon_r^{\alpha_r},\ ,\ \alpha_i\in Z$$

где $\sigma-$ особые единицы, то есть корни из обычной единицы, содержащиеся в $O(\lambda)$; единицы ε_i – основные единицы.

Очевидно, теорема Дирихле допускает и теоретико-групповую интерпретацию: группа единиц кольца $O(\lambda)$ является прямым произведением циклической группы конечного порядка корней из 1 и свободной абелевой группы ранга $r=n_1+n_2-1$.

Наряду с основными единицами принято рассматривать и независимые единицы.

Определение 1. Система единиц $\{\eta_i\}$, $i=1,2,\ldots,t;\ t\le r$, называется независимой, если равенство $\prod_{i=1}^{t}\eta_i^{\beta_i}=1$ имеет место лишь при $\beta_i=0\ (i=1,2,\ldots,t)$.

Для r независимых единиц η_i составим матрицу

$$\begin{pmatrix} \ln\left|\eta_1^{(1)}\right| & \ln\left|\eta_2^{(1)}\right| & \ldots & \ln\left|\eta_r^{(1)}\right| \\ \ln\left|\eta_1^{(2)}\right| & \ln\left|\eta_2^{(2)}\right| & \ldots & \ln\left|\eta_r^{(2)}\right| \\ \cdot & \cdot & \cdot & \cdot \\ \ln\left|\eta_1^{(r+1)}\right| & \ln\left|\eta_2^{(r+1)}\right| & \ldots & \ln\left|\eta_r^{(r+1)}\right| \end{pmatrix},$$

где индекс j в выражении $\ln\left|\eta_i^{(j)}\right|$ означает сопряжение относительно корней (1).

Все миноры порядка r этой матрицы равны по абсолютному значению, и их называют регулятором R_η, построенным на независимых единицах. Все системы основных единиц имеют один и тот же регулятор R.

Определение 2. Единицы $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_r$ образуют основную систему, если 1)они независимы и 2) их регулятор минимальный.

Разыскание системы основных единиц произвольного алгебраического числового поля есть одна из важных задач. Сами основные единицы используются при вычислении числа классов идеалов и решении многих частных типов и классов диофантовых уравнений.

Отметим, что построение основной системы единиц осуществляется либо непосредственно, на основе некоторых теорем, способов и конструкций, либо путем преобразования независимой системы.

Известные приемы и методы решения задач построения независимых и основных систем основаны на самых разнообразных

идеях, достаточно полные, но краткие обзоры их представлены в депонированной рукописи [1], у В.Нарковича [7] и Х.Циммера [8]. В настоящее время возрастает интерес к задаче разыскания основных единиц. Созданы новые приемы, процедуры и методы, позволяющие проводить численные расчеты единиц, сравнение известных путей и способов.

Ниже исследуются чисто кубические поля. По теореме Дирихле в таких полях существует одна основная единица ε, называемая прямой в случае $|\varepsilon|>1$ и обратной при $|\varepsilon|<1$.

Таблицы основных единиц приводились К.Ф. Гауссом (1808), А.А. Марковым (1891), Р. Дедекиндом (1900), К. Вольфе (1923), Дж. Касселом (1950), Э. Зельмаром (1955), Х. Вадом (1970), Р. Гютингом (1976) и К. Накамулем (1988). Указанные таблицы частично воспроизведены в [1, 2, 3]; наиболее полное их сопоставление осуществлено в [1].

Рассмотрим процедуру извлечения корня из некоторой степени основной единицы чисто кубического поля $K\left(\sqrt[3]{m}\right)$.

Пусть $m=ab^2$, где $(a,b)=1$, целые $a,b>0$ и свободны от квадратов.

Как известно, чисто кубическое поле $K\left(\sqrt[3]{m}\right)$ относится к *первому типу*, если $\left(a^2 \bmod 9\right)\neq\left(b^2 \bmod 9\right)$ и ко *второму типу* при $a^2\equiv b^2 \pmod 9$. Дедекиндом было доказано, что если поле $K\left(\sqrt[3]{m}\right)$ первого типа, то числа 1, $w=\sqrt[3]{m}$, $\overline{w}=\sqrt[3]{\overline{m}}=\sqrt[3]{a^2b}$ образуют целый базис, а в случае, когда поле $K\left(\sqrt[3]{m}\right)$ второго типа, то целый базис составляет тройка: 1, $w=\sqrt[3]{m}$, $\overline{w}=\frac{1}{3}\left|1+q_1\sqrt[3]{m}+q_2\sqrt[3]{\overline{m}}\right|$, где $q_1,q_2=\pm1$ независимо друг от друга и $q_1\equiv b \pmod 3$, $q_2\equiv a \pmod 3$.

Очевидно, если $\varepsilon=x+y\sqrt[3]{m}+z\sqrt[3]{m^2}$ есть единица чисто кубического поля $K\left(\sqrt[3]{m}\right)$, то (x,y,z) есть решение диофантова уравнения $x^3+my^3+m^2z^3-3mxyz=1$. (2)

Пусть (x_0,y_0,z_0) - целое решение уравнения (2) и $\rho^3=1$, $\rho\neq1$; полагая $x_n+\rho y_n\sqrt[3]{m}+\rho^2z_n\sqrt[3]{m^2}=\left(x_0+\rho y_0\sqrt[3]{m}+\rho^2z_0\sqrt[3]{m^2}\right)^n$, находим, следуя [91], рекуррентные формулы

$$\begin{cases} x_{n+1}=x_0x_n+mz_0y_n+my_0z_n,\\ y_{n+1}=y_0x_n+x_0y_n+mz_0z_n,\\ z_{n+1}=z_0x_n+y_0y_n+x_0z_n. \end{cases}$$

Заметим, что в чисто кубическом поле $K\left(\sqrt[3]{m}\right)$, где $m=\frac{1}{2}i(i+1)(2i+1)$, целое i – нечетно, основная единица есть $\varepsilon=-1+6(2i+1)\sqrt[3]{m}-12\sqrt[3]{m^2}$ [4]. Тогда минимальный многочлен для ε имеет вид $\varepsilon^3-3\varepsilon^2+3s\varepsilon-1$, где $s=1+216\sum_{j=1}^{i}j^2$. И если $x_0=1$, $x_1=x_2=0$, $x_{n+1}=z_n$, $y_{n+1}=x_n-3sz_n$, $z_{n+1}=y_n+3z_n$,

$\varepsilon^n=x_n+y_n\varepsilon+z_n\varepsilon^2=$

$=x_n+\left(x_{n-1}-3sx_1\right)\varepsilon+x_{n+1}\varepsilon^2$; $n=1,2,3,\ldots$, то $x_{n+3}=x_n-3sx_{n+1}+3x_{n+2}$ и

$$x_{n+3}=\sum_{t=0}\sum_{j=0}\left\{3^{n-2t+j}\binom{n-2t}{t-j}\binom{n-3t+j}{2j}s^{2j}-3^{n-3t-1+j}\binom{n-2t-1}{t-j}\binom{n-3t-1+j}{1+2j}s^{1+2j}\right\}.$$

Это дает возможность вычислять явно все последовательные степени ε.

Известные алгоритмы определения основной единицы чисто кубического поля $K\left(\sqrt[3]{m}\right)$ не дают абсолютной уверенности в том, что получаемые единицы будут основными. Это побуждает к поиску тестов, позволяющих находить основную единицу, если известна нетривиальная единица. Ниже рассматривается задача извлечения корня из чисто кубического числа с нормой +1, приводящего к искомой основной единице. Для ее решения известны два способа.

Способ 1 [3].

Пусть кубическое число $\varepsilon\in K\left(\sqrt[3]{m}\right)$ имеет норму +1 и является корнем уравнения

$$\varepsilon^3=p_1\varepsilon^2+p_2\varepsilon+1 \qquad (3)$$

и пусть $\varepsilon=\varepsilon_0^N$, где ε_0 - также кубическое число, определяемое уравнением

$$\varepsilon_0^3=p_1'\varepsilon_0^2+p_2'\varepsilon_0+1. \qquad (4)$$

Очевидно, основные симметрические функции p_1,p_2 от корней уравнения (3) будут симметрическими функциями от корней уравнения (4), а значит, они рационально выражаются через основные симметрические функции p_1' и p_2'.

Задача извлечения корня N-й степени из ε сводится к разысканию p_1' и p_2' по данным p_1, p_2 и N. Таким образом, будем иметь систему двух уравнений с двумя неизвестными, и достаточно взять простые множители канонического разложения.

Пусть, например, N=2. Тогда

$$\begin{cases} p_1 = p_1'^2 + 2p_2', \\ p_2 = 2p_1' - p_2'^2. \end{cases} \quad (5)$$

Исключая p_2', получаем

$\left(p_1'^2 - p_1\right)^2 - 8p_1' + 4p_2 = 0$. Рациональный корень этого уравнения, если он существует, принимаем за p_1', затем находим p_2'.

При извлечении кубического корня аналогично системе (5) получим систему уравнений

$$\begin{cases} p_1 = p_1'^3 + 3p_1'p_2' + 3, \\ p_2 = p_2'^3 - 3p_1'p_2' - 3. \end{cases} \quad (6)$$

Отсюда легко показать, что p_1' является делителем числа p_1-3, а p_2' - делитель числа p_2+3.

В общем случае для произвольного нечетного простого N=p составляется система уравнений относительно неизвестных p_1' и p_2':

$$\begin{cases} \varphi_1\left(p_1', p_2'\right) = p_1, \\ \varphi_2\left(p_1', p_2'\right) = p_2. \end{cases}$$

Дополнительно выводимые вспомогательные критерии позволяют свести дело к сравнительно небольшому конечному числу испытаний; они, в основном, опираются на соображения делимости и утверждения типа малой теоремы Ферма. Таким путем получаем вспомогательные сравнения следующего вида:

$$\left.\begin{aligned} p_1' - p_2' &\equiv p_1 - p_2 \\ -p_1' - p_2' &\equiv -p_1 - p_2 \end{aligned}\right\} \pmod N.$$

Из условий делимости следует конечное число комбинаций для p_1' и p_2' и для каждой такой комбинации – конечное число возможностей для показателя N=p.

Способ 2 [6].

По заданной единице ε определяются коэффициенты ее минимального многочлена. Далее вычисляется $\varepsilon^{\frac{1}{N}}$ (в качестве ε берется обратная единица такая, что $0 < \varepsilon < 1$) и находятся значения коэффициентов минимального многочлена для $\varepsilon^{\frac{1}{N}}$, если это целое кубическое число.

Очевидно, эти значения будут целыми тогда и только тогда, когда $\varepsilon^{\frac{1}{N}}$ – целое кубическое число, а значит, $\varepsilon^{\frac{1}{N}}$ – тоже единица.

1. Пусть a,b – два различных взаимно простых числа, a и b свободны от квадратов, a>0, b>0, тогда $m=ab^2 > 1$ свободно от кубов.

Легко показать, что целые числа чисто кубического поля $K\left(\sqrt[3]{m}\right)$ имеют вид:

$\alpha = \left(x + y\sqrt[3]{ab^2} + z\sqrt[3]{a^2b}\right)/3$, где $x, y, z \in Z$

и $x \equiv y \equiv z \equiv 0 \pmod 3$,

если $(a \pm b) \bmod 9 \neq 0$ (чисто кубическое поле 1 типа),

или $x \equiv ay \equiv bz \pmod 3$,

если $a \equiv \pm b \pmod 3$ (чисто кубическое поле 2 типа).

Очевидно, α удовлетворяет минимальному многочлену

$\alpha^3 - x\alpha^2 + \left(x^2 - abyz\right)\alpha/3 - \mathrm{Norm}\alpha = 0$,

где

$$\mathrm{Norm}\alpha = \left(x^3 + ab^2y^3 + a^2bz^3 - 3abxyz\right)/27 =$$

$$= \alpha\{\left(x^2 - abyz\right) + \left(az^2 - xy\right)\sqrt[3]{ab^2} +$$

$$+\left(by^2 - xz\right)\sqrt[3]{a^2b}\}/9 = \alpha\{\left(x - y\sqrt[3]{ab^2}\right)^2 +$$

$$+\left(y\sqrt[3]{ab^2} - z\sqrt[3]{a^2b}\right)^2 + \left(z\sqrt[3]{a^2b} - x\right)^2\}/18.$$

Легко устанавливаются следующие свойства единиц $K\left(\sqrt[3]{m}\right)$:

Лемма 1. Если $\mu = \left(x + y\sqrt[3]{ab^2} + z\sqrt[3]{a^2b}\right)/3 > 1$ - единица $K\left(\sqrt[3]{m}\right)$, то:

1) $\mathrm{Norm}\,\mu = 1$;

2) $xyz \neq 0$;

3) $x,\ y\sqrt[3]{ab^2}$ и $z\sqrt[3]{a^2b} \geq 1$;

4) $\mu > 3$.

Рассмотрим теперь соотношение между численным значением единицы и её минимальным многочленом.

Лемма 2. Пусть $\varepsilon = \mu^{-1} =$

$$= \left(X + Y\sqrt[3]{ab^2} + Z\sqrt[3]{a^2b}\right)/3 < 1,$$

тогда ε удовлетворяет минимальному многочлену $\varepsilon^3 - p_1\varepsilon^2 + p_2\varepsilon - 1 = 0$,

где $p_2 = \left(X^2 - abYZ\right)/3$.

Если $|ab| > 8$, то $p_2 > X^2/6$

и $|p_2 - \mu| < 2,75\sqrt{\varepsilon}$.

Из лемм 1 и 2 вытекает основная

Теорема 2. Пусть ε - единица чисто кубического поля $K\left(\sqrt[3]{m}\right)$, $0 < \varepsilon < 1$ и $\varepsilon_N = \varepsilon^{1/N}$ для некоторого целого положительного N.

1. Если ε_N - единица $K\left(\sqrt[3]{m}\right)$, то $\left|p_2 - \varepsilon_N^{-1}\right| < 2,75\varepsilon_N^{0,5}$.

2.При $\varepsilon_N < 0,04$ единица ε_N принадлежит чисто кубическому полю $K\left(\sqrt[3]{m}\right)$ тогда и только тогда, когда $\varepsilon_N^3 - p_1\varepsilon_N^2 + p_2\varepsilon_N - 1 = 0$, где $p_2 = \left\{\varepsilon_N^{-1}\right\}$, $p_1 = \left\{p_2\varepsilon_N^{-1} - \varepsilon_N^{-2}\right\}$ (символ {A} означает ближайшее целое число к вещественному числу A}.

Из выше изложенного вытекает алгоритм поиска основной единицы.

Пусть $\mu > 1$ - единица чисто кубического поля $K\left(\sqrt[3]{m}\right)$, $m=ab^2$, a и b целые числа, (a,b)=1, a и b свободны от квадратов, $|ab| > 8$. Обозначим $\mu(k) = \mu^{\frac{1}{k}}$.

1. Вычисляем

$$L = \begin{cases} 1 + \sqrt[3]{ab^2} + \sqrt[3]{a^2b} & \text{для полей 1 типа,} \\ \left(1 + \sqrt[3]{ab^2} + \sqrt[3]{a^2b}\right)/3 & \text{для полей 2 типа.} \end{cases}$$

2. Полагаем к=2.

3. Находим наименьшее целое число N такое, что $\mu^{\frac{1}{N}} < L$, то есть $N = \left[1 + \frac{\log\mu}{\log L}\right]$.

4. Если k≥N, то переходим к пункту 7.

5. Если не существует целое рациональное число p_2 такое, что $\left|p_2 - \mu(k)\right| < 2,75\sqrt{\mu(k)}$, то переходим к пункту 6 иначе если $p_1 = p_2\mu(k) - \mu^2(k) + \mu^{-1}(k)$ есть целое рациональное число, то переходим к пункту 7.

6. В качестве значения к выбираем следующее простое число и возвращаемся к пункту 4.

7. Полагаем $\mu = \mu(k)$ и переходим к пункту 3.

8. Значение μ определяет основную единицу. Конец.

Пример.

Пусть $\mu = x + y\sqrt[3]{23} + z\sqrt[3]{23^2}$

есть единица $K\left(\sqrt[3]{23}\right)$, где

x=25140112962713791879829592761725844051435101951166439999601;

y=88401156386104845950860246287875956789850137822456184256 60;

z=31084842228000027504059301520668641067249666353134343732 22;

$\mu \approx 7,542 \cdot 10^{58}$.

Находим, что L=11,93 а N=55.

Полагаем к=2, тогда

p_2=27462763678869134462755733220 3,

p_1=506123590417203.

$\mu(2) = \sqrt{\mu}$ есть единица. Так как существуют p_2 и p_1 целые числа, то повторяем вычисления с пункта 3. Находим N=28 и новое $\mu(2)$, которое не будет единицей, так как не выполняется условие пункта 5.

Берём следующее простое значение к=3.

Тогда p_2=6500020803, p_1=-124197 и получаем, что $\mu(3)$ есть единица $K\left(\sqrt[3]{23}\right)$.

Заменяем μ на $\sqrt[3]{\mu}$ и повторяем вычисления. Получаем N=10 при этом оказывается, что значения к=3, к=5 и к=7 не приводят к единицам, а следующее простое число к=11 оказывается больше N=10. Таким образом, оказывается, что исходная единица является шестой степенью основной единицы ε_o чисто кубического поля $K\left(\sqrt[3]{23}\right)$:

$$\varepsilon_o = \sqrt[6]{\mu} = 2166673601 + 761875860\sqrt[3]{23} + 267901370\sqrt[3]{23^2}.$$

Список литературы

1. Аванесов Э.Т., Гусев В.А., Каляманова К.Э. Методы вычисления основных единиц / Иван. энерг. ин-т им. В.И. Ленина. – Иваново, 1986. – 152 с. – Деп. в ВИНИТИ 2.06.86, № 3931.

2. Биллевич К.К. Численные методы в задачах теории алгебраических полей n-го порядка / СКГМИ. – Орджоникидзе, 1965. – 190 с. – Деп. в ВИНИТИ 10.10.85, №7174.

3. Делоне Б.Н., Фаддеев Д.К. Теория иррациональностей 3-й степени // Тр. МИАН СССР. – М., 1940. – Т.XI – 327 с.

4. Bernstein L. Applications of units // J.Number Theory. – 1978. – V.10. – № 3. – P. 354–383.

5. Dirichlet P.G.Lejene. Zur theorie der komplexen einhei – ten // Bericht. Verh. Preuss. Arad. Wiss. – 1846. – P. 103–107.

6. Hendy M., Jeans N. Determining the fundamental unit of a pure cubic field given any unit // Math. Comput. – 1978. – V.32. – №143. – P. 925–935.

7. Narkiewich W. Elementary and analytic theory of algebraic numbers. – Warszawa: PAN, 1974. – 387 p.

8. Zimmer H. Computational problems, methods and results in algebraic number theory // Lecture Notes in Math. – 1972. – V. 262. – P. 43.

9. Meissel E. Beitrag zur Pellschen Jleichung hoherer Jrade // Progr. 283 Ober-Kealschule Kiel. – 1891. – P. 1–11.