УДК 511.23

СПЕЦИАЛЬНЫЙ БАЗИС КОЛЬЦА ЦЕЛЫХ МАКСИМАЛЬНОГО ДЕЙСТВИТЕЛЬНОГО ПОДПОЛЯ 2-КРУГОВОГО ПОЛЯ

Р.Ж. Алеев, О.В. Митина

При изучении единиц целочисленных групповых колец циклических 2-групп было выяснено, что особую роль играют вычисления по модулю 2. В данной работе строится особый базис кольца целых максимального действительного кругового поля, полученного присоединением первообразного (примитивного) корня из единицы степени 2^n. Вычисления в этом базисе значительно облегчат нахождение единиц целочисленных групповых колец циклических 2-групп.

Ключевые слова: единицы групповых колец, целочисленное групповое кольцо.

Введение. Круговое поле, полученное присоединением первообразного (примитивного) корня из 1 степени 2^n, будем обозначать как $\mathbf{Q}_{2^n}$ или $\mathbf{Q}\left(\zeta_{2^n}\right)$, назовём 2-круговое поле, где ζ_{2^n} – примитивный корень из 1 степени 2^n. Так как поля $\mathbf{Q}_1=\mathbf{Q}_2=\mathbf{Q}$ и $\mathbf{Q}_4=\mathbf{Q}\left(i\right)$ давно детально изучены, а рассматриваемые далее задачи для таких полей тривиальны, то без ограничения общности будем считать, что $n\geq 3$ и обозначать для удобства $2^n=8m$.

Пусть K - подполе поля комплексных чисел $\mathbf{C}$ и $\overline{\mathbf{Z}}$ - кольцо всех целых алгебраических чисел. Обозначим через $\mathrm{Int}(K)=K\cap\overline{\mathbf{Z}}$ кольцо целых поля K и также через $\mathrm{Un}\left(\mathrm{Int}\left(K\right)\right)$ - группу единиц кольца $\mathrm{Int}\left(K\right)$.

1. Общие сведения

Обозначения. Положим $\xi_{8m}=\alpha$ и, не ограничивая общности, можем считать, что

$$\alpha=e^{i\frac{2\pi}{8m}}=\cos\frac{2\pi}{8m}+i\sin\frac{2\pi}{8m}.$$

Тогда, в частности:

$$\alpha^{4m}=-1,\ \alpha^{2m}=i,\ \alpha^{m}=\frac{\sqrt{2}}{2}\left(1+i\right).$$

Хорошо известен следующий результат.

Лемма 1. Целым базисом расширения $\mathbf{Q}(\alpha)/\mathbf{Q}$ является последовательность элементов $1,\alpha,\alpha^2,...,\alpha^{4m-1}$.

Определение. Для любого натурального n множество:

$$2\mathbf{Z}[\zeta_{8m}]=\{2\rho \mid \rho\in 2\mathbf{Z}[\zeta_{8m}]\}$$

является идеалом в $\mathbf{Z}[\zeta_{2n}]$. Поэтому возникает *сравнимость элементов из кольца* $\mathbf{Z}[\zeta_{2n}]$ *по модулю этого идеала*. Для краткости будем писать для элементов $\rho,\sigma\in Z[\zeta_{2n}]$:

$$\rho\equiv\sigma \pmod 2,$$

если $\rho\equiv\sigma \pmod{2\mathbf{Z}[\zeta_{8m}]}$, то есть $\rho\in\sigma+2\mathbf{Z}[\zeta_{8m}]$.

Замечание. В силу леммы 1 имеем, что:

$$2\mathbf{Z}[\alpha]=\left\{2\sum_{j=0}^{4m-1}b_j\alpha^j \,\middle|\, \{b_0,b_1,\ldots,b_{4m-1}\}\subset\mathbf{Z}\right\}.$$

В частности, получим, что для элемента $b=\sum_{j=0}^{4m-1}b_j\alpha^j\in\mathbf{Z}[\alpha]$ сравнение

$$b\equiv 1 \pmod 2$$

выполняется тогда и только тогда, когда b_0 - нечётное число, b_j - четное число для $j\in\{1,2,...,4m-1\}$.

2. Две полезных последовательности

Обозначение. Для любого целого j положим:

$$s_j=\alpha^j+\alpha^{-j}=2\cos\frac{2\pi}{8m}j=2\cos\frac{\pi}{4m}j.$$

Свойства последовательности $\{s_j\}_{j\in\mathbf{Z}}$ изучены в лемме 2 работы [1]. Из них для последующих применений извлечём очевидное, но весьма полезное следствие.

Лемма 2. *Последовательность* $\{s_j\}_{j\in\mathbf{Z}}$ *по модулю* 2 *периодична с периодом* $4m$ *и имеет следующие свойства*.

1. $s_0\equiv s_{2m}\equiv 0 \pmod 2$, $s_m\equiv s_{3m}\equiv\sqrt{2} \pmod 2$.

2. *Набор* $(s_1,...,s_{4m-1})$ *симметричен относительно центра, то есть для* $j\in\{1,2,\ldots,2m\}$:

$$s_{4m-j}\equiv s_j \pmod 2.$$

Для любых целых j и k:

$$s_j s_k = s_{j+k} + s_{k-j},$$

в частности, $s_j^2 \equiv s_{2j} \pmod 2$, *причём* $s_0^2 \equiv s_{2m}^2 \equiv s_m^2 \equiv s_{3m}^2 \equiv 0 \pmod 2$.

Обозначение. Для любого целого j положим:

$$r_j = s_j + s_{2m-j}.$$

Замечание. Ясно, что

$$r_j = s_j + s_{2m-j} = 2\cos\frac{\pi}{4m} j + 2\cos\frac{\pi}{4m}(2m - j) =$$
$$= 2\cos\frac{\pi}{4m} j + 2\cos\left(\frac{\pi}{2} - \frac{\pi}{4m} j\right) = 2\cos\frac{\pi}{4m} j + 2\sin\frac{\pi}{4m} j.$$

Лемма 3. *Последовательность* $\{r_j\}_{j\in\mathbf{Z}}$ *периодична с периодом* $8m$. *Кроме того, отрезок* $(r_0,...,r_{8m-1})$ *последовательности* $\{r_j\}_{j\in\mathbf{Z}}$ *разбивается на части*:

$$\{r_0 = 2\} \cup R_0 = \left(r_1,...,r_m = 2\sqrt{2},...,r_{2m-1}\right),$$

$$\{r_{2m} = 2\} \cup R_1 = \left(r_{2m+1},...,r_{3m} = 0,...,r_{4m-1}\right),$$

$$\{r_{4m} = -2\} \cup R_2 = \left(r_{4m+1},...,r_{5m} = -2\sqrt{2},...,r_{6m-1}\right),$$

$$\{r_{6m} = -2\} \cup R_3 = \left(r_{6m+1},...,r_{7m} = 0,...,r_{8m-1}\right).$$

Упорядоченные наборы R_0, R_1, R_2 *и* R_3 *имеют следующие свойства*.

1. $R_2 = -R_0$ *и* $R_3 = -R_1$, *то есть состоят из противоположных чисел.*

2. *Для любого целого числа* j:

$$r_{2m+j} = r_j - 2s_{2m-j} = r_{-j}.$$

3. *Каждый из наборов* R_0 и R_2 *центрально симметричен, то есть для любых* $k \in \{0,2\}$ *и* $j \in \{1,...,m\}$:

$$r_{2mk+j} = r_{2m(k+1)-j}.$$

Каждый из наборов R_1 *и* R_3 *центрально антисимметричен, то есть для любых* $k \in \{1,3\}$ *и* $j \in \{1,\ldots,m\}$

$$r_{2mk+j} = -r_{2m(k+1)-j}.$$

Доказательство. Всё получается из леммы 2 в [1] простыми вычислениями, ибо $r_j = s_j + s_{2m-j}$ для любого целого j.

Лемма доказана.

Рассмотрим последовательность $\{r_j\}_{j\in\mathbf{Z}}$, приведённую по модулю 2.

Лемма 4. *Последовательность* $\{r_j\}_{j\in\mathbf{Z}}$ *по модулю* 2 *периодична с периодом* $2m$. *Более точно, в обозначениях леммы* 3 *последовательность* $\{r_j\}_{j\in\mathbf{Z}}$ *по модулю* 2 *имеет следующие свойства.*

1. $r_0 \equiv r_m \equiv 0 \pmod 2$.

2. $R_0 \equiv R_1 \equiv R_2 \equiv R_3 \pmod 2$. *Здесь имеется в виду поэлементная сравнимость по модулю* 2 *упорядоченных наборов* R_0, R_1, R_2 *и* R_3.

3. Набор R_0 *центрально симметричен по модулю* 2, то есть для любого $j \in \{1,\ldots,m\}$:

$$r_j \equiv r_{2m-j} \pmod 2.$$

Доказательство. Всё очевидно следует из леммы 3.
Лемма доказана.

Лемма 5. *Для любого целого числа* j *имеем:*

$$r_j \equiv (1+i)s_j = \sqrt{2}\alpha^m s_j \pmod 2.$$

Доказательство. Для любого целого числа j имеем:

$$r_j = s_j + s_{2m-j} = \left(\alpha^j + \alpha^{-j}\right) + \left(\alpha^{2m-j} + \alpha^{-2m+j}\right) =$$

$$= \left(a^j + a^{-j}\right) + \left(a^{2m}a^{-j} + a^{-2m}a^j\right) =$$

$$= \left(a^j + a^{-j}\right) + \left(ia^{-j} - ia^j\right) = \left(1-i\right)a^j + \left(1+i\right)a^{-j} =$$

$$= (1+i)\alpha^j + (1+i)\alpha^{-j} = (1+i)\left(\alpha^j + \alpha^{-j}\right) = (1+i)s_j \pmod 2.$$

Далее:

$$1+i = \sqrt{2}\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) = \sqrt{2}\alpha^m.$$

Лемма доказана.

Лемма 6. *Элементы последовательностей* $\{s_j\}_{j\in\mathbf{Z}}$ и $\{r_j\}_{j\in\mathbf{Z}}$ *перемножаются по модулю* 2 *следующим образом. Для любых целых* j *и* k:

$s_j s_k = s_{j+k} + s_{k-j}$,

в частности, $s_k^2 \equiv s_{2k} \pmod 2$, $s_0^2 \equiv s_m^2 \equiv 0 \pmod 2$;

$s_j r_k = r_{k-j} + r_{k+j}$,

в частности, $s_k r_k \equiv r_{2k} \pmod 2$;

$r_j r_k \equiv 0 \pmod 2$.

Доказательство. Применяя лемму 5, всё легко получится из леммы 2.

Лемма доказана.

3. Максимальное действительное подполе $\mathbf{Q}_{2^n}$ R кругового поля $\mathbf{Q}_{2^n}$

Лемма 7. *Для любого натурального числа* j *выполняются следующие равенства*

$$s_{2j} = s_1^{2j} + \sum_{k=0}^{j-1} (-1)^{j-k} \left(C_{j+1}^{j-k} + C_{j+k-1}^{j-k-1} \right) s_1^{2k},$$

$$s_{2j+1} = s_1^{2j+1} + \sum_{k=0}^{j-1} (-1)^{j-k} \left(C_{j+1+k}^{j-k} + C_{j+k}^{j-k-1} \right) s_1^{2k+1},$$

$$s_1^{2j} = C_{2j}^{j} + s_{2j} + \sum_{k=1}^{j-1} C_{2j}^{k} s_{2(j-k)},$$

$$s_1^{2j+1} = s_{2j+1} + \sum_{k=1}^{j-1} C_{2j+1}^{k} s_{2(j-k)+1}.$$

Доказательство. Первые две формулы непосредственно следуют из предложения 1 в [2].

По формуле бинома Ньютона:

$$\left(\alpha + \alpha^{-1}\right)^{2j} = \alpha^{2j} + \sum_{k=1}^{2j-1} C_{2j}^{k} \alpha^{2j-k} \alpha^{-k} + \alpha^{-2j} = \alpha^{2j} + \alpha^{-2j} + \sum_{k=1}^{2j-1} C_{2j}^{k} \alpha^{2(j-k)} =$$

$$= \left(\alpha^{2j} + \alpha^{-2j}\right) + \sum_{n=1}^{j-1} C_{2j}^{n} \alpha^{2(j-k)} + C_{2j}^{j} + \sum_{k=j+1}^{2j-1} C_{2j}^{k} \alpha^{2(j-k)} =$$

во второй сумме положим $j - k = l - j \leftrightarrow k = 2j - l$

$$= C_{2j}^{j} + \left(\alpha^{2j} + \alpha^{-2j}\right) + \sum_{k=1}^{j-1} C_{2j}^{k} \alpha^{2(j-k)} + \sum_{l=1}^{j-1} C_{2j}^{2j-l} \alpha^{-2(j-l)} =$$

так как $C_{2j}^{k} = C_{2j}^{2j-k}$, то

$$= C_{2j}^{j} + \left(\alpha^{2j} + \alpha^{-2j}\right) + \sum_{k=1}^{j-1} C_{2j}^{k} \left(\alpha^{2(j-k)} + \alpha^{-2(j-k)}\right),$$

что и надо. Для нечётной степени аналогично.

Лемма доказана.

Лемма 8. *Степень расширения* $\left[\mathbf{Q}(\alpha)\cap\mathbf{R}:\mathbf{Q}\right]=2^{n-2}$ *и поле* $\mathbf{Q}(\alpha)\cap\mathbf{R}$ *имеет два следующих целых базиса*:

А. $1, s_1=a+a^{-1}, s_1^2=\left(a+a^{-1}\right)^2,\ldots,s_1^{2^{n-2}-1}=\left(a+a^{-1}\right)^{2^{n-2}-1}$.

Б. $1, s_1=\alpha+\alpha^{-1}, s_2=\alpha^2+\alpha^{-2},\ldots,s_{2^{n-2}-1}=\alpha^{2^{n-2}-1}+\alpha^{-2^{n-2}+1}$.

В частности, кольцом целых $\mathrm{Int}\left(\mathbf{Q}\left(a\right)\ \mathbf{R}\right)$ *поля* $\mathbf{Q}\left(a\right)\ \mathbf{R}$ *является кольцо* $\mathbf{Z}\left[\alpha+\alpha^{-1}\right]$.

Доказательство. Ясно, что $\mathbf{Q}\left(\alpha^{-1}+\alpha\right)\subseteq\mathbf{Q}(\alpha)\cap\mathbf{R}$. Пусть $\beta=\sum_i a_i\alpha^i\in\mathbf{Q}(\zeta)\cap\mathbf{R}$, где для любого i коэффициенты $a_i\in\mathbf{Q}$. Тогда $\overline{\beta}=\beta$, но $\overline{\beta}=\sum_i a_i\overline{\alpha}^i=\sum_i a_i\alpha^{-i}$. Поэтому $\beta=\sum_i\frac{a_i}{2}\left(\alpha^i+\alpha^{-i}\right)$. Поскольку $\alpha^i+\alpha^{-i}$ выражается с целыми коэффициентами через $\alpha+\alpha^{-1}$ по лемме 7, то $\beta\in\mathbf{Q}\left(\alpha^{-1}+\alpha\right)$, то есть $\mathbf{Q}\left(\alpha^{-1}+\alpha\right)\supseteq\mathbf{Q}(\alpha)\cap\mathbf{R}$. Таким образом, $\mathbf{Q}\left(a^{-1}+a\right)=\mathbf{Q}\left(a\right)\ \mathbf{R}$.

Ясно, что $\mathbf{Q}\left(a^{-1}+a\right)=\mathbf{Q}\left(a\right)\ \mathbf{R}$ - неподвижное относительно комплексного сопряжения подполе поля $\mathbf{Q}(\alpha)$. Всё следует из леммы 1 по основной теореме теории Галуа [3, §58] и теореме из [3, §59, с. 202].

Утверждение о базисах следует из [4] и леммы 7.

Замечание. Как в замечании на с. 2, в силу леммы 8 имеем, что

$$2\mathbf{Z}\left[\alpha+\alpha^{-1}\right]=\left\{2\sum_{j=0}^{2^{n-2}-1}b_j\,s_j\,\middle|\,\left\{b_0,b_1,\ldots,b_{2^{n-2}-1}\right\}\subset\mathbf{Z}\right\}.$$

В частности, получим, что для $b=\sum_{j=0}^{2^{n-2}-1}b_j s_j\in\mathbf{Z}\left[\alpha+\alpha^{-1}\right]$ сравнение

$$b\equiv 1\pmod 2$$

выполняется тогда и только тогда, когда b_0 - нечётное число, b_j - чётное число для $j\in\left\{1,2,\ldots,2^{n-2}-1\right\}$.

Определение. Обозначим для удобства:

$$\vec{S}=\left(s_1,\ldots,s_{m-1}\right)\text{ и }\vec{R}=\left(r_1,\ldots,r_{m-1}\right).$$

Определим в поле $\mathbf{Q}\left(a\right)\ \mathbf{R}$ новый особый (упорядоченный) базис:

$$\vec{B} = \left(1, \vec{S}, s_m, \vec{R}\right) = \left(1, s_1, ..., s_{m-1}, s_m, r_1, ..., r_{m-1}\right).$$

Также пусть $R_{\mathbf{Z}}$ подгруппа (по сложению), порождённая $\vec{R}$, то есть:

$$R_{\mathbf{Z}} = \left\{a_1 r_1 + ... + a_{m-1} r_{m-1} \middle| \{a_1, ..., a_{m-1}\} \subset \mathbf{Z}\right\}.$$

Наконец, определим подгруппу (по сложению):

$$\tilde{\mathrm{R}} = \mathrm{R}_{\mathbf{Z}} + 2\mathbf{Z}\left[\mathrm{s}_1\right] = \mathrm{R}_{\mathbf{Z}} + 2\mathbf{Z}\left[\alpha + \alpha^{-1}\right].$$

Лемма 9. *Определённый выше базис* $\vec{B}$ *поля* $\mathbf{Q}(a)$ $\mathbf{R}$ *имеет следующие свойства.*

1. *Для любого* $j \in \{1, 2, ..., m-1\}$:

$$r_j = s_j + s_{2m-j} \text{ и } s_{2m+j} = r_{m-j} - s_{m-j}.$$

2. $\vec{B}$ *– целый базис поля* $\mathbf{Q}(a)$ $\mathbf{R}$.

3. *Элементы базиса* $\vec{B}$ *перемножаются по модулю* 2 *следующим образом:*

$s_j s_k = s_{k-j} + s_{k+j}$, *если* $j \le k$ *и* $k + j \le m$, *в частности,* $s_j^2 \equiv s_{2j} \pmod 2$;

$s_j s_k = s_{k-j} + r_{2m-(k+j)} - s_{2m-(k+j)}$, *если* $j \le k$ *и* $k + j > m$,

в частности, $s_j^2 \equiv r_{2m-2j} - s_{2m-2j} \pmod 2$ *и* $s_m^2 \equiv 0 \pmod 2$;

$s_j r_k = r_{k-j} + r_{k+j}$ *если* $j \le k$ *и* $k + j < m$, *в частности,* $s_j r_j \equiv r_{2j} \pmod 2$;

$s_j r_k = r_{j-k} + r_{k+j}$ *если* $j \le k$ *и* $k + j = m$, *в частности,* $s_{m/2} r_{m/2} \equiv 0 \pmod 2$;

$s_j r_k = r_{k-j} + r_{2^{n-2}-(k+j)}$ *если* $j \le k$, $k + j > m$,

в частности, $s_j r_j \equiv r_{2m-2j} \pmod 2$;

$s_{2^{n-3}} r_k \equiv 0 \pmod 2$;

$s_j r_k \equiv r_{j-k} + r_{k+j} \pmod 2$, *если* $k < j < m$ *и* $k + j < m$;

$s_j r_k \equiv r_{j-k} \pmod 2$, *если* $k < j < m$ *и* $k + j = m$;

$s_j r_k \equiv r_{j-k} + r_{2m-(k+j)} \pmod 2$, *если* $k < j < m$ *и* $k + j > m$;

$r_j r_k \equiv 0 \pmod 2$.

Доказательство

1. Для любого $j \in \{1, 2, ..., m-1\}$ по определению $r_j = s_j + s_{2m-j}$ и

$$s_{m+j} = s_{2m-(m-j)} = s_{2m-(m-j)} + s_{m-j} - s_{m-j} = r_{m-j} - s_{m-j}.$$

2. Утверждение следует из леммы 8 и утверждения 1 данной леммы.

3. Утверждение – непосредственное следствие леммы 6 и утверждения 1 данной леммы.

Лемма доказана.

Теорема. *Определённая ранее подгруппа* $\tilde{R}$ *является идеалом кольца* $\mathbf{Z}[s_1] = \mathbf{Z}\left[\alpha + \alpha^{-1}\right]$, *причём*

$$R_{\mathbf{Z}}^2 \subseteq 2\mathbf{Z}\left[\alpha + \alpha^{-1}\right].$$

Иными словами $\tilde{R} / 2\mathbf{Z}\left[\alpha + \alpha^{-1}\right]$ *является идеалом с нулевым умножением фактор-кольца* $\mathbf{Z}\left[\alpha + \alpha^{-1}\right] / 2\mathbf{Z}\left[\alpha + \alpha^{-1}\right]$.

Доказательство. Это непосредственное следствие леммы 9.

Библиографический список

1. Алеев, Р.Ж. Сравнение по модулю 2 круговых единиц в полях Q_{16} и Q_{32} / Р.Ж. Алеев, О.В. Митина, Е.А. Христенко // Челяб. физ.-мат. журн. – 2016. - Т. 1, Вып. 4. – С. 8-29.

2. Алеев, Р.Ж, Вычисление квантовых факториалов и к ним обратных / Р.Ж. Алеев, И.Р. Мухамадеева // Челяб. физ.-мат. журн. – 2016. - Т. 1, Вып. 1. - С. 6–15.

3. Ван дер Варден, Б.Л. Алгебра / Б.Л. Ван дер Варден. – 2-е изд. - М.: Наука, 1979. – 624 с.

4. Liang, J.J. On the integral basis of the maximal real subfield of a cyclotomic field / J.J. Liang // Journ. für die Reine und Angew. Math., Band 286/287, 1976. - P. 223-226.

К содержанию