Построение накрытий простых групп с помощью евклидовых решёток

А. К. МАРТИРОСОВ
Московский физико-технический институт
e-mail: ar.martirosov2011@yandex.ru

УДК 512.542.5

Ключевые слова: система Штейнера, линейный код, сильно регулярный граф, евклидово кольцо, решётка, простая группа, накрытие группы, мультипликатор Шура.

Аннотация

Целью данной работы является построение некоторых исключительных (не вкладывающихся в бесконечные семейства) накрытий конечных простых групп. Основным инструментом при этом служат дискретные решётки в действительных и комплексных евклидовых пространствах.

Пусть G — произвольная группа. Её накрытием называется любая группа $\tilde{G}$, в которой существует подгруппа $Z \leqslant Z(\tilde{G}) \cap \tilde{G}'$, удовлетворяющая условию $\tilde{G}/Z \cong G$.

Известно, что для любой конечной группы G любое её накрытие также конечно, причём существует некоторое накрытие $\tilde{G}$ наибольшего порядка. Соответствующая подгруппа $Z \leqslant \tilde{G}$ определена однозначно с точностью до изоморфизма и называется мультипликатором Шура группы G. Если $G' = G$ (в частности, если G простая неабелева), то и $\tilde{G}$ определена однозначно с точностью до изоморфизма.

Суть используемого метода в общем случае заключается в следующем. В пространстве $\mathbb{R}^n$ или $\mathbb{C}^n$ строится некоторая решётка X, рассматриваемая как $\mathcal{E}$-модуль для некоторого евклидова кольца $\mathcal{E}$. В силу дискретности X её группа автоморфизмов G конечна. Фактор-решётка X по некоторой подрешётке αX, $\alpha \in \mathcal{E}$, рассматривается как векторное пространство над полем $\mathcal{E}/\alpha\mathcal{E}$, на котором вводится билинейная или полуторалинейная форма, индуцированная скалярным произведением в $\mathbb{R}^n$ ($\mathbb{C}^n$). В результате этого фактор-группа G по подгруппе скалярных матриц оказывается вложенной в некоторую конечную линейную группу, откуда и следует существование накрытия этой линейной группы или её подгруппы.

В данной работе метод будет продемонстрирован на примере исключительных накрытий $2 \cdot \Omega_8^+(2)$, $3 \cdot \mathrm{U}_4(3)$ и $4 \cdot M_{22}$. В процессе их построения будут также получены исключительные накрытия $3 \cdot A_6$, $3 \cdot A_7$ (в действительности при $n \neq 6, 7$ группа A_n не допускает тройного накрытия) и вложение $\mathrm{U}_4(3) \,.\, 2 \hookrightarrow \mathrm{U}_6(2)$.

Abstract

A. K. Martirosov, Constructions of coverings of simple groups using Euclidean lattices, Fundamentalnaya i prikladnaya matematika, vol. 25 (2024), no. 1, pp. 161—203.

The goal of this work is to construct some exceptional (not involved in any infinite family) coverings of finite simple groups. The main tool of this construction is provided by discrete lattices in real and complex Euclidean spaces.

Let G be any group. Its covering group is any group $\tilde{G}$ with a subgroup $Z \leqslant Z(\tilde{G}) \cap \tilde{G}'$ satisfying the condition $\tilde{G}/Z \cong G$.

Фундаментальная и прикладная математика, 2024, том 25, № 1, с. 161—203.

It is known that, for any finite group G, any of its covering groups is also finite, and there is a cover $\tilde{G}$ of the maximal order. The corresponding subgroup $Z \leqslant \tilde{G}$ is uniquely defined up to isomorphism and is called the Schur multiplier of G. If $G' = G$ (in particular, if G is non-Abelian simple), then $\tilde{G}$ is also uniquely defined up to isomorphism.

The essence of the method used is as follows. A lattice X considered as an $\mathcal{E}$-module for some Euclidean ring $\mathcal{E}$ is constructed in the space $\mathbb{R}^n$ or $\mathbb{C}^n$. Since X is discrete, its automorphism group G is finite. The quotient of the lattice X by some of its sublattice αX, $\alpha \in \mathcal{E}$, is considered as a vector space over the field $\mathcal{E}/\alpha\mathcal{E}$, on which we define a bilinear or sesquilinear form induced by the usual dot product in $\mathbb{R}^n$ ($\mathbb{C}^n$). As a result, the quotient group G by the subgroup of scalar matrices turns out to be embedded in some finite linear group, and the existence of a cover of this linear group or its subgroup now follows.

In this work, the method will be demonstrated by the example of exceptional coverings $2 \cdot \Omega_8^+(2)$, $3 \cdot \mathrm{U}_4(3)$ and $4 \cdot M_{22}$. While constructing them, the exceptional covers $3 \cdot A_6$, $3 \cdot A_7$ (in fact, for $n \neq 6, 7$, the group A_n does not admit a triple cover) and the embedding $\mathrm{U}_4(3) \,.\, 2 \hookrightarrow \mathrm{U}_6(2)$ will also be obtained.

1. Обозначения

— n — циклическая группа порядка n;
— $\mathrm{L}_n(q)$ — проективная специальная линейная группа $\mathrm{PSL}_n(q)$;
— $\mathrm{U}_n(q)$ — проективная специальная унитарная группа $\mathrm{PSU}_n(q)$;
— $A : B$, $A \cdot B$, $A \,.\, B$ — расщепляющееся, нерасщепляющееся и произвольное расширения группы A при помощи группы B соответственно;
— $A \times B$ — прямое произведение групп A и B;
— симметрическая разность подмножеств X, Y далее называется *суммой* и обозначается $X + Y$;
— $(a^p\, b^q \ldots)$ — вектор, у которого некоторые p координат равны a, некоторые q координат равны b и т. д.;
— $[a^p\, b^q \ldots]$ — вектор, у которого некоторые p координат имеют квадрат модуля a, некоторые q координат имеют квадрат модуля b и т. д.

2. Предварительные сведения

2.1. Системы Штейнера

Определение 2.1. *Системой Штейнера* $S(t, k, v)$ называется пара $(\Omega, \mathcal{B})$, где Ω — множество порядка v и $\mathcal{B}$ — некоторый набор подмножеств Ω порядка k, называемых *блоками*, удовлетворяющий следующему условию: каждое подмножество Ω порядка t содержится в единственном блоке.

Автоморфизмом системы Штейнера $(\Omega, \mathcal{B})$ называется перестановка на множестве Ω, переводящая блоки в блоки.

Нетрудно видеть, что $|\mathcal{B}| = C_v^t / C_k^t$. Также нетрудно видеть, что если множества Ω, $\mathcal{B}$ удовлетворяют свойству, что каждое подмножество $X \subseteq \Omega$ порядка t

содержится *хотя бы в одном* из блоков $\mathcal{B}$, причём $|\mathcal{B}| = C_v^t/C_k^t$, то для каждого подмножества X такой блок ровно один, т. е. $(\Omega, \mathcal{B})$ является системой Штейнера $S(t,k,v)$.

2.2. Линейные коды над конечными полями

Определение 2.2. Пусть $\mathbb{F} = \mathbb{F}_q$ — конечное поле порядка q. Подпространство A в пространстве строк $\mathbb{F}^n$ называется $[n,k,d]_q$-*кодом*, если $\dim A = k$ и минимальное число ненулевых координат в ненулевых строках из A равно d. Элементы кода A называются *кодовыми словами*. *Носителем* $\operatorname{supp} v$ кодового слова $v \in A$ называется множество его ненулевых координат, а *весом* $\operatorname{wt} v$ слова v называется мощность множества $\operatorname{supp} v$.

Изоморфизмом двух кодов $A, B \leqslant \mathbb{F}^n$ называется мономиальное преобразование пространства $\mathbb{F}^n$, переводящее A в B. *Автоморфизмом* кода A называется изоморфизм A в себя. *Двойственным* к A кодом называется ортогональное дополнение к A относительно естественного скалярного произведения на $\mathbb{F}^n$:

$$f(x,y) = \sum_{i=1}^{n} x_i y_i, \quad x = (x_1, \ldots, x_n), \quad y = (y_1, \ldots, y_n),$$

либо если q является квадратом и поле $\mathbb{F}$ допускает автоморфизм порядка 2 (сопряжение), то иногда рассматривается произведение

$$f(x,y) = \sum_{i=1}^{n} x_i \bar{y}_i.$$

Код A называется *самодвойственным*, если он совпадает со своим двойственным.

Так как автоморфизм кода по определению является перестановкой не самого кода A, а всего пространства $\mathbb{F}^n$, то нетривиальные автоморфизмы A могут действовать на A тривиально. Это происходит, например, с одномерным кодом $A = \langle (1, \ldots, 1) \rangle \leqslant \mathbb{F}^n$.

2.3. Сильно регулярные графы

Определение 2.3. *Сильно регулярным графом* $\operatorname{srg}(v,k,\lambda,\mu)$ называется простой неориентированный граф G с множеством вершин V, обладающий следующими свойствами:

1) $|V| = v$;
2) каждая вершина имеет ровно k соседей;
3) любые две соседние вершины имеют ровно λ общих соседей;
4) любые две несоседние вершины имеют ровно μ общих соседей.

Докажем основное соотношение на параметры сильно регулярного графа.

Лемма 2.1. *Для сильно регулярного графа* $\mathrm{srg}(v,k,\lambda,\mu)$ *выполнено равенство* $(v-k-1)\mu = k(k-\lambda-1)$.

Доказательство. Рассмотрим произвольную вершину $x \in V$ и разобьём множество V на три яруса: первый ярус состоит из одной вершины x, второй ярус состоит из всех её соседей, третий — из остальных вершин. Посчитаем двумя способами число рёбер, соединяющих второй ярус с третьим. Каждая вершина второго яруса имеет k соседних, из которых одна совпадает с x и ещё λ вершин лежат во втором ярусе. Следовательно, искомое число рёбер равно $k(k-\lambda-1)$. С другой стороны, каждая вершина третьего яруса имеет μ соседей во втором ярусе, следовательно, искомое число рёбер равно $(v-k-1)\mu$. □

Сильно регулярные графы часто возникают из теоретико-групповых соображений.

Лемма 2.2. *Пусть* G *— транзитивная группа перестановок ранга* 3 *на множестве* X. *Пусть также* $|G|$ *чётный. Тогда на множестве* X *можно естественным образом определить некоторый сильно регулярный граф, на котором* G *действует автоморфизмами.*

Доказательство. По условию G имеет три орбиты при действии на $X \times X$, одна из которых — это $\{(x,x),\ x \in X\}$. Обозначим через Γ, Δ оставшиеся две орбиты. Пусть $g \in G$ — инволюция, (xy) — одна из её транспозиций. Можно считать, что $(x,y) \in \Gamma$. Тогда для любого $(a,b) \in \Gamma$ найдётся $h \in G$, $h(a,b) = (x,y)$ и $(h^{-1}gh)(a,b) = (b,a) \in \Gamma$, т. е. орбита Γ *симметрична*. Следовательно, Δ также симметрична.

Определим граф на X следующим образом: вершины $x \neq y \in X$ соседние тогда и только тогда, когда $(x,y) \in \Gamma$. Такое определение корректно в силу симметричности Γ. Ясно, что G действует на нём автоморфизмами, и так как G транзитивна на парах соседних и на парах несоседних рёбер, то граф сильно регулярный. □

2.4. Евклидовы кольца в $\mathbb{C}$

Определение 2.4. *Евклидовым кольцом* называется ассоциативное коммутативное кольцо $\mathcal{E}$ с единицей без делителей нуля, на котором определена *норма* $N\colon \mathcal{E}\setminus\{0\} \to \mathbb{N}\cup\{0\}$, удовлетворяющая следующим условиям:

1) $N(ab) \geqslant N(a)$ для всех $a,b \in \mathcal{E}\setminus\{0\}$, причём $N(ab) = N(a)$ тогда и только тогда, когда b обратим;
2) для любых $a \in \mathcal{E}$, $b \in \mathcal{E}\setminus\{0\}$ существуют $q,r \in \mathcal{E}$, такие что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$.

Как известно, евклидовы кольца являются кольцами главных идеалов, и следовательно, факториальны.

Лемма 2.3. *В евклидовом кольце* $\mathcal{E}$ *обратимыми являются в точности все ненулевые элементы минимальной нормы.*

Доказательство. Пусть $b \in \mathcal{E} \setminus \{0\}$ — элемент минимальной нормы. Тогда для некоторых $q, r \in \mathcal{E}$ имеем $1 = qb + r$, и если $r \neq 0$, то $N(r) < N(b)$, что противоречит выбору b. Следовательно, $1 = qb$, т. е. b обратим.

С другой стороны, все обратимые элементы имеют одинаковую норму: если $e \in \mathcal{E}$ обратим, то $N(e) = N(e \cdot 1) = N(1)$. □

Далее рассматриваются кольца вида $\mathbb{Z}[\alpha] = \{m + n\alpha,\ m, n \in \mathbb{Z}\}$, где $\alpha \in \mathbb{C}$. Чтобы такое множество было кольцом, необходимо и достаточно, чтобы α было целым алгебраическим числом степени не выше 2. Оно является дискретным подмножеством $\mathbb{C}$ тогда и только тогда, когда либо $\alpha \in \mathbb{Z}$ (но тогда $\mathbb{Z}[\alpha] = \mathbb{Z}$ — этот случай не рассматривается), либо $\alpha \notin \mathbb{R}$.

Теорема 1. *Пусть $\alpha \in \mathbb{C} \setminus \mathbb{R}$ — целое алгебраическое число степени 2. Кольцо $\mathcal{E} = \mathbb{Z}[\alpha]$ является евклидовым относительно нормы $N\colon \mathcal{E} \setminus \{0\} \to \mathbb{N} \cup \{0\}$, $N(z) = |z|^2$, тогда и только тогда, когда каждый открытый круг в $\mathbb{C}$ радиуса 1 содержит элемент из $\mathcal{E}$.*

Доказательство. Функция N корректно определена, поскольку элементы $\mathcal{E}$ целые алгебраические и $\alpha \notin \mathbb{R}$. Она мультипликативна: $N(ab) = N(a)N(b)$ для любых $a, b \in \mathcal{E} \setminus \{0\}$, следовательно, $N(ab) \geqslant N(a)$. Если $N(ab) = N(a)$, то $N(b) = |b|^2 = 1$, и если $b = m + n\alpha$, то $b^{-1} = \bar{b} = m + n\bar{\alpha}$. Так как $\alpha + \bar{\alpha} \in \mathbb{Z}$, то $\bar{\alpha} \in \mathcal{E}$, $b^{-1} \in \mathcal{E}$, т. е. b обратим. Обратно, если b обратим, то $b^{-1} \in \mathcal{E}$, следовательно, числа $|b|^2$, $|b^{-1}|^2$ целые и $1 = |bb^{-1}|^2 = |b|^2|b^{-1}|^2$, откуда получаем, что $N(b) = |b|^2 = 1$, $N(ab) = N(a)$ для всех $a \in \mathcal{E} \setminus \{0\}$.

Пусть каждый открытый круг в $\mathbb{C}$ радиуса 1 содержит элемент из $\mathcal{E}$. Возьмём произвольные элементы $a \in \mathcal{E}$, $b \in \mathcal{E} \setminus \{0\}$ и найдём элемент $q \in \mathcal{E}$, лежащий в круге радиуса 1 с центром в точке $a/b \in \mathbb{C}$. Если $r = a - qb$, то либо $r = 0$, либо

$$N(r) = N(b)\left|\frac{a}{b} - q\right|^2 < N(b),$$

следовательно, E является евклидовым кольцом.

Обратно, пусть кольцо $\mathcal{E}$ евклидово относительно нормы N. Тогда для любых $a, b \in \mathcal{E}$, $b \neq 0$, найдутся $q, r \in \mathcal{E}$ с условием $a = qb + r$, где $|r| < |b|$. Это означает, что

$$\left|\frac{a}{b} - q\right| = \left|\frac{r}{b}\right| < 1,$$

т. е. любой открытый круг радиуса 1 с центром в точке a/b, $a, b \in \mathcal{E}$, $b \neq 0$, содержит элемент из $\mathcal{E}$.

Докажем, что множество $X = \{a/b,\ a, b \in \mathcal{E},\ b \neq 0\}$ всюду плотно в $\mathbb{C}$. Множество $Y = \{(m + ni)/k,\ m, n, k \in \mathbb{Z},\ k \neq 0\}$ всюду плотно в $\mathbb{C}$, поскольку представляет собой множество всех точек в $\mathbb{R}^2$ с рациональными координатами. Применяя к Y некоторое (непрерывное) невырожденное $\mathbb{R}$-линейное преобразование плоскости $\mathbb{R}^2$, получаем, что множество $\{a/k,\ a \in \mathcal{E},\ k \in \mathbb{Z} \setminus \{0\}\}$, а следовательно и X, всюду плотно в $\mathbb{C}$.

Пусть теперь некоторый открытый круг U радиуса 1 с центром в точке $z \in \mathbb{C}$ не пересекает $\mathcal{E}$. Если на границе U имеется не более двух точек $\mathcal{E}$, то

и в некоторой окрестности замкнутого круга $\bar{U}$ также имеется не более двух точек $\mathcal{E}$. Но тогда, взяв круг радиуса 1 с центром из X, достаточно близким к z, получим противоречие. Пусть теперь на границе U лежат три различные точки $a, b, c \in \mathcal{E}$. Нетрудно доказать, что тогда

$$z = \frac{a(b\bar{b} - c\bar{c}) + b(c\bar{c} - a\bar{a}) + c(a\bar{a} - b\bar{b})}{a\bar{b} - \bar{a}b + b\bar{c} - \bar{b}c + c\bar{a} - \bar{c}a},$$

т. е. z представляется в виде дробно-рациональной функции от чисел a, b, c, $\bar{a}$, $\bar{b}$, $\bar{c}$. Так как $\mathcal{E}$ замкнуто относительно комплексного сопряжения (см. первый абзац доказательства), то $z \in X$ — противоречие. □

Другими словами, чтобы кольцо $\mathcal{E}$ было евклидовым, необходимо и достаточно, чтобы открытые круги радиуса 1 с центрами в точках из $\mathcal{E}$ покрывали всю комплексную плоскость, для чего достаточно, чтобы три круга с центрами в точках 0, 1, α покрывали треугольник, образованный этими точками.

Из доказательства теоремы 1 (как и из леммы 2.3) следует, что обратимыми в $\mathcal{E}$ являются в точности все элементы нормы 1.

Бывает полезна следующая лемма.

Лемма 2.4. *Пусть $a \in \mathcal{E} \setminus \{0\}$. Тогда фактор-кольцо $\mathcal{E}/a\mathcal{E}$ конечно и имеет порядок $|a|^2$.*

Доказательство. Аддитивная группа кольца $\mathcal{E}$ является свободной абелевой группой ранга 2 с базисом $\{1, \alpha\}$. Пусть $a = m + n\alpha$, $m, n \in \mathbb{Z}$, и $\alpha^2 - p\alpha + q = 0$, $p = \alpha + \bar{\alpha} \in \mathbb{Z}$, $q = \alpha\bar{\alpha} \in \mathbb{Z}$. Умножение на a в кольце $\mathcal{E}$ задаётся в этом базисе матрицей

$$C = \begin{pmatrix} m & -qn \\ n & m + pn \end{pmatrix},$$

следовательно, $|\mathcal{E}/a\mathcal{E}| = |\det C| = |m^2 + pmn + qn^2| = |m + n\alpha|^2 = |a|^2$. □

2.5. Решётки в евклидовых пространствах

Будем рассматривать одновременно действительный и комплексный случаи. В действительном случае положим $\mathcal{E} = \mathbb{Z}$, в комплексном случае $\mathcal{E}$ — любое евклидово кольцо вида $\mathcal{E} = \mathbb{Z}[\alpha]$, где α — недействительное целое алгебраическое число степени 2. Обозначим через $\mathbb{K}$ любое из полей $\mathbb{R}$, $\mathbb{C}$.

Рассмотрим конечно порождённый $\mathcal{E}$-модуль $X \leqslant \mathbb{K}^n$. Так как он не имеет кручения, то он является свободным $\mathcal{E}$-модулем. Обозначим через (X, X) множество скалярных произведений пар векторов из X. Это множество содержит 0 и замкнуто относительно умножения на элементы $\mathcal{E}$, но может быть незамкнуто по сложению, как показывает пример $L = \langle (1, 0), (\pi, 1) \rangle \leqslant \mathbb{R}^2$: здесь $1, \pi^2 + 1 \in (L, L)$, но $\pi^2 + 2 \notin (L, L)$.

Определение 2.5. *Решёткой* в $\mathbb{K}^n$ называется конечно порождённый $\mathcal{E}$-модуль $X \leqslant \mathbb{K}^n$ со свойством $(X, X) = \sigma\mathcal{E}$ для некоторого $\sigma \in \mathbb{K}$, $\sigma \neq 0$.

Из условия $(X, X) = \sigma\mathcal{E}$ следует дискретность решётки. Действительно, в недискретном $\mathcal{E}$-модуле найдётся последовательность ненулевых элементов, стремящаяся к нулю. Тогда их скалярные квадраты тоже будут стремиться к нулю, что невозможно, поскольку множество $\sigma\mathcal{E} \subseteq \mathbb{K}$ дискретно. Можно показать, что дискретность конечно порождённого $\mathcal{E}$-модуля $X \leqslant \mathbb{K}^n$ эквивалентна существованию в X базиса над $\mathcal{E}$, линейно независимого над $\mathbb{K}$. Для решёток, изучаемых в данной работе, это свойство будет очевидно, поэтому доказательство этого факта можно опустить.

Определение 2.6. *Автоморфизмом* решётки X называется ортогональное (унитарное) преобразование пространства $\mathbb{K}^n$, сохраняющее X.

Лемма 2.5. *Пусть $X \leqslant \mathbb{K}^n$ — решётка ранга n. Тогда группа её автоморфизмов конечна.*

Доказательство. Пусть $x_1, \ldots, x_n$ — базис X над $\mathcal{E}$. Как отмечалось выше, он также является базисом пространства $\mathbb{K}^n$, следовательно, автоморфизм X однозначно определяется образами элементов $x_1, \ldots, x_n$. Но так как X дискретна, то для образа каждого x_i имеется только конечное число возможностей. □

При вычислении автоморфизмов решётки бывает полезно следующее наблюдение: если $X \leqslant \mathbb{K}^n$ — n-мерная решётка и ортогональное (унитарное) преобразование $g \in \mathrm{O}_n(\mathbb{R})$ ($g \in \mathrm{U}_n(\mathbb{C})$) удовлетворяет условию $gX \subseteq X$, то $gX = X$ и g является автоморфизмом. Действительно, в базисе решётки X преобразование g имеет матрицу с элементами из $\mathcal{E}$ и её определитель по модулю равен 1. Тогда он обратим в $\mathcal{E}$, следовательно, образ базиса будет базисом.

Определение 2.7. n-мерная решётка $X \leqslant \mathbb{K}^n$ называется *унимодулярной*, если из условий $u \in \mathbb{K}^n$, $(u, v) \in \sigma\mathcal{E}$ для всех $v \in X$ следует, что $u \in X$. Решётка X называется *чётной*, если $(v, v) \in 2\,\mathrm{Re}(\sigma\mathcal{E})$ для всех $v \in X$, где $\mathrm{Re}(\sigma\mathcal{E})$ обозначает множество действительных частей всех чисел в $\sigma\mathcal{E}$.

3. Двойное накрытие $\Omega_8^+(2)$

3.1. Построение и свойства решётки E_8

Определение 3.1. Обозначим через E_8 множество векторов $v = (x_1, \ldots, x_8) \in \in \mathbb{R}^8$, удовлетворяющих следующим условиям:

1) $x_i \in \mathbb{Z}$ для всех i;
2) $x_1 \equiv \ldots \equiv x_8 \pmod 2$;
3) $x_1 + \ldots + x_8 \equiv 0 \pmod 4$.

Очевидно, что E_8 — аддитивная подгруппа в $\mathbb{Z}^8$, и следовательно, свободная абелева группа. Так как она содержит векторы $4e_i$, $i = 1, \ldots, 8$, где e_i — базисные орты, то $\mathrm{rk}\, E_8 = 8$.

Все координаты каждого вектора в E_8 имеют одну чётность; вектор $v \in E_8$ назовём *чётным*, если все его координаты чётны, и *нечётным* в противном случае.

Обозначим через $(a^p\, b^q \ldots)$ любой вектор, у которого некоторые p координат равны a, некоторые q координат равны b и т. д. *Нормой* вектора $v \in E_8$ будем называть его скалярный квадрат $(v, v) \in \mathbb{Z}$ (без извлечения квадратного корня).

Лемма 3.1.

1. *E_8 содержит все векторы вида*
   - $\big((\pm 2)^2\, 0^6\big)$,
   - $\big((\pm 4)^1\, 0^7\big)$,
   - $\big((\pm 1)^8\big)$, *число минусов чётно.*
2. *E_8 порождается векторами* $(1, \ldots, 1)$, $(2^2\, 0^6)$.

Доказательство. Первое утверждение леммы проверяется непосредственно. Докажем второе утверждение.

Пусть $v \in E_8$. Если v нечётный, то, заменяя его на вектор $v - (1, \ldots, 1)$, можем считать, что он чётный. Теперь с помощью векторов $2e_i + 2e_j$ можно занулить все координаты, кроме первой. Из условия 3 определения 3.1 следует, что тогда $v = 4ke_1$, $k \in \mathbb{Z}$. Так как $4e_1 = (2e_1 + 2e_2) + (2e_1 + 2e_3) - (2e_2 + 2e_3)$, то лемма доказана. □

Лемма 3.2.

1. *Множество скалярных произведений векторов из E_8 совпадает с множеством $4\mathbb{Z}$.*
2. *Норма каждого вектора из E_8 делится на* 8.
3. *Если $u \in \mathbb{R}^8$ обладает тем свойством, что $(u, v) \in 4\mathbb{Z}$ для всех $v \in E_8$, то $u \in E_8$.*

Доказательство. Скалярные произведения любых двух порождающих векторов из пункта 2 леммы 3.1 делятся на 4, следовательно, это верно для любых двух векторов в E_8. Так как $(4, 0, \ldots, 0) \cdot (1, \ldots, 1) = 4$, то первое утверждение доказано.

Второе утверждение следует из первого утверждения и того факта, что скалярные квадраты порождающих векторов делятся на 8.

Докажем третье утверждение. Пусть $u = (x_1, \ldots, x_8)$. Так как $(u, 4e_i) = 4x_i \in 4\mathbb{Z}$ для всех i, то $u \in \mathbb{Z}^8$, а так как $(u, 2e_i + 2e_j) = 2x_i + 2x_j \in 4\mathbb{Z}$ для всех i, j, то $x_1 \equiv \ldots \equiv x_8 \pmod 2$. Наконец, $(u, (1, \ldots, 1)) = x_1 + \ldots + x_8 \in 4\mathbb{Z}$, следовательно, $u \in E_8$. □

Таким образом, E_8 является чётной унимодулярной решёткой. Оказывается, что она является единственной с точностью до изоморфизма чётной унимодулярной решёткой ранга 8 в $\mathbb{R}^8$.

Обозначим через E_8^i множество векторов в E_8 с нормой $8i$, $i \geqslant 0$.

Лемма 3.3. $|E_8^1| = 240$, $|E_8^2| = 2160 = 16 \cdot 135$.

Доказательство. Пусть $v \in E_8^1$. Тогда v имеет строение $\big((\pm 2)^2\, 0^6\big)$ или $\big((\pm 1)^8\big)$. Все векторы первого вида лежат в E_8, и их число — $C_8^2 \cdot 4 = 112$.

Если же $v = \big((\pm 1)^8\big)$, то из условия 3 определения 3.1 следует, что число минусов должно быть чётно. Число таких векторов — $2^7 = 128$. Таким образом, $|E_8^1| = 112 + 128 = 240$.

Пусть $v \in E_8^2$. Тогда v имеет строение $\big((\pm 4)^1 0^7\big)$, $\big((\pm 3)^1 (\pm 1)^7\big)$ или $\big((\pm 2)^4 0^4\big)$. В первом случае получаем 16 векторов. Во втором случае некоторый вектор $v \pm 4e_i$ имеет строение $\big((\pm 1)^8\big)$, которое было рассмотрено выше. Число таких векторов — $8 \cdot 2^7 = 1024 = 16 \cdot 64$. В третьем случае все векторы с таким строением принадлежат E_8 и их число — $C_8^4 \cdot 2^4 = 1120 = 16 \cdot 70$. Таким образом, $|E_8^2| = 16(1 + 64 + 70) = 16 \cdot 135 = 2160$. □

3.2. Фактор-решётка $E_8/2E_8$

Фактор-решётка $E_8/2E_8$ (рассматриваемая как аддитивная группа) является элементарной абелевой группой порядка 2^8. Очевидно, что каждый вектор из E_8 содержится в своём смежном классе по $2E_8$ вместе со своим противоположным. Изучим распределение векторов из E_8^1, E_8^2 по смежным классам E_8 по $2E_8$.

Лемма 3.4. *Векторы из E_8^1, E_8^2 не лежат в $2E_8$. Каждый ненулевой смежный класс E_8 по $2E_8$ содержит либо ровно два вектора из E_8^1 (отличающиеся знаком), либо восемь попарно ортогональных пар противоположных векторов из E_8^2.*

Доказательство. Для $w \in E_8$ имеем $(2w, 2w) = 4(w, w) \in 32\mathbb{Z}$, поэтому векторы из E_8^1, E_8^2 не лежат в $2E_8$. Пусть векторы $u, v \in E_8^1 \cup E_8^2$ лежат в одном смежном классе по $2E_8$ и при этом $u \neq \pm v$. Заменяя v на $-v$, можно считать, что $(u, v) \geqslant 0$. Так как $u - v = 2w$, $w \in E_8$ и $u \neq v$, то

$$(u - v, u - v) = (u, u) + (v, v) - 2(u, v) \leqslant 16 + 16 = 32,$$
$$(u - v, u - v) = 4(w, w) \geqslant 32,$$

следовательно, $u, v \in E_8^2$, $(u, v) = 0$. Так как число ненулевых попарно ортогональных векторов в $\mathbb{R}^8$ не может быть больше восьми, то векторы из $E_8^0 \cup E_8^1 \cup E_8^2$ занимают не менее

$$1 + \frac{|E_8^1|}{2} + \frac{|E_8^2|}{16} = 1 + 120 + 135 = 256$$

смежных классов. Отсюда следует, что это все смежные классы E_8 по $2E_8$ и в каждом смежном классе, содержащем векторы из E_8^2, содержится ровно восемь попарно ортогональных пар противоположных векторов из E_8^2. □

Фактор-решётка $E_8/2E_8$ может быть также рассмотрена как векторное пространство размерности 8 над полем $\mathbb{Z}_2$. Факторизацию подмножества $A \subseteq E_8$ по $2E_8$ будем обозначать чертой: $(A + 2E_8)/2E_8 = \bar{A}$. Обозначим $V = E_8/2E_8$ и введём на V билинейную и квадратичную формы следующим образом:

$$f\colon V\times V\to\mathbb{Z}_2,\quad f(\bar u,\bar v)=\frac{(u,v)}{4}\pmod 2,\quad u,v\in E_8,$$
$$Q\colon V\to\mathbb{Z}_2,\quad Q(\bar u)=\frac{(u,u)}{8}\pmod 2,\quad u\in E_8.$$

Эти определения корректны, поскольку для $x,y\in E_8$

$$\frac{(u+2x,v+2y)}{4}=\frac{(u,v)}{4}+2\cdot\frac{(u,y)}{4}+2\cdot\frac{(x,v)}{4}+4\cdot\frac{(x,y)}{4}\equiv\frac{(u,v)}{4}\pmod 2,$$
$$\frac{(u+2x,u+2x)}{8}=\frac{(u,u)}{8}+2\cdot\frac{(u,x)}{4}+4\cdot\frac{(x,x)}{8}\equiv\frac{(u,u)}{8}\pmod 2.$$

Из равенств

$$Q(\bar u+\bar v)=\frac{(u,u)+2(u,v)+(v,v)}{8}=Q(\bar u)+Q(\bar v)+f(\bar u,\bar v)$$

следует, что Q — квадратичная форма на V с ассоциированной билинейной формой f.

Лемма 3.5. *Форма f невырожденна, и Q имеет тип $+$.*

Доказательство. Невырожденность f означает, что если $f(\bar u,\bar v)=0$ для некоторого $\bar u\in V$ и всех $\bar v\in V$, то $\bar u=\bar 0$. Если $u\in E_8$ обладает таким свойством, то $(u,v)\in 8\mathbb{Z}$ для всех $v\in E_8$, следовательно, $(u/2,v)\in 4\mathbb{Z}$ для всех $v\in E_8$. По лемме 3.2 $u/2\in E_8$, $u\in 2E_8$, $\bar u=\bar 0$.

Знак невырожденной квадратичной формы на векторном пространстве размерности $2m$ над полем порядка $q=2^k$ определяется числом сингулярных векторов этой формы: оно вычисляется по формуле $q^{2m-1}\pm(q^m-q^{m-1})$, где знак совпадает со знаком этой формы. Сингулярные векторы для Q — это в точности $\{\bar 0\}\cup\bar E_8^2$, и их число $-1+135=136=2^7+2^4-2^3$. Следовательно, Q — квадратичная форма типа $+$. □

3.3. Автоморфизмы E_8

Пусть $G=\operatorname{Aut}E_8$ — группа автоморфизмов E_8. Для каждого $X\subseteq\Omega=\{1,\dots,8\}$ обозначим через ε_X преобразование $\mathbb{R}^8$, действующее по правилу

$$\varepsilon_X e_i=\begin{cases}e_i, & i\notin X,\\ -e_i, & i\in X.\end{cases}$$

Для каждого $\sigma\in S_8$ будем обозначать той же буквой σ преобразование $\mathbb{R}^8$, действующее по правилу $\sigma e_i=e_{\sigma(i)}$.

Лемма 3.6.

1. *Для каждого подмножества $X\subseteq\Omega$ чётного порядка преобразование ε_X лежит в G. Такие преобразования образуют элементарную абелеву подгруппу $2^7\leqslant G$.*
2. *Все преобразования из S_8 лежат в G.*

3. *Подгруппа S_8 нормализует подгруппу 2^7, и полупрямое произведение $N = 2^7 : S_8$ совпадает с подгруппой всех мономиальных автоморфизмов E_8.*
4. *N действует транзитивно на векторах из E_8^2 каждого из трёх типов из леммы* 3.3.

Доказательство. Преобразования ε_X, $|X|$ чётно, $\sigma \in S_8$ оставляют порождающие векторы решётки E_8 в E_8, и следовательно, являются автоморфизмами. Для $X \subseteq \Omega$, $\sigma \in S_8$ имеем

$$\sigma\varepsilon_X\sigma^{-1}e_i = \sigma\varepsilon_X e_{\sigma^{-1}(i)} = \\ = \begin{cases} \sigma e_{\sigma^{-1}(i)}, & \sigma^{-1}(i) \notin X, \\ -\sigma e_{\sigma^{-1}(i)}, & \sigma^{-1}(i) \in X \end{cases} = \begin{cases} e_i, & i \notin \sigma(X), \\ -e_i, & i \in \sigma(X) \end{cases} = \varepsilon_{\sigma(X)}e_i,$$

т. е. S_8 нормализует 2^7.

Пусть $d\sigma \in G$ — мономиальное преобразование, где $d = \operatorname{diag}(d_1, \ldots, d_8)$ — диагональная матрица, $\sigma \in S_8$. Так как $\sigma \in G$, то $d \in G \leqslant \mathrm{O}_8(\mathbb{R})$, следовательно, $d_i = \pm 1$ для всех i. Применяя d к вектору $(1, \ldots, 1) \in E_8$, получаем, что число минусов среди $d_1, \ldots, d_8$ должно быть чётным. Таким образом, $d\sigma \in N$.

Четвёртое утверждение проверяется непосредственно. □

Рассмотрим группу $A = 2^7$ диагональных преобразований как $\mathbb{Z}_2S_8$-модуль. Можно считать, что он отождествлён с группой подмножеств Ω чётного порядка относительно операции суммы подмножеств (т. е. симметрической разности). Модуль A содержит одномерный подмодуль $A_0 = \langle\Omega\rangle$. Изучим действие подгруппой $A_8 \leqslant S_8$ на A.

Лемма 3.7. *$\mathbb{Z}_2A_8$-фактор-модуль A/A_0 неприводим, и $[A, A_8] = A$, в частности, расширение $\mathbb{Z}_2A_8$-модулей $A_0 \leqslant A$ не расщепляется.*

Доказательство. A_8 имеет на A/A_0 орбиты порядков 1, $C_8^2 = 28$, $(1/2)C_8^4 = 35$. Так как 29 и 36 не являются степенями двойки, то фактор-модуль A/A_0 неприводим.

Каждое подмножество Ω порядка 2 есть сумма двух подмножеств порядка 2. Так как A_8 действует на таких подмножествах транзитивно и они порождают A (как аддитивную группу), то $[A, A_8] = A$. Если бы расширение $\mathbb{Z}_2A_8$-модулей $A_0 \leqslant A$ расщеплялось, то $[A, A_8]$ содержалось бы в дополняющем подмодуле, поскольку действие A_8 на A_0 тривиально. □

Рассмотрим матрицу

$$U = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 \end{pmatrix}.$$

Нетрудно видеть, что $U \in \mathrm{O}_8(\mathbb{R})$ и что U оставляет в E_8 порождающие векторы E_8, следовательно, $U \in G$.

Наконец, докажем основной результат данного раздела.

Теорема 2. *$G \cong 2 \,.\, \mathrm{O}_8^+(2)$, причём расширение $2 \,.\, \Omega_8^+(2)$ не расщепляется, т. е. группа $\Omega_8^+(2)$ допускает двойное накрытие.*

Доказательство. Группа G действует на пространстве V линейными преобразованиями, сохраняющими квадратичную форму Q, т. е. ортогональными преобразованиями из $\mathrm{O}_8^+(2)$. Пусть K — ядро этого действия. Так как K сохраняет смежный класс $\overline{4e_1}$, то $K \leqslant N$. Так как векторы $\pm(2e_i + 2e_j)$ являются единственными векторами из E_8^1 в своих смежных классах, то K оставляет на месте любое двухэлементное подмножество Ω, следовательно, $K \leqslant 2^7$. Наконец, если $g \in K$ меняет знак в одной координате и не меняет в другой, то соответствующий вектор $2e_i + 2e_j$ не остаётся в своём смежном классе, следовательно, $K = \{\pm E\}$.

Таким образом, $G/\{\pm E\}$ вкладывается в $\mathrm{O}_8^+(2)$. Найдём порядок группы G. Нетрудно видеть, что матрица U сливает между собой три N-орбиты на E_8^2 в одну, следовательно, G транзитивно действует на E_8^2 и, в частности, на $\bar{E}_8^2$. Стабилизатор смежного класса $\overline{4e_1}$ в G совпадает с подгруппой мономиальных автоморфизмов, т. е. с N, откуда следует, что $|G| = 135 \cdot |N| = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7 = 2 \cdot |\mathrm{O}_8^+(2)|$ и $G \cong 2 \,.\, \mathrm{O}_8^+(2)$.

Обозначим $N_0 = 2^7 : A_8 \leqslant N$. Из леммы 3.7 следует, что $N_0' \geqslant 2^7$, откуда $N_0' = N_0$, $N_0 \leqslant 2 \,.\, \Omega_8^+(2)$. Так как расширение $\mathbb{Z}_2 A_8$-модулей $A_0 \leqslant A$ не расщепляется, то и расширение $2 \,.\, \Omega_8^+(2)$ не расщепляется.

Теорема доказана. □

В действительности мультипликатор Шура группы $\Omega_8^+(2)$ изоморфен 2×2 [1]. Существование такого накрытия следует из того, что группы $\Omega_8^+(q)$ допускают исключительный внешний автоморфизм порядка 3, который в случае $q = 2$ не продолжается на построенное накрытие $2 \cdot \Omega_8^+(2)$, а следовательно, переставляет по циклу три инволюции в центральной подгруппе 2×2.

4. Тройное накрытие $\mathrm{U}_4(3)$

4.1. Гексакод и его свойства

Гексакод играет огромную роль в изучении многих спорадических простых групп и их накрытий, например, его можно использовать для построения группы Матье M_{24}. Построим этот код.

В группе S_6 централизатором транспозиции является подгруппа $S_4 \times 2$, где подгруппа S_4 может быть выбрана в подгруппе A_6. Так как S_6 допускает внешний автоморфизм, переводящий транспозиции в тройные транспозиции (произведения трёх независимых транспозиций), то то же верно и для тройных

транспозиций. Пусть

$$S = C_{A_6}\big((12)(34)(56)\big) = \langle (135)(246), (13)(24), (12)(34)\rangle \cong S_4.$$

Пусть также $\mathbb{F}$ — поле порядка 4, $\mathbb{F} = \{0, 1, \omega, \bar{\omega}\}$, $\omega^2 + \omega + 1 = 0$, и $V = \mathbb{F}^6$ — шестимерное пространство строк над $\mathbb{F}$. Группа S_6 естественным образом действует на множестве координат этого пространства.

Определение 4.1. *Гексакодом* называется S-подмодуль $\mathcal{H} \leqslant V$, порождённый вектором $(\omega, \bar{\omega}, \omega, \bar{\omega}, \omega, \bar{\omega})$.

Лемма 4.1.

1. *$\mathcal{H}$ порождается векторами*

$$(\omega, \bar{\omega}, \bar{\omega}, \omega, \bar{\omega}, \omega), \quad (\bar{\omega}, \omega, \bar{\omega}, \omega, \omega, \bar{\omega}), \quad (\bar{\omega}, \omega, \omega, \bar{\omega}, \bar{\omega}, \omega)$$

   как векторное пространство и является самодвойственным $[6, 3, 4]_4$-кодом. В частности, слово гексакода однозначно восстанавливается по произвольно заданным значениям произвольных трёх координат.
2. *$\operatorname{Aut}\mathcal{H} \cong 3\cdot A_6$, где центральная подгруппа порядка 3 действует скалярными преобразованиями $\omega^k E$, а группа A_6 действует на координатах естественным образом.*
3. *Подгруппа $3 \times S \leqslant \operatorname{Aut}\mathcal{H}$ имеет следующие пять орбит при действии на $\mathcal{H}$.*

Представитель орбиты	Длина орбиты
$(0, 0, 0, 0, 0, 0)$	1
$(1, 1, 1, 1, 0, 0)$	$3 \cdot 3 = 9$
$(0, 1, 0, 1, \omega, \bar{\omega})$	$12 \cdot 3 = 36$
$(\omega, \bar{\omega}, \omega, \bar{\omega}, \omega, \bar{\omega})$	$4 \cdot 3 = 12$
$(1, 1, \omega, \omega, \bar{\omega}, \bar{\omega})$	$2 \cdot 3 = 6$

Доказательство. Очевидно, что вектор из определения 4.1 вместе с векторами пункта 1 леммы образует S-орбиту, следовательно, эти четыре вектора порождают $\mathcal{H}$ как подпространство. Нетрудно проверить, что последние три линейно независимы и в сумме дают первый, следовательно, $\dim\mathcal{H} = 3$. Так как порождающие векторы $\mathcal{H}$ попарно ортогональны (относительно скалярного произведения $(x, y) = \sum\limits_{i=1}^{6} x_i\bar{y}_i$), то $\mathcal{H}$ самодвойственный.

Представители орбит в пункте 3 находятся небольшим перебором, и длины орбит вычисляются непосредственно. Так как сумма длин полученных орбит равна $64 = 4^3$, то найдены все векторы; отсюда видно, что минимальное расстояние кода $\mathcal{H}$ равно 4, т. е. $\mathcal{H}$ является $[6, 3, 4]_4$-кодом. Последнее утверждение пункта 1 следует из того, что значения трёх фиксированных координат можно задать $4^3 = 64$ способами и, так как в каждом случае найдётся не более одного такого слова в $\mathcal{H}$, на самом деле оно будет ровно одно.

Найдём группу автоморфизмов $\mathcal{H}$. Для начала пусть $D = \operatorname{diag}(d_1, \ldots, d_6)$ — диагональный автоморфизм $\mathcal{H}$. Так как $D(1, 1, 1, 1, 0, 0) = (d_1, d_2, d_3, d_4, 0, 0)$,

$D(0,0,1,1,1,1) = (0,0,d_3,d_4,d_5,d_6)$ и слово гексакода однозначно восстанавливается по трём координатам, то $d_1 = \ldots = d_6$, т. е. $D = \omega^k E$ — скалярное преобразование. Таким образом, группа $\operatorname{Aut}\mathcal{H}/\langle\omega E\rangle$, действуя на координатах, вкладывается в S_6. Нетрудно видеть, что преобразование

$$g\colon (x_1,x_2,x_3,x_4,x_5,x_6) \mapsto (x_3,x_1,x_2,x_4,\bar\omega x_5,\omega x_6)$$

является автоморфизмом $\mathcal{H}$ и индуцирует на координатах тройной цикл, не лежащий в подгруппе S. Так как подгруппа S в A_6 максимальна, то $\langle\omega E,S,g\rangle = 3\,.\,A_6$. С другой стороны, если $\operatorname{Aut}\mathcal{H} \cong 3\,.\,S_6$, то найдётся диагональное преобразование $D = (d_1,\ldots,d_6)$, которое в произведении с транспозицией (56) даст автоморфизм $\mathcal{H}$. Тогда векторы $(1,1,1,1,0,0)$, $(0,0,1,1,1,1)$ должны перейти в коллинеарные, следовательно, $D = \omega^k E$ и сама транспозиция (56) будет автоморфизмом. Но это неверно, так как вектор $(0,1,0,1,\bar\omega,\omega)$ не лежит в $\mathcal{H}$.

Осталось доказать, что расширение $3\,.\,A_6$ не расщепляется, для чего достаточно проверить, что нетривиальные скалярные преобразования являются коммутаторами. Если преобразование h действует по правилу

$$h\colon (x_1,x_2,x_3,x_4,x_5,x_6) \mapsto (\omega x_1,\bar\omega x_2,x_3,x_6,x_4,x_5),$$

то $h \in \operatorname{Aut}\mathcal{H}$ и $ghg^{-1}h^{-1} = \bar\omega E$ (преобразования применяются справа налево), что и утверждалось. □

Таким образом, построено тройное накрытие группы A_6.

4.2. Кольцо целых эйзенштейновых чисел

Далее в этом разделе используются следующие обозначения:

$$\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}, \quad \zeta = e^{\frac{2\pi i}{6}} = \frac{1}{2} + \frac{i\sqrt{3}}{2}, \quad \theta = i\sqrt{3},$$
$$\mathcal{E} = \{m + n\omega,\ m,n \in \mathbb{Z}\} = \mathbb{Z}[\omega].$$

Определение 4.2. *$\mathcal{E}$ — кольцо целых эйзенштейновых чисел.*

Нетрудно видеть, что каждый открытый круг в $\mathbb{C}$ содержит элемент из $\mathcal{E}$, поэтому кольцо $\mathcal{E}$ евклидово по теореме 1. Обратимыми в нём являются все числа нормы 1, т. е. ζ^k, $k = 0,1,\ldots,5$.

Приведём некоторые полезные соотношения:

$$\omega^2 = \bar\omega = -1-\omega, \quad \zeta = 1+\omega, \quad \omega = \zeta^2, \quad \theta = \omega - \bar\omega = 1 + 2\omega = -\frac{3}{\theta},$$
$$|m+n\omega|^2 = m^2 - mn + n^2, \quad \theta\zeta = \omega - 1.$$

Для $x,y,z \in \mathcal{E}$ будем писать $x \equiv y \pmod z$, если $(x-y)/z \in \mathcal{E}$. Число $m+n\omega \in \mathcal{E}$ делится на θ в $\mathcal{E}$ тогда и только тогда, когда $m+n$ делится на 3 (в $\mathbb{Z}$).

Найдём натуральные числа k, для которых в $\mathcal{E}$ существует число нормы k. Это условие на k эквивалентно представимости k в виде $k = m^2 - mn + n^2$, $m,n \in \mathbb{Z}$.

Теорема 3. *Простое число p представимо в виде $p = m^2 - mn + n^2$ тогда и только тогда, когда $p \equiv 1 \pmod 3$ или $p = 3$.*

Доказательство. Если $p = m^2 - mn + n^2$, то $p = (m + n\omega)(m + n\bar{\omega})$, и $|m+n\omega| = |m+n\bar{\omega}| > 1$, следовательно, p не простой элемент кольца $\mathcal{E}$. Обратно, если простое число p не является простым элементом кольца $\mathcal{E}$, то $p = ab$, где $a, b \in \mathcal{E}$ необратимы. Тогда $p^2 = |a|^2|b|^2$, причём $|a|^2, |b|^2 > 1$, следовательно, $|a|^2 = |b|^2 = p$. Так как $|a| = |b|$, $\arg a + \arg b = \arg p = 0$, то $a = \bar{b}$, т. е. $p = (m + n\omega)(m + n\bar{\omega}) = m^2 - mn + n^2$.

Итак, нужно доказать, что p является квадратом по модулю 3 тогда и только тогда, когда $p \in \mathcal{E}$ не является простым элементом. Если p не является простым элементом, то

$$p = m^2 - mn + n^2 \equiv m^2 + 2mn + n^2 = (m + n)^2 \pmod 3.$$

Обратно, пусть p является квадратом по модулю 3. Тогда $p \neq 2$, и можно считать, что $p \neq 3$, поскольку 3 не является простым элементом $\mathcal{E}$. Тогда по квадратичному закону взаимности

$$1 = \left(\frac{p}{3}\right) = (-1)^{(p-1)/2} \left(\frac{3}{p}\right) = \left(\frac{-3}{p}\right),$$

т. е. существует целое число k, не делящееся на p, с условием $k^2+3 \equiv 0 \pmod p$. Рассмотрим фактор-кольцо $R = \mathcal{E}/p\mathcal{E}$. Элементы k, $-k$ различны в этом фактор-кольце, поскольку $2k/p \notin \mathbb{Z}$, и являются в нём корнями многочлена $x^2 + 3$. Кроме того, элемент $\theta = i\sqrt{3}$ является корнем этого многочлена и отличен от $\pm k$ в R. Действительно, $(\pm k - \theta)/p \notin \mathcal{E}$, так как $\mathrm{Re}\big((\pm k - \theta)/p\big) = \pm\,(k/p)$ не является полуцелым. Таким образом, ненулевой многочлен второй степени имеет как минимум три различных корня в R, следовательно, R не является полем и p не является простым элементом кольца $\mathcal{E}$. □

Следствие 4.2. *Натуральное число k представимо в виде $k = m^2 - mn + n^2$, $m, n \in \mathbb{Z}$, тогда и только тогда, когда каждый простой делитель p числа k, не являющийся квадратом по модулю 3, входит в разложение k в чётной степени.*

Доказательство. Если числа $k, l \in \mathbb{N}$ представимы в таком виде, то $k = |a|^2$, $l = |b|^2$, $a, b \in \mathcal{E}$, и $kl = |ab|^2$, $ab \in \mathcal{E}$, т. е. kl также представимо в таком виде. Поскольку $p^2 = p^2 - p \cdot 0 + 0^2$, то импликация $\Leftarrow$ доказана.

Обратно, пусть $k = m^2 - mn + n^2$, $m, n \in \mathbb{Z}$, и p — некоторый простой делитель числа k, не являющийся квадратом по модулю 3. Если n не делится на p, то в поле $\mathbb{Z}_p$ получаем

$$0 = k = m^2 - mn + n^2 = n^2 \left(\left(\frac{m}{n}\right)^2 - \frac{m}{n} + 1\right),$$

следовательно, многочлен $f(x) = x^2 - x + 1$ имеет корень в $\mathbb{Z}_p$. Для $p = 2$ это неверно, а для $p \neq 2$ наличие корня квадратного трёхчлена в $\mathbb{Z}_p$ определяется

его дискриминантом — он равен $1-4=-3$. Но так как $p\neq 3$, то

$$\left(\frac{-3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)=-1,$$

следовательно, многочлен f не имеет корней в $\mathbb{Z}_p$.

Таким образом, n делится на p, и тогда m делится на p. Следовательно,

$$\frac{k}{p^2}=\left(\frac{m}{p}\right)^2-\frac{m}{p}\cdot\frac{n}{p}+\left(\frac{n}{p}\right)^2\in\mathbb{Z},$$

и число k/p^2 представимо в таком виде. Проводя для него те же рассуждения, получаем импликацию $\Rightarrow$. □

Для каждого $z\in\mathcal{E}$ числа $ze^{2\pi ik/6}=z\zeta^k$ по модулю равны z, следовательно, для каждого $n\in\mathbb{N}$ количество чисел в $\mathcal{E}$ с квадратом модуля n делится на 6. Для $n=1,3,4,9$ имеется по шесть чисел: ζ^k, $\theta\zeta^k$, $2\zeta^k$, $3\zeta^k$, а для $n=7$ имеется двенадцать чисел: $(2-\omega)\zeta^k$, $(3+\omega)\zeta^k$.

4.3. Решётка A и её свойства

Число $2\in\mathcal{E}$ имеет норму 4 и является простым элементом, следовательно, фактор-кольцо $\mathcal{E}/2\mathcal{E}$ изоморфно полю $\mathbb{F}$ порядка 4. Представители смежных классов по $2\mathcal{E}$ — это 0, 1, ω, $\bar{\omega}$. Таким образом, каждый вектор $(z_1,\dots,z_6)\in\mathcal{E}^6$, рассматриваемый по модулю 2, превращается в вектор из $\mathbb{F}^6$.

Определение 4.3. Обозначим через A множество векторов $v=(z_1,\dots,z_6)\in\in\mathcal{E}^6$, обладающих свойством $v \bmod 2\in\mathcal{H}$.

Таким образом,

$$A=\{(x_1+2a_1,\dots,x_6+2a_6),\ x_p\in\{0,1,\omega,\bar{\omega}\},\ (x_1,\dots,x_6)\in\mathcal{H},\ a_p\in\mathcal{E}\}.$$

Так как $A\leqslant\mathcal{E}^6$ и A содержит векторы $2e_p$, $p=1,\dots,6$, то A является свободным шестимерным $\mathcal{E}$-модулем.

Лемма 4.3. *A порождается как $\mathcal{E}$-модуль векторами $2e_p$, $p=1,\dots,6$, и базисными векторами кода $\mathcal{H}$:*

$$(1,1,1,1,0,0),\quad (0,1,0,1,\omega,\bar{\omega}),\quad (0,0,1,1,1,1).$$

Доказательство. Так как $v \bmod 2\in\mathcal{H}$, то v является линейной комбинацией с коэффициентами из $\mathcal{E}/2\mathcal{E}\cong\mathbb{F}$ трёх векторов, выписанных выше. Переходя к прообразам в кольце $\mathcal{E}$, получим разложение v в линейную комбинацию с коэффициентами из $\mathcal{E}$ этих трёх векторов и векторов $2e_p$. □

Нормой вектора $v\in A$ будем называть его скалярный квадрат $(v,v)\in\mathbb{Z}$ (без извлечения квадратного корня).

Лемма 4.4.

1. *Множество скалярных произведений векторов из A совпадает с идеалом $2\mathcal{E}$ кольца $\mathcal{E}$.*

2. *Множество вещественных частей этих скалярных произведений совпадает с множеством целых чисел* $\mathbb{Z}$.
3. *Норма каждого вектора из* A *является целым числом, делящимся на* 2.
4. *Если* $u \in \mathbb{C}^6$ *обладает свойством, что* $(u, v) \in 2\mathcal{E}$ *для всех* $v \in A$, *то* $u \in A$.

Доказательство. Скалярные произведения пар порождающих векторов A делятся на 2, причём существует пара векторов со скалярным произведением 2, откуда следует утверждение 1. Если $m + n\omega \in \mathcal{E}$ делится на 2, то m, n чётны и $\mathrm{Re}(m + n\omega) = m - n/2 \in \mathbb{Z}$. Так как $\mathrm{Re}(2 + 2\omega) = 1$, то второе утверждение доказано. Наконец, третье утверждение следует из второго утверждения и того факта, что норма каждого порождающего вектора делится на 2.

Докажем утверждение 4. Вычисляя скалярные произведения u с векторами $2e_p$, получаем, что все координаты u лежат в $\mathcal{E}$. Если $v \in \mathcal{H}$ — произвольный вектор, рассматриваемый как вектор из A, то $(u, v) \equiv 0 \pmod 2$ и, так как код $\mathcal{H}$ самодвойственный, $u \bmod 2 \in \mathcal{H}$. Это и означает, что $u \in A$. □

Таким образом, A является чётной унимодулярной решёткой в $\mathbb{C}^6$.

Теперь найдём векторы из A небольшой нормы. Обозначим через $(a^p\, b^q \ldots)$ любой вектор, у которого некоторые p координат равны a, некоторые q координат равны b и т. д. Через $[a^p\, b^q \ldots]$ обозначим любой вектор, у которого некоторые p координат имеют квадрат модуля a и т. д. Обозначим через A^n множество векторов нормы $n \in \mathbb{Z}$.

Лемма 4.5. $|A^2| = 0$, $|A^4| = 756 = 2^2 \cdot 3^3 \cdot 7$, $|A^6| = 4032 = 2^6 \cdot 3^2 \cdot 7$, $|A^8| = 20412 = 2^2 \cdot 3^6 \cdot 7$.

Доказательство. Для начала заметим, что норма числа $m + n\omega \in \mathcal{E}$ делится на 4 тогда и только тогда, когда m, n делятся на 2, т. е. когда $m + n\omega$ делится на 2. Действительно, импликация $\Leftarrow$ очевидна, а если $|m + n\omega|^2 = m^2 - mn + n^2$ делится на 4, то, как и в доказательстве следствия 4.2, получаем, что m, n делятся на 2. Отсюда следует, что в каждом векторе $v \in A$ число координат, нормы которых не делятся на 4, равно 0, 4 или 6.

Если $v \in A$, $(v, v) = 2$, то две координаты v имеют норму 1, а остальные равны нулю, что противоречит предыдущему абзацу. Пусть $v \in A$, $(v, v) = 4$. Тогда, с учётом предыдущего абзаца, v имеет строение $[4^1\, 0^5]$ или $[1^4\, 0^2]$. В первом случае получаем $6 \cdot 6 = 36$ векторов $2\zeta^k e_p$, во втором — $C_6^2 \cdot 3 \cdot 2^4 = 720$ векторов вида $\omega^k \cdot \big((\pm 1)^2 (\pm\omega)^1 (\pm\bar{\omega})^1\, 0^2\big)$ — итого $36 + 720 = 756$ векторов в A^4.

Пусть $v \in A$, $(v, v) = 6$. Тогда v имеет строение $[3^1\, 1^3\, 0^2]$ или $[1^6]$. Все числа нормы 3 в $\mathcal{E}$ — это $\pm\theta\omega^k$, $k = 0, 1, 2$, и так как $\theta = 1 + 2\omega \equiv 1 \pmod 2$, то числа нормы 3 разбиваются на три пары сравнимых по модулю 2 чисел. Следовательно, имеется $C_6^2 \cdot 3 \cdot 2^4 \cdot 4 = 2880$ векторов первого типа. Векторы второго типа совпадают с аналогичными векторами в $\mathcal{H}$ с точностью до изменения знаков координат, следовательно, их число — $18 \cdot 2^6 = 1152$. Итого $|A^6| = 2880 + 1152 = 4032$.

Пусть $v \in A$, $(v, v) = 8$. Тогда v имеет строение $[4^2\, 0^4]$, $[4^1\, 1^4\, 0^1]$, $[3^2\, 1^2\, 0^2]$, $[3^1\, 1^5]$. В первом случае имеем $C_6^2 \cdot 6^2 = 540$ векторов $2\zeta^k e_p + 2\zeta^m e_q$. В остальных

случаях получаем соответственно $C_6^2 \cdot 3 \cdot 2^4 \cdot 2 \cdot 6 = 8640$, $C_6^2 \cdot 3 \cdot 2^4 \cdot C_4^2 = 4320$, $18 \cdot 2^6 \cdot 6 = 6912$ векторов. Итого $|A^8| = 540 + 8640 + 4320 + 6912 = 20412$. $\square$

4.4. Автоморфизмы решётки A. Тройное накрытие $\mathrm{U}_4(3)$

Обозначим $G = \operatorname{Aut} A$. Автоморфизмы кода $\mathcal{H}$ естественным образом индуцируют автоморфизмы A. Кроме того, преобразования, произвольно меняющие знаки координат, также являются автоморфизмами A, причём подгруппа таких преобразований инвариантна при $\operatorname{Aut}\mathcal{H} \cong 3 \cdot A_6$, так что $2^6 : (3 \cdot A_6) \hookrightarrow G$. Обозначим эту подгруппу автоморфизмов через N.

Заметим, что матрица

$$U = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 1 & 1 & 0 & \bar{\omega} & \omega \\ 0 & 1 & \bar{\omega} & \omega & 1 & 0 \\ 0 & 1 & \omega & \bar{\omega} & 0 & 1 \end{pmatrix} \qquad (*)$$

является унитарной и сохраняет в A порождающие векторы A (действие матрицей на вектор осуществляется умножением вектор-строки слева на матрицу), следовательно, $U \in G$. Заметим также, что $U^2 = E$. Теперь исследуем действие G на A^8.

Лемма 4.6. *G действует на A^8 транзитивно.*

Доказательство. Для начала заметим, что для любых двух координат $p \neq q \in \Omega = \{1, \ldots, 6\}$ найдётся автоморфизм кода $\mathcal{H}$, оставляющий их на месте и умножающий их на любые заданные ненулевые числа из $\mathbb{F}$. Действительно, поскольку подгруппа $S \cong S_4 \leqslant \operatorname{Aut}\mathcal{H}$ действует на координатах Ω перестановками без умножения на ω^k и имеет две орбиты при действии на парах координат, то утверждение достаточно проверить для одной пары из каждой из этих орбит. Если h — преобразование из доказательства леммы 4.1, то преобразования $\omega^k h^{\pm 1}$ умножают каждую пару координат $\{1,2\}$, $\{2,3\}$ на произвольно заданные различные ненулевые числа, а скалярные преобразования умножают их на любое заданное ненулевое число.

Теперь докажем, что N действует транзитивно на каждом из четырёх типов векторов в A^8, описанных при доказательстве леммы 4.5. Транзитивность действия на векторах типа $[4^2\,0^4]$ следует из предыдущего абзаца и 2-транзитивности A_6 на Ω. Исследуем действие на векторах типа $[4^1\,1^4\,0^1]$. Применяя автоморфизм $\mathcal{H}$, а затем меняя знаки в координатах подходящим образом, можем привести вектор такого типа к виду $(a, b, 1, 1, 1, 1)$. Применяя автоморфизм $(12)(34)$, можем считать, что $b = 0$, и, изменяя знак первой координаты, можем считать, что $a \in \{1, \omega, \bar{\omega}\}$. Теперь, применяя автоморфизм $h^{\pm 1}$, получаем $a = 1$.

Исследуем действие на векторах типа $[3^2\,1^2\,0^2]$. Снова применяя автоморфизм $\mathcal{H}$ и меняя знаки в координатах, можно считать, что вектор имеет вид

$(0,0,a,b,c,d)$, где $a,b,c,d \in \{1,\theta\}$. Преобразования h, $(12)(34)$ индуцируют на $\{3,4,5,6\}$ всю группу S_4, действующую на этом множестве 2-транзитивно без умножения координат на числа. Следовательно, любой такой вектор можно привести к $(0,0,1,1,\theta,\theta)$.

Исследуем действие на векторах типа $[3^1\,1^5]$. Группа $\operatorname{Aut}\mathcal{H}$ действует транзитивно на векторах веса 6 в $\mathcal{H}$, следовательно, можно считать, что вектор получается из $(1,1,\omega,\omega,\bar{\omega},\bar{\omega})$ умножением одной из координат на θ. Применяя автоморфизмы $(12)(34)$, $(34)(56)$, можно считать, что θ находится в первой, третьей или пятой координате. Наконец, применяя автоморфизм $(135)(246)$ и умножая вектор на ω^k для подходящего k, получаем, что θ находится в первой координате.

Осталось заметить, что автоморфизм U, определённый выше, сливает между собой эти четыре N-орбиты — это проверяется непосредственными вычислениями. □

Рассмотрим фактор-решётку $A/2A$. Она имеет порядок $(2^2)^6 = 4096$ и может быть отождествлена с шестимерным векторным пространством V над полем $\mathcal{E}/2\mathcal{E} \cong \mathbb{F}$ порядка 4. Каждый вектор $v \in A$ содержится в своём смежном классе по $2A$ вместе со своим противоположным.

Лемма 4.7. *Каждый ненулевой смежный класс A по $2A$ содержит либо ровно два (противоположных) вектора из A^4, либо ровно два (противоположных) вектора из A^6, либо ровно двенадцать векторов из A^8, разбивающихся на шесть попарно ортогональных пар противоположных векторов.*

Доказательство. Пусть $u,v \in A^0 \cup A^4 \cup A^6 \cup A^8$, $u \neq \pm v$, $u-v \in 2A$. Заменяя v на $-v$, можно считать, что $\operatorname{Re}(u,v) \geqslant 0$. Тогда $u - v = 2w$, $w \in A$, и

$$(u-v,u-v) = (u,u) + (v,v) - 2\operatorname{Re}(u,v) \leqslant 16,$$
$$(u-v,u-v) = 4(w,w) \geqslant 4 \cdot 4 = 16,$$

так как $w \neq 0$. Отсюда получаем $u,v \in A^8$, $\operatorname{Re}(u,v) = 0$. Заметим, что векторы

$$\begin{gathered}(2,2,0,0,0,0),\\ (2,-2,0,0,0,0),\\ (0,0,2,2,0,0),\\ (0,0,2,-2,0,0),\\ (0,0,0,0,2,2),\\ (0,0,0,0,2,-2),\end{gathered} \qquad (**)$$

лежащие в A^8, лежат в одном смежном классе по $2A$ и попарно ортогональны. По доказанному если некоторый вектор $v = (a_1,\ldots,a_6) \in A^8$, отличный от них и их противоположных, лежит в том же смежном классе, то вещественная часть его скалярного произведения с каждым из них равна нулю. Отсюда следует, что все координаты v имеют нулевые вещественные части. Но из классификации A^8 следует, что таких векторов не существует, так как каждый вектор в A^8 имеет

координату нормы 1 или 4, а такие числа имеют ненулевую вещественную часть. Таким образом, выписанные векторы являются единственными векторами из A^8 в своём смежном классе. Из транзитивности G на A^8 следует, что то же верно для всех смежных классов, содержащих векторы из A^8: в них содержится ровно по шесть попарно ортогональных пар противоположных векторов из A^8.

Итак, векторы из $A^0 \cup A^4 \cup A^6 \cup A^8$ занимают ровно

$$1 + \frac{756}{2} + \frac{4032}{2} + \frac{20412}{12} = 4096$$

смежных классов, т. е. все смежные классы. □

Определим на $V = A/2A$ полуторалинейную форму $f\colon V \times V \to \mathbb{F}$ по формуле

$$f(\tilde{u}, \tilde{v}) = \frac{(u, v)}{2} \pmod 2,$$

где $\tilde{u} = u + 2A$, $\tilde{v} = v + 2A$. Это определение корректно: для $x, y \in A$ имеем

$$\frac{(u + 2x, v + 2y)}{2} = \frac{(u, v)}{2} + (u, y) + (x, v) + 2(x, y) \equiv \frac{(u, v)}{2} \pmod 2.$$

Так как комплексное сопряжение в $\mathcal{E}$ индуцирует нетривиальный автоморфизм поля $\mathcal{E}/2\mathcal{E}$, то нетрудно видеть, что форма действительно полуторалинейная (т. е. $f(\lambda u, v) = \lambda f(u, v)$, $f(u, \lambda v) = \bar{\lambda} f(u, v)$, $\lambda \in \mathbb{F}$) и сопряжённо-симметрическая ($f(v, u) = \overline{f(u, v)}$). Кроме того, она невырожденна: если вектор $u \in A$ таков, что $f(\tilde{u}, \tilde{v}) = 0$ для всех $v \in A$, то $(u, v) \in 4\mathcal{E}$, $(u/2, v) \in 2\mathcal{E}$ для всех $v \in A$. По лемме 4.4 $u/2 \in A$, $u \in 2A$, $\tilde{u} = 0$.

Группа G действует на V линейными преобразованиями, сохраняющими f, т. е. унитарными преобразованиями. Если K — ядро этого действия, то K оставляет на месте все пары векторов $\pm 2e_p$, $p = 1, \ldots, 6$, и следовательно, действует диагональными преобразованиями $\operatorname{diag}(\pm 1, \ldots, \pm 1)$. Если найдётся элемент $g \in K$, меняющий знак в координате p и не меняющий знак в координате q, то найдётся вектор $v \in A^4$ типа $[1^4\, 0^2]$, у которого координаты p, q ненулевые. Тогда вектор gv не совпадает с $\pm v$ и, следовательно, не лежит с v в одном смежном классе. Таким образом, $K = \langle -E \rangle$, и $G/\langle -E \rangle \hookrightarrow \mathrm{GU}_6(2)$. Скалярные преобразования $\omega^k E \in G$ действуют на V скалярными преобразованиями, поэтому $G/\langle \zeta E \rangle \hookrightarrow \mathrm{PGU}_6(2)$. Далее будет доказано, что на самом деле $G/\langle \zeta E \rangle \hookrightarrow \mathrm{PSU}_6(2) = \mathrm{U}_6(2)$.

Теорема 4. $|G| = 2^9 \cdot 3^7 \cdot 5 \cdot 7 = 6 \cdot |\mathrm{U}_4(3)| \cdot 2$.

Доказательство. Рассуждая как в доказательстве леммы 4.6, нетрудно показать, что G транзитивна на A^4. Пусть $G_1 = \mathrm{St}_G(2e_1)$, так что $|G| = 756 \cdot |G_1|$. Подгруппа G_1 действует транзитивно на множестве X векторов из A^4, ортогональных $2e_1$. Действительно, X состоит из векторов $2\zeta^k e_p$, $p = 2, \ldots, 6$, и векторов типа $[1^4\, 0^2]$ с нулевой первой координатой, так что $|X| = 6 \cdot 5 + 5 \cdot 3 \cdot 2^4 = 270$. Стабилизатор вектора $2e_1$ в $\operatorname{Aut} \mathcal{H}$, изоморфный A_5, действует на остальных

координатах транзитивно, причём, как было показано в первом абзаце доказательства леммы 4.6, найдётся автоморфизм из A_5, умножающий любую из координат $2,\dots,6$ на любое ненулевое число.

Пусть вектор v имеет тип $[1^4\,0^2]$ и нулевую первую координату. Композицией автоморфизма из $3\times A_5$, преобразования $h^{\pm1}$ из леммы 4.1 и замены знаков в координатах можно оставить на месте вектор $2e_1$ и перевести v в вектор $(0,0,1,1,1,1)$. Наконец, два типа векторов из X сливаются при действии автоморфизмом U, сохраняющим вектор $2e_1$.

Пусть $G_2=\mathrm{St}_{G_1}(2e_2)=\mathrm{St}_G(2e_1,2e_2)$, так что $|G|=756\cdot270\cdot|G_2|$. Тогда G_2 стабилизирует вектор $(2,2,0,0,0,0)$, а следовательно, переставляет между собой векторы $(**)$. Векторы $2e_p$, $p=3,4,5,6$, при действии G_2 должны переходить в векторы из A^4, ортогональные $2e_1$, $2e_2$, имеющие с векторами $(**)$ скалярные произведения 0, ±4. Множество Y таких векторов состоит из $\pm2e_p$, $p=3,4,5,6$, и векторов $(0,0,\pm1,\pm1,\pm1,\pm1)$, откуда получаем, что $|Y|=8+16=24$. Нетрудно видеть, что элементами из G_2 можно переставить между собой все векторы каждого из этих двух классов, а сами классы сливаются между собой при помощи преобразования

$$\frac12\begin{pmatrix}2&0&0&0&0&0\\0&2&0&0&0&0\\0&0&1&1&1&1\\0&0&1&1&-1&-1\\0&0&1&-1&1&-1\\0&0&1&-1&-1&1\end{pmatrix}\in G_2.$$

Пусть $G_3=\mathrm{St}_{G_2}(2e_3)=\mathrm{St}_G(2e_1,2e_2,2e_3)$, так что $|G|=756\cdot270\cdot24\cdot|G_3|$. При действии G_3 вектор $(0,0,2,2,0,0)$ должен перейти в вектор из $(**)$, имеющий с $2e_3$ скалярное произведение 4, т. е. в $(0,0,2,\pm2,0,0)$. Тогда $2e_4$ переходит в $\pm2e_4$, причём оба варианта возможны, так как преобразование, изменяющее знак в четвёртой координате, лежит в G_3. Пусть $G_4=\mathrm{St}_{G_3}(2e_4)$, $|G|=$ $=756\cdot270\cdot24\cdot2\cdot|G_4|$. При действии G_4 векторы $2e_5$, $2e_6$ переходят в векторы из Y, имеющие нулевые первые четыре координаты, т. е. в $\pm2e_5$, $\pm2e_6$. При этом $2e_5$ не может перейти в $\pm2e_6$, иначе такое преобразование с точностью до изменения знаков в координатах будет представлять собой перестановку последних двух координат, а такое преобразование не является автоморфизмом A. С другой стороны, изменение знаков в последних двух координатах даёт возможность независимо перевести $2e_5$ в $\pm2e_5$ и $2e_6$ в $\pm2e_6$.

Итак, $|G|=756\cdot270\cdot24\cdot2\cdot2\cdot2=39\,191\,040=2^9\cdot3^7\cdot5\cdot7$. □

Чтобы найти изоморфный тип группы G, рассмотрим фактор-решётку $A/\theta A$, $\theta=1+2\omega=i\sqrt3$. Она имеет порядок $3^6=729$ и может быть рассмотрена как шестимерное векторное пространство W над полем $\mathcal{E}/\theta\mathcal{E}\cong\mathbb{Z}_3$ порядка 3. Определим на нём билинейную форму $t\colon W\times W\to\mathbb{Z}_3$ по правилу $t(\hat u,\hat v)=(u,v)\bmod\theta$, где $\hat u=u+\theta A$, $\hat v=v+\theta A$. Это определение корректно: для $x,y\in A$ имеем

$$(u+\theta x,v+\theta y)=(u,v)+\theta(x,y)+\bar\theta(u,y)+3(x,y)\equiv(u,v)\ (\mathrm{mod}\ \theta),$$

поскольку $\bar{\theta} = -\theta$. Так как $\lambda \equiv \bar{\lambda} \pmod{\theta}$ для любого $\lambda \in \mathcal{E}$, то форма t действительно билинейная и симметрическая. Векторы $\widehat{2e_p}$, $p = 1, \ldots, 6$, образуют базис W, поскольку матрица Грама формы t на этих векторах является единичной матрицей. В частности, форма t невырожденна.

Знак невырожденной симметрической билинейной формы на $2m$-мерном пространстве над полем нечётного порядка q определяется по формуле $\varepsilon^m\delta$, где $\varepsilon, \delta = \pm 1$, $q \equiv \varepsilon \pmod{4}$, и $\delta = 1$ тогда и только тогда, когда форма допускает ортонормированный базис. В нашем случае знак формы t равен $(-1)^3 \cdot 1 = -1$.

Заметим, что так как $\omega \equiv 1 \pmod{\theta}$, то для каждого вектора $v \in A$ векторы v, ωv, $\bar{\omega} v$ лежат в одном смежном классе по θA. Пусть $u, v \in A^4$, $u \neq \omega^k v$, $u - v \in \theta A$. Заменим вектор v на $\omega^k v$ так, чтобы $\operatorname{Re}(u, v) \geqslant 0$. Тогда $u - v = \theta w \neq 0$ и

$$12 \leqslant (\theta w, \theta w) = (u - v, u - v) = (u, u) + (v, v) - 2\operatorname{Re}(u, v) \leqslant 4 + 4 = 8 -$$

противоречие. Следовательно, векторы из A^4 разбиваются ровно по три коллинеарных вектора в каждом смежном классе A по θA.

Теперь найдём ядро M действия G на W. Из предыдущего абзаца следует, что M действует диагональными преобразованиями $\operatorname{diag}(\omega^{k_1}, \ldots, \omega^{k_6})$. Как и при изучении автоморфизмов гексакода, применив такое преобразование к векторам $(1,1,1,1,0,0) \in A$, $(0,0,1,1,1,1) \in A$, получим $k_1 = \ldots = k_6$, $M = \langle \omega E \rangle$. Таким образом, $G/\langle \omega E \rangle \hookrightarrow \mathrm{O}_6^-(3)$. Так как $|G/\langle \omega E \rangle| = 2^9 \cdot 3^6 \cdot 5 \cdot 7$, $|\mathrm{O}_6^-(3)| = 2^{10} \cdot 3^6 \cdot 5 \cdot 7$, то $G \cong 3 \,.\, \Omega_6^-(3) \,.\, 2$. Как известно, расширение $\Omega_6^-(3) = 2 \,.\, \mathrm{P}\Omega_6^-(3)$ не расщепляется и $\mathrm{P}\Omega_6^-(3) \cong \mathrm{U}_4(3)$. Так как расширение $3 \,.\, A_6 \leqslant G$ также не расщепляется и преобразование $-E \in G$ индуцирует то же преобразование на W, то окончательно получаем

$$G \cong 6 \cdot \mathrm{P}\Omega_6^-(3) \,.\, 2 \cong 6 \cdot \mathrm{U}_4(3) \,.\, 2.$$

Расширение $G/\langle \omega E \rangle \cong \Omega_6^-(3) \,.\, 2$ не совпадает с $\mathrm{SO}_6^-(3)$, поскольку оно содержит отражения относительно базисных векторов, имеющие определитель -1.

В качестве побочного результата теперь можно получить включение $\mathrm{U}_4(3) \,.\, 2 \hookrightarrow \mathrm{U}_6(2)$. Действительно, ранее было доказано, что $G/\langle \zeta E \rangle \cong \cong \mathrm{U}_4(3) \,.\, 2 \hookrightarrow \mathrm{PGU}_6(2)$. Так как группа $\mathrm{U}_4(3)$ проста и $|\mathrm{PGU}_6(2)/\mathrm{U}_6(2)| = 3$, то $\mathrm{U}_4(3) \,.\, 2 \hookrightarrow \mathrm{U}_6(2)$.

Стоит отметить, что группа $\mathrm{U}_4(3)$ допускает накрытие $3^2 \cdot \mathrm{U}_4(3)$. Это следует из того, что $\mathrm{U}_4(3)$ допускает автоморфизм, не продолжающийся на построенное накрытие $3 \cdot \mathrm{U}_4(3)$. Мультипликатор Шура группы $\mathrm{U}_4(3)$ изоморфен 4×3^2 [1], где четверное накрытие — это естественное накрытие $4 \cdot \mathrm{U}_4(3) = \mathrm{SU}_4(3)$. Также отметим, что в группе $\mathrm{U}_4(3)$ содержится подгруппа $\mathrm{L}_3(4)$, следовательно, естественное накрытие $4 \cdot \mathrm{U}_4(3)$ даёт исключительное накрытие $4 \cdot \mathrm{L}_3(4)$.

4.5. Тройное накрытие A_7

Обозначим через H подгруппу в G, порождённую подгруппой $3 \cdot A_6 \leqslant N$ и матрицей U $(*)$. Орбита Z вектора $u = (0,0,1,1,1,1)$ при действии подгруппой

$3 \cdot A_6$ состоит из всех векторов веса 4 нормы 4 с координатами 0, 1, ω, $\bar{\omega}$. Они разбиваются на пятнадцать троек коллинеарных векторов. Отождествим эти векторы с теми же векторами в $\mathcal{H}$. Множество прямых, порождённых векторами из Z, обозначим через $\hat{Z}$. Добавив к Z векторы $2\omega^k e_p$, $p = 1, \ldots, 6$, $k = 0, 1, 2$, получим множество L, и множество прямых, порождённых векторами из L, обозначим через $\hat{L}$. Таким образом, $|\hat{Z}| = 15$, $|\hat{L}| = 21$.

Через $\operatorname{supp} v$ будем обозначать носитель вектора v.

Лемма 4.8. *Скалярное произведение любых двух векторов из Z принадлежит множеству $\{0, 2\omega^k, 4\omega^k\}$.*

Доказательство. Так как $3 \cdot A_6$ действует на Z транзитивно, то утверждение достаточно проверить для вектора u и любого вектора $v \in Z$. Если v имеет нули в паре координат $\{1, 2\}$, $\{3, 4\}$ или $\{5, 6\}$, то остальные четыре координаты равны, и утверждение очевидно. Если $|\operatorname{supp} u \cap \operatorname{supp} v| = 3$, то на пересечении этих носителей v имеет три различные координаты, следовательно, $(u, v) = 1 + \omega + \bar{\omega} = 0$. Если же один из нулей v находится в координате 3 или 4, а второй — в координате 5 или 6, то значения координат в $\operatorname{supp} u \cap \operatorname{supp} v$ совпадают, и лемма доказана. □

Лемма 4.9. *Множество прямых $\hat{L}$ инвариантно при действии H.*

Доказательство. Очевидно, что $\hat{L}$ инвариантно при действии $3 \cdot A_6$, так что нужно проверить его инвариантность при действии матрицей U. Так как строки матрицы $2U$ являются векторами из L, то прямые $\langle 2e_p \rangle$ при действии U переходят в прямые из $\hat{L}$. Заметим, что $U^T = \bar{U}$, следовательно, для $v \in Z$ координаты вектора vU равны половинам скалярных произведений v со строками матрицы $2U$ и по лемме 4.8 они лежат в $\{0, \omega^k, 2\omega^k\}$. Так как vU — вектор нормы 4 в A, то $vU \in L$. □

Таким образом, H действует транзитивно на множестве $\hat{L}$ из 21 прямой.

Лемма 4.10. *Каждая прямая из $\hat{L}$ ортогональна ровно десяти прямым в $\hat{L}$ и ровно двумя способами дополняется до шестёрки попарно ортогональных прямых.*

Доказательство. В силу транзитивности H на $\hat{L}$ утверждение достаточно проверить для прямой $l = \langle 2e_1 \rangle$. Она ортогональна пяти прямым $\langle 2e_p \rangle$, $p = 2, \ldots, 6$, и пяти прямым в $\hat{Z}$ с нулевой первой координатой (последние пять прямых порождаются последними пятью строками матрицы $2U$). Так как подгруппа $3 \times A_5$, стабилизирующая прямую l, действует транзитивно на каждой из этих пятёрок, а матрица U стабилизирует l и переставляет их между собой, то $\mathrm{St}_H(l)$ действует транзитивно на десяти прямых, ортогональных l. Теперь достаточно доказать, что прямые $\langle 2e_1 \rangle$, $\langle 2e_2 \rangle$ единственным образом дополняются до шестёрки попарно ортогональных прямых. Но существует всего пять прямых, ортогональных им обеим — $\langle 2e_3 \rangle, \ldots, \langle 2e_6 \rangle$ и $\langle u \rangle$, причём последняя не ортогональна остальным, т. е. тройка $\langle 2e_1 \rangle$, $\langle 2e_2 \rangle$, $\langle u \rangle$ не дополняется до такой шестёрки, откуда и следует утверждение леммы. □

Из леммы 4.10 следует, что на множестве $\hat{L}$ имеется ровно $(21 \cdot 2)/6 = 7$ шестёрок попарно ортогональных прямых. Так как каждая прямая в $\hat{L}$ является пересечением некоторых двух шестёрок, то ядро действия H на множестве таких шестёрок действует тривиально на $\hat{L}$ и, следовательно, состоит из диагональных матриц $\operatorname{diag}(\omega^{k_1}, \dots, \omega^{k_6})$. Как было доказано (с. 182), такое преобразование является скалярным, следовательно, $H/\langle \omega E \rangle \hookrightarrow S_7$. Ясно, что подгруппа $A_6 \leqslant H/\langle \omega E \rangle$ при этом вложении попадает в подгруппу A_7, и нетрудно проверить, что матрица U индуцирует на множестве шестёрок чётную перестановку, следовательно, $H/\langle \omega E \rangle \hookrightarrow A_7$. Наконец, подгруппа A_6 в A_7 максимальна, поэтому $H \cong 3 \cdot A_7$ (расширение не расщепляется, поскольку не расщепляется расширение $3 \cdot A_6$).

Мультипликатор Шура групп A_n, $n \geqslant 5$, $n \neq 6, 7$, имеет порядок 2, а при $n = 6, 7$ он циклический порядка 6 [1]. Двойные накрытия групп A_n могут быть построены, например, путём их вложения в ортогональные группы $\Omega_n(q)$ и дальнейшего расширения до спинорных групп $2 \cdot \Omega_n(q)$.

Тройное накрытие A_6 можно построить ещё несколькими способами. Например, A_6 вкладывается в $\mathrm{L}_3(4)$ и в группе $\mathrm{SL}_3(4) = 3 \cdot \mathrm{L}_3(4)$ расширяется до накрытия $3 \cdot A_6$. Кроме того, группа $3 \cdot A_6$ вкладывается в группу Матье M_{24} в качестве централизатора элемента порядка 3 с неподвижными точками (нормализатором этой подгруппы порядка 3 является расширение $3 \cdot S_6$, не являющееся центральным).

5. Четверное накрытие M_{22}

В данном разделе будет построена группа $4 \cdot M_{22}$. Группа M_{22} — третья по величине из пяти спорадических простых групп Матье; она имеет порядок $|M_{22}| = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443\,520$.

5.1. Система Штейнера $S(3, 4, 10)$

Напомним некоторые факты о группе S_6 и её автоморфизмах. Для краткости произведения трёх независимых транспозиций далее называются тройными транспозициями.

Предложение 5.1. *Группа S_6 содержит десять S_3-подгрупп, изоморфных $\mathbb{Z}_3 \times \mathbb{Z}_3$. Каждая из них порождается двумя независимыми тройными циклами и состоит из четырёх тройных циклов, четырёх произведений пар независимых тройных циклов и единицы.*

Группа автоморфизмов группы S_6 имеет порядок $6! \cdot 2$ и содержит S_6 в качестве подгруппы индекса 2. Внешние автоморфизмы S_6 переставляют классы сопряжённости транспозиций и тройных транспозиций, а также классы сопряжённости тройных циклов и произведений пар независимых тройных циклов. Классы сопряжённости транспозиций и тройных транспозиций имеют порядок 15.

S_3-подгруппы S_6 можно отождествить с разбиениями множества $X = \{1,2,3,4,5,6\}$ на две тройки. Транспозиция нормализует S_3-подгруппу тогда и только тогда, когда она содержится в одной из троек. Тройная транспозиция нормализует S_3-подгруппу тогда и только тогда, когда каждая из трёх транспозиций содержит по одному элементу из каждой тройки. Отсюда следует, что каждая нечётная инволюция в S_6 нормализует ровно четыре S_3-подгруппы.

Пусть $\Omega = \mathrm{Syl}_3(S_6)$, $|\Omega| = 10$. Назовём блоками четвёрки подгрупп из Ω, нормализуемые нечётными инволюциями в S_6, и множество блоков обозначим через $\mathcal{B}$. Докажем, что $(\Omega, \mathcal{B})$ — система Штейнера $S(3,4,10)$. Предположим, что для данных трёх подгрупп нет транспозиции, нормализующей каждую из них. Ясно, что для двух подгрупп найдутся сразу две такие транспозиции: для подгрупп $\langle (ijk), (lmn)\rangle$, $\langle (ijn), (lmk)\rangle$ этими транспозициями будут (ij), (lm). По предположению третья из выбранных подгрупп имеет вид $\langle (im\cdot), (lj\cdot)\rangle$. Тогда все три подгруппы нормализуются инволюцией $(il)(jm)(kn)$. Поскольку число нечётных инволюций равно $30 = C_{10}^3/C_4^3$, то утверждение доказано. Более того, доказано, что имеется взаимно-однозначное соответствие между блоками в $\mathcal{B}$ и нечётными инволюциями в S_6.

Ясно, что введённая структура на множестве Ω сохраняется при автоморфизмах группы S_6. Если автоморфизм S_6 оставляет на месте все S_3-подгруппы S_6, то он оставляет на месте и все нечётные инволюции, а следовательно, является тождественным. Таким образом, $\mathrm{Aut}\, S_6$ вкладывается в группу автоморфизмов системы $(\Omega, \mathcal{B})$. Можно доказать, что все системы Штейнера $S(3,4,10)$ изоморфны и их группа автоморфизмов имеет порядок $6! \cdot 2$, следовательно, она совпадает с $\mathrm{Aut}\, S_6$.

Рассмотрим действие группы $\mathrm{P\Gamma L}_2(9) = \mathrm{PGL}_2(9) : \mathrm{Aut}\, \mathbb{F}_9$ на проективной прямой $L = \mathbb{F}_9 \cup \{\infty\}$, где $\mathbb{F}_9$ — поле порядка 9. Нетрудно показать, что орбита подмножества $\{\infty, 0, 1, 2\} \subset L$ при действии этой группой состоит из тридцати подмножеств и задаёт на L структуру системы Штейнера $S(3,4,10)$. Поскольку все такие системы изоморфны, то $\mathrm{P\Gamma L}_2(9) \cong \mathrm{Aut}(\Omega, \mathcal{B}) \cong \mathrm{Aut}\, S_6$, откуда также следует изоморфизм $\mathrm{L}_2(9) \cong A_6$.

Следует отметить, что группа M_{22} является подгруппой чётных перестановок в полной группе автоморфизмов (единственной) системы Штейнера $S(3,6,22)$.

Множество блоков $\mathcal{B}$ разобьём на два класса $\mathcal{B}_1$, $\mathcal{B}_2$, состоящие из четвёрок S_3-подгрупп, нормализуемых соответственно транспозициями и тройными транспозициями. Каждый из этих классов имеет порядок 15. Они инвариантны при сопряжении элементами S_6 и переставляются при внешнем автоморфизме S_6. Группа S_6 действует на каждом классе транзитивно, и так как $|S_6/A_6| = 2$, то и A_6 действует на них транзитивно. Следовательно, при построении системы $S(3,4,10)$ через проективную прямую L классы блоков можно определить как $\mathrm{L}_2(9)$-орбиты на множестве всех блоков. Так как подгруппы $\mathrm{PGL}_2(9)$ и S_6 в $\mathrm{Aut}\, S_6$ не совпадают, то $\mathrm{PGL}_2(9)$ действует на тридцати блоках транзитивно.

Следующее утверждение проверяется непосредственно (пункты, связанные только с классом $\mathcal{B}_2$, можно проверить для $\mathcal{B}_1$ и применить внешний автоморфизм S_6).

Лемма 5.2.

1. *Любые два блока из одного класса пересекаются по одной или двум точкам.*
2. *Любые два блока из разных классов пересекаются по нулю или двум точкам.*
3. *Если* $A, B \in \mathcal{B}_i$, $|A \cap B| = 2$, *то* $A + B \in \mathcal{B}_i$.
4. *Если* $A, B \in \mathcal{B}_i$, $|A \cap B| = 1$, *то* $A + B + \Omega \in \mathcal{B}_i$.

5.2. Коды $\mathcal{C}_{10}$ и $\mathcal{C}_{10}^*$

Для построения группы $4 \cdot M_{22}$ используется некоторый $[10, 5, 4]_2$-код и двойственный к нему. Займёмся его построением.

Отождествим элементы множества $\Omega = \mathrm{Syl}_3(S_6)$ с координатами десятимерного пространства строк $\mathbb{F}^{10}$, где $\mathbb{F} = \mathbb{F}_2$ — поле порядка 2. При этом подмножества Ω соответствуют двоичным наборам в $\mathbb{F}^{10}$, а сумма двоичных наборов соответствует сумме (симметрической разности) подмножеств.

Обозначим через $\mathcal{C}_{10}$, $\mathcal{C}_{10}^*$ подпространства в $\mathbb{F}^{10}$, порождённые всеми блоками из $\mathcal{B}_1$, $\mathcal{B}_2$ соответственно. Так как внешний автоморфизм S_6 действует на координатах и переставляет классы $\mathcal{B}_1$, $\mathcal{B}_2$, то он переставляет подпространства $\mathcal{C}_{10}$, $\mathcal{C}_{10}^*$, следовательно, $\mathcal{C}_{10}$, $\mathcal{C}_{10}^*$ изоморфны как коды. По второму пункту леммы 5.2 каждый блок из $\mathcal{B}_1$ ортогонален каждому блоку из $\mathcal{B}_2$ относительно стандартного скалярного произведения в $\mathbb{F}^{10}$, следовательно, $\mathcal{C}_{10}^* \leqslant \mathcal{C}_{10}^{\perp}$, $\dim \mathcal{C}_{10} = \dim \mathcal{C}_{10}^* \leqslant 10 - \dim \mathcal{C}_{10}$, $\dim \mathcal{C}_{10} \leqslant 5$. С другой стороны, по четвёртому пункту леммы 5.2 код $\mathcal{C}_{10}$ содержит нулевое слово, пятнадцать слов веса 4, пятнадцать слов веса 6 и слово $(1, \ldots, 1)$ веса 10 — итого тридцать два кодовых слова. Следовательно, $\dim \mathcal{C}_{10} = \dim \mathcal{C}_{10}^* = 5$, код $\mathcal{C}_{10}^*$ является двойственным для $\mathcal{C}_{10}$ и код $\mathcal{C}_{10}$ не содержит других слов, кроме перечисленных выше. Таким образом, коды $\mathcal{C}_{10}$, $\mathcal{C}_{10}^*$ являются двойственными $[10, 5, 4]_2$-кодами с весовым распределением $0^1\, 4^{15}\, 6^{15}\, 10^1$. Заметим, что отсюда также следует третий пункт леммы 5.2.

Лемма 5.3. *Группа автоморфизмов кода* $\mathcal{C}_{10}$ *изоморфна* S_6.

Доказательство. Автоморфизм φ кода $\mathcal{C}_{10}$ представляет собой перестановку множества Ω, сохраняющую $\mathcal{C}_{10}$. Так как любая перестановка на Ω сохраняет стандартное скалярное произведение, то φ сохраняет и код $\mathcal{C}_{10}^*$. Так как все кодовые слова веса 4 этих кодов являются блоками из $\mathcal{B}$, то φ является автоморфизмом системы Штейнера $(\Omega, \mathcal{B})$, а в группе $\mathrm{Aut}(\Omega, \mathcal{B}) \cong \mathrm{Aut}\, S_6$ стабилизатором класса $\mathcal{B}_1$ является подгруппа S_6. □

Лемма 5.4. A_6 *действует неприводимо на* $\mathcal{C}_{10}/\langle\Omega\rangle$, *и* $[A_6, \mathcal{C}_{10}] = \mathcal{C}_{10}$, *в частности, расширение* $\mathbb{F}_2\, A_6$*-модулей* $\langle\Omega\rangle \leqslant \mathcal{C}_{10}$ *не расщепляется.*

Доказательство. A_6 транзитивно действует на ненулевых векторах фактор-пространства $\mathcal{C}_{10}/\langle\Omega\rangle$, следовательно, это действие неприводимо. Каждое множество порядка 6 в $\mathcal{C}_{10}$ является суммой двух блоков из $\mathcal{B}_1$, каждый из которых является образом другого при действии элементом из A_6. Следовательно, все множества порядка 6 в $\mathcal{C}_{10}$ лежат в $[A_6, \mathcal{C}_{10}]$, и так как они порождают $\mathcal{C}_{10}$, то $[A_6, \mathcal{C}_{10}] = \mathcal{C}_{10}$. Наконец, если бы расширение $\mathbb{F}_2 A_6$-модулей $\langle\Omega\rangle \leqslant \mathcal{C}_{10}$ расщеплялось, то $[A_6, \mathcal{C}_{10}]$ содержалось бы в инвариантном дополнении для $\langle\Omega\rangle$, поскольку действие на $\langle\Omega\rangle$ тривиально. □

Все те же утверждения, разумеется, верны и для S_6.

5.3. Сильно регулярный граф $\mathrm{srg}(77, 16, 0, 4)$

Система Штейнера $S = S(3, 6, 22)$, группой автоморфизмов которой является группа $M_{22} : 2$, приводит к конструкции сильно регулярного графа $\mathrm{srg}(77, 16, 0, 4)$. А именно, в качестве V возьмём множество из 77 блоков системы S. Два блока этой системы пересекаются по нулю или двум точкам. Назовём два блока соседними, если они не пересекаются. Нетрудно проверить, что такой граф удовлетворяет всем условиям определения 2.3. С другой стороны, имеет место следующая теорема [2].

Теорема 5. *Все графы* $\mathrm{srg}(77, 16, 0, 4)$ *изоморфны, и их группа автоморфизмов изоморфна* $M_{22} : 2 \cong \mathrm{Aut}\, S(3, 6, 22)$.

5.4. Евклидово кольцо $\mathbb{Z}[\zeta]$

Для построения накрытия $4 \cdot M_{22}$ используется кольцо $\mathcal{E} = \mathbb{Z}[\zeta]$, где $\zeta = (-1 + i\sqrt{7})/2$ (всюду далее в этом разделе ζ обозначает именно это число). Выпишем основные соотношения на ζ:

$$\zeta + \bar{\zeta} = -1, \quad \bar{\zeta} = -1 - \zeta, \quad |\zeta|^2 = \zeta\bar{\zeta} = 2, \quad \zeta^2 + \zeta + 2 = 0, \quad \zeta^2 = -2 - \zeta.$$

Нетрудно видеть, что для кольца $\mathcal{E}$ выполнено условие теоремы 1, следовательно, оно евклидово. Если $a = m + n\zeta \in \mathcal{E}$, $n \neq 0$, то $|a| \geqslant |\operatorname{Im} a| = |(n\sqrt{7})/2| > 1$, следовательно, обратимыми в $\mathcal{E}$ являются только числа $a = \pm 1$. Положим $\lambda = 1 + 2\zeta = i\sqrt{7} \in \mathcal{E}$. Так как $|\zeta|^2 = 2$ и $|\lambda|^2 = 7$ — простые числа, то ζ, $\bar{\zeta}$, λ, $\bar{\lambda}$ — простые элементы кольца $\mathcal{E}$. Так как ζ, $\bar{\zeta}$ не ассоциированы, то они взаимно просты. В частности, разложение числа 2 на простые множители имеет вид $2 = \zeta\bar{\zeta}$.

Выясним, какие натуральные числа могут быть нормами элементов из $\mathcal{E}$. Для $m + n\zeta \in \mathcal{E}$ имеем $|m + n\zeta|^2 = m^2 - mn + 2n^2$. Следовательно, вопрос сводится к тому, какие натуральные числа представимы в виде $m^2 - mn + 2n^2$, $m, n \in \mathbb{Z}$.

Теорема 6. *Простое число* $p \in \mathbb{N}$ *представимо в виде* $p = m^2 - mn + 2n^2$, $m, n \in \mathbb{Z}$, *тогда и только тогда, когда* p *является квадратом по модулю* 7, *т. е. когда* $p \equiv 0, 1, 2, 4 \pmod 7$.

Доказательство. Если $p = m^2 - mn + 2n^2$, то $p = (m + n\zeta)(m + n\bar{\zeta})$ и $|m+n\zeta| = |m+n\bar{\zeta}| > 1$, следовательно, p не простой элемент кольца $\mathcal{E}$. Обратно, если простое число p не является простым элементом кольца $\mathcal{E}$, то $p = ab$, где $a, b \in \mathcal{E}$ необратимы. Тогда $p^2 = |a|^2|b|^2$, причём $|a|^2, |b|^2 > 1$, следовательно, $|a|^2 = |b|^2 = p$. Так как $|a| = |b|$, $\arg a + \arg b = \arg p = 0$, то $a = \bar{b}$, т. е. $p = (m + n\zeta)(m + n\bar{\zeta}) = m^2 - mn + 2n^2$.

Итак, нужно доказать, что p является квадратом по модулю 7 тогда и только тогда, когда $p \in \mathcal{E}$ не является простым элементом. Если p не является простым элементом, то

$$p = m^2 - mn + 2n^2 \equiv m^2 + 6mn + 9n^2 = (m + 3n)^2 \pmod 7.$$

Обратно, пусть p является квадратом по модулю 7. Числа 2 и 7 не являются простыми элементами $\mathcal{E}$, так как $2 = \zeta\bar{\zeta}$, $7 = \lambda\bar{\lambda}$, поэтому можно считать, что $p \neq 2, 7$. Тогда по квадратичному закону взаимности

$$1 = \left(\frac{p}{7}\right) = (-1)^{(p-1)/2}\left(\frac{7}{p}\right) = \left(\frac{-7}{p}\right),$$

т. е. существует целое число k, не делящееся на p, с условием $k^2+7 \equiv 0 \pmod p$. Рассмотрим фактор-кольцо $R = \mathcal{E}/p\mathcal{E}$. Элементы k, $-k$ различны в этом фактор-кольце, поскольку $2k/p \notin \mathbb{Z}$, и являются в нём корнями многочлена $x^2 + 7$. Кроме того, элемент $\lambda = i\sqrt{7}$ является корнем этого многочлена и отличен от $\pm k$ в R. Действительно, $(\pm k - \lambda)/p \notin \mathcal{E}$, так как $\mathrm{Re}(\pm k - \lambda)/p = \pm k/p$ не является полуцелым. Таким образом, ненулевой многочлен второй степени имеет как минимум три различных корня в R, следовательно, R не является полем и p не является простым элементом кольца $\mathcal{E}$. □

Следствие 5.5. *Натуральное число k представимо в виде $k = m^2 - mn + 2n^2$, $m, n \in \mathbb{Z}$, тогда и только тогда, когда каждый простой делитель p числа k, не являющийся квадратом по модулю 7, входит в разложение k в чётной степени.*

Доказательство. Если числа $k, l \in \mathbb{N}$ представимы в таком виде, то $k = |a|^2$, $l = |b|^2$, $a, b \in \mathcal{E}$, и $kl = |ab|^2$, $ab \in \mathcal{E}$, т. е. kl также представимо в таком виде. Поскольку $p^2 = p^2 - p \cdot 0 + 2 \cdot 0^2$, то импликация $\Leftarrow$ доказана.

Обратно, пусть $k = m^2 - mn + 2n^2$, $m, n \in \mathbb{Z}$, и p — некоторый простой делитель числа k, не являющийся квадратом по модулю 7. Если n не делится на p, то в поле $\mathbb{Z}_p$ получаем

$$0 = k = m^2 - mn + 2n^2 = n^2\left(\left(\frac{m}{n}\right)^2 - \frac{m}{n} + 2\right),$$

следовательно, многочлен $f(x) = x^2 - x + 2$ имеет корень в $\mathbb{Z}_p$. Так как $p \neq 2$, то наличие корня квадратного трёхчлена в $\mathbb{Z}_p$ определяется его дискриминантом — он равен $1 - 8 = -7$. Но так как $p \neq 7$, то

$$\left(\frac{-7}{p}\right) = (-1)^{(p-1)/2}\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = -1,$$

следовательно, многочлен f не имеет корней в $\mathbb{Z}_p$.

Таким образом, n делится на p, и тогда m делится на p. Следовательно,

$$\frac{k}{p^2} = \left(\frac{m}{p}\right)^2 - \frac{m}{p}\cdot\frac{n}{p} + 2\left(\frac{n}{p}\right)^2 \in \mathbb{Z},$$

и число k/p^2 представимо в таком виде. Проводя для него те же рассуждения, получаем импликацию $\Rightarrow$. □

В таблице 1 выписаны все числа из $\mathcal{E}$ с нормами, не превосходящими 16.

Таблица 1. Элементы небольшой нормы в $\mathcal{E}$

$N(a)$	a
0	0
1	± 1
2	$\pm\zeta$, $\pm\bar{\zeta} = \pm(1+\zeta)$
4	$\pm\zeta^2 = \pm(2+\zeta)$, $\pm\bar{\zeta}^2 = \pm(1-\zeta)$, ± 2
7	$\pm\lambda = \pm(1+2\zeta)$
8	$\pm 2\zeta$, $\pm 2\bar{\zeta} = \pm(2+2\zeta)$, $\pm\zeta^3 = \pm(2-\zeta)$, $\pm\bar{\zeta}^3 = \pm(3+\zeta)$
9	± 3
11	$\pm(1-2\zeta)$, $\pm(1-2\bar{\zeta}) = \pm(3+2\zeta)$
14	$\pm(4+\zeta)$, $\pm(4+\bar{\zeta}) = \pm(3-\zeta)$
16	$\pm(1+3\zeta)$, $\pm(1+3\bar{\zeta}) = \pm(2+3\zeta)$, $\pm(2-2\zeta)$, $\pm(2-2\bar{\zeta}) = \pm(4+2\zeta)$, ± 4

5.5. Построение и свойства решётки L

Пусть $\mathcal{C}_{10}$, $\mathcal{C}_{10}^*$ — двоичные коды, определённые в подразделе 5.2. Они имеют длину $n = 10$, размерность $k = 5$ и минимальное расстояние $d = 4$. Они изоморфны, имеют S_6 своей группой автоморфизмов и являются ортогональными дополнениями друг к другу в $\mathbb{F}^{10}$, где $\mathbb{F}$ — поле порядка 2. Пусть также $\mathcal{E}$ — евклидово кольцо $\mathbb{Z}[\zeta]$, $\zeta = (-1+i\sqrt{7})/2$. Для чисел $a, b, c \in \mathcal{E}$ будем писать $a \equiv b \pmod{c}$, если $(a-b)/c \in \mathcal{E}$.

Так как $|\mathcal{E}/\zeta\mathcal{E}| = |\zeta|^2 = 2$, то можно отождествить фактор-кольцо $\mathcal{E}/\zeta\mathcal{E}$ с полем $\mathbb{F} = \mathbb{F}_2$. Тогда каждый вектор $(z_1, \ldots, z_{10}) \in \mathcal{E}^{10}$, рассматриваемый по модулю ζ, превращается в двоичный вектор в $\mathbb{F}^{10}$. Заметим, что для числа $a = m + n\zeta \in \mathcal{E}$ его образ в $\mathcal{E}/\zeta\mathcal{E} \cong \mathbb{F}$ совпадает с чётностью целого числа m.

Определение 5.1. Обозначим через L множество векторов $v = (z_1, \ldots, z_{10}) \in \in \mathbb{C}^{10}$, $z_p = a_p + b_p\,\zeta$, удовлетворяющих следующим условиям:

1) $a_p, b_p \in \mathbb{Z}$;

2) $m(v) = \bigl(1/(2\bar{\zeta})\bigr) \sum\limits_{p=1}^{10} z_p \in \mathcal{E}$;
3) $m(v) \equiv z_1 \equiv \ldots \equiv z_{10} \pmod{\zeta}$;
4) $\bigl(v - (z_1, \ldots, z_1)\bigr)/\zeta \in \mathcal{C}_{10}$;
5) $(b_1, \ldots, b_{10}) \in \mathcal{C}_{10}^*$.

В силу условия 3 условие 4 корректно, а так как $\mathbf{1} = (1, \ldots, 1) \in \mathcal{C}_{10}$, то оно эквивалентно условию $\bigl(v - (z_p, \ldots, z_p)\bigr)/\zeta \in \mathcal{C}_{10}$ для любого фиксированного p.

Вектор $v \in L$ назовём *чётным*, если $m(v) \equiv 0 \pmod{\zeta}$, и *нечётным*, если $m(v) \equiv 1 \pmod{\zeta}$. По условию 3 все координаты вектора v сравнимы по модулю ζ и в поле $\mathcal{E}/\zeta\mathcal{E}$ имеют ту же чётность, что и вектор v. Для чётного вектора $v \in L$ условие 4 переписывается в виде $v/\zeta \in \mathcal{C}_{10}$, а для нечётного — в виде $\bigl(v - (1, \ldots, 1)\bigr)/\zeta \in \mathcal{C}_{10}$. Заметим, что чётность вектора v определяется чётностью целых чисел a_p.

Обозначим через $(a^p\, b^q \ldots)$ любой вектор, у которого некоторые p координат равны a, некоторые q координат равны b и т. д. Через $[a^p\, b^q \ldots]$ обозначим любой вектор, у которого некоторые p координат имеют квадрат модуля a, и т. д.

Лемма 5.6.

1. *L является свободным 10-мерным $\mathcal{E}$-модулем.*
2. *L содержит все векторы вида*
   - $\pm 4e_p$, $\pm 4\zeta e_p$, $p = 1, \ldots, 10$,
   - $\bigl((\pm 2)^k\, 0^{10-k}\bigr)$ *с носителем в $\mathcal{C}_{10}$ и с любым выбором знаков,*
   - $\pm 2\zeta e_p \pm 2\zeta e_q$ *с любым выбором знаков,*
   - $\bigl((\pm\zeta)^4 (\pm 2)^2\, 0^4\bigr)$ *с носителем в $\mathcal{C}_{10}$, множество координат, равных $\pm\zeta$, является элементом $\mathcal{C}_{10}^*$, и число координат, равных $-\zeta$, чётно,*
   - $\bigl((\pm\zeta^2)^4\, 0^6\bigr)$ *с носителем в $\mathcal{C}_{10}^*$, число минусов чётно,*
   - $\bigl((1 + 2\zeta)^1\, 1^9\bigr)$.
3. *L порождается как аддитивная группа следующими векторами*:
   - $4\zeta e_1$,
   - $4e_p$, $p = 1, \ldots, 10$,
   - $(2^4\, 0^6)$ *с носителем в $\mathcal{C}_{10}$,*
   - $2\zeta e_1 + 2\zeta e_p$, $p = 2, \ldots, 10$,
   - $\bigl((\zeta^2)^4\, 0^6\bigr)$ *с носителем в $\mathcal{C}_{10}^*$,*
   - $(1 + 2\zeta, 1, \ldots, 1)$.

Доказательство. Очевидно, что L замкнуто относительно сложения и умножения на ζ, и следовательно, является $\mathcal{E}$-модулем. Так как $L \leqslant \mathcal{E}^{10}$, то L — свободный $\mathcal{E}$-модуль. Второе утверждение леммы проверяется непосредственно, и так как $4e_p \in L$ для всех p, то L имеет ранг 10.

Докажем утверждение 3. Пусть $v = (z_1, \ldots, z_{10}) \in L$, $z_p = a_p + b_p\zeta$. Если v нечётный, то заменяя его на вектор $v - (1 + 2\zeta, 1, \ldots, 1)$, можем считать, что он чётный, т. е. все числа $a_p \in \mathbb{Z}$ чётные. Множество координат с нечётными b_p

является элементом $\mathcal{C}_{10}^*$, и так как $\zeta^2 = -2 - \zeta$, то вычитая из v несколько векторов $\big((\zeta^2)^4\,0^6\big)$, получим, что все b_p чётные. Теперь при помощи векторов $2\zeta e_1 + 2\zeta e_p$ можно убрать коэффициенты при ζ во всех координатах, кроме первой.

По условию 4 в определении L множество координат, в которых $a_p \equiv 2 \pmod 4$, является элементом $\mathcal{C}_{10}$, следовательно, вычитая векторы $(2^4\,0^6)$, можно считать, что все a_p делятся на 4, а вычитая векторы $4e_p$ — что все a_p равны нулю. Теперь v имеет вид $v = 2k\zeta e_1$, $k \in \mathbb{Z}$. По условию 2 $(2k\zeta)/(2\bar{\zeta}) = (k\zeta)/(\bar{\zeta}) \in \mathcal{E}$, следовательно, k чётно. Но теперь v является кратным вектору $4\zeta e_1$. □

Можно заметить, что в доказательстве леммы 5.6 не использовалось условие $m(v) \equiv z_1 \pmod\zeta$, следовательно, оно следует из остальных (что нетрудно доказать и непосредственно).

Нормой вектора $v \in L$ будем называть его скалярный квадрат $(v, v) \in \mathbb{Z}$ (без извлечения квадратного корня). Для числа $m + n\zeta \in \mathcal{E}$ его *свободным членом* будем называть число m.

Лемма 5.7.

1. *Множество скалярных произведений векторов из L совпадает с идеалом $4\mathcal{E}$ кольца $\mathcal{E}$.*
2. *Множество вещественных частей этих скалярных произведений совпадает с множеством $2\mathbb{Z}$.*
3. *Норма каждого вектора из L является целым числом, делящимся на 4.*

Доказательство. Вычисляя скалярные произведения всех пар векторов в пункте 3 леммы 5.6, получаем, что все они делятся на 4 в $\mathcal{E}$, следовательно, скалярное произведение любых двух векторов в L делится на 4 в $\mathcal{E}$. При этом скалярное произведение векторов $4e_2$ и $(1 + 2\zeta, 1, \dots, 1)$ равно 4, следовательно, множество скалярных произведений векторов из L совпадает с $4\mathcal{E}$.

Число $m + n\zeta \in \mathcal{E}$ делится на 4, если m, n делятся на 4 в $\mathbb{Z}$. Следовательно, в этом случае $\operatorname{Re}(m + n\zeta) = m - n/2$ делится на 2. Так как скалярное произведение векторов $4\zeta e_2$ и $(1+2\zeta, 1, \dots, 1)$ равно 4ζ и $\operatorname{Re} 4\zeta = -2$, то утверждение 2 доказано.

Утверждение 3 теперь следует из утверждения 2 и того, что нормы всех векторов в пункте 3 леммы 5.6 делятся на 4. □

Таким образом, L является чётной решёткой в $\mathbb{C}^{10}$.

Заметим, что нормы порождающих векторов из леммы 5.6 делятся на 16. Однако утверждение 3 леммы 5.7 нельзя усилить: в L существует вектор $(\zeta^2+4, \zeta^2, \zeta^2, \zeta^2, 0, \dots, 0)$ с нормой 20, не делящейся на 8.

Лемма 5.8.

1. *В L нет векторов нормы 4, 8, 12.*
2. *В L содержится $6\,160 = 2^4 \cdot 5 \cdot 7 \cdot 11$ векторов нормы 16.*

Доказательство. Для начала заметим, что число $m + n\zeta \in \mathcal{E}$ имеет нечётную норму тогда и только тогда, когда m нечётно, а n чётно. Все координаты вектора $v \in L$ сравнимы по модулю ζ, поэтому если одна из них имеет нечётную норму, то свободные члены всех координат нечётны, в частности, все координаты ненулевые. Также наличие координаты с нормой 2 гарантирует наличие не менее чем четырёх ненулевых координат, поскольку элементы нормы 2 в $\mathcal{E}$ имеют нечётные коэффициенты при ζ.

Пусть $v \in L$, $(v, v) = 4$. Тогда v имеет строение $[4^1\, 0^9]$, $[2^2\, 0^8]$, $[2^1\, 1^2\, 0^7]$ или $[1^4\, 0^6]$. По предыдущему абзацу последние три случая невозможны. Элементы нормы 4 в $\mathcal{E}$ не делятся на $2\bar{\zeta}$, так как $N(2\bar{\zeta}) = 8$, поэтому и первый случай невозможен.

Пусть $v \in L$, $(v, v) = 8$. Учитывая первый абзац доказательства, получаем, что v имеет строение $[8^1\, 0^9]$, $[4^2\, 0^8]$ или $[2^4\, 0^6]$. Среди элементов нормы 8 в $\mathcal{E}$ только $\pm 2\bar{\zeta}$ делятся на $2\bar{\zeta}$. Но вектор $\big((\pm 2\bar{\zeta})^1\, 0^9\big)$ не удовлетворяет условию 4 определения L, поэтому первый случай невозможен. Во втором случае из условия 5 получаем вектор $\big((\pm 2)^1\, 0^9\big)$, который не удовлетворяет условию 4. В третьем случае, поскольку вектор v чётный, получаем, что $v = \big((\pm\zeta)^4\, 0^6\big)$. Но такой вектор не может удовлетворять одновременно условиям 4 и 5.

Пусть $v \in L$, $(v, v) = 12$. Тогда v имеет строение $[8^1\, 4^1\, 0^8]$, $[4^3\, 0^7]$, $[4^2\, 2^2\, 0^6]$, $[4^1\, 2^4\, 0^5]$, $[2^6\, 0^4]$, $[2^2\, 1^8]$. В первых двух случаях координаты с нормой 4 равны ± 2, следовательно, условие 4 не выполнено. В третьем случае ненулевые координаты образуют элемент $\mathcal{C}_{10}^*$ и свободные члены чётны, следовательно, $v = \big((\pm\zeta^2)^2(\pm\zeta)^2\, 0^6\big)$. Тогда получаем противоречие с условием 4. В четвёртом случае координаты с нормой 2 равны $\pm\zeta$ и образуют элемент $\mathcal{C}_{10}^*$, следовательно, координата с нормой 4 равна ± 2. Тогда снова получаем противоречие с условием 4. В пятом случае все ненулевые координаты равны $\pm\zeta$ и условия 4, 5 не могут быть выполнены одновременно, а шестой случай невозможен, поскольку тогда v имеет ровно два нечётных коэффициента при ζ.

Пусть теперь $v \in L$, $(v, v) = 16$. Тогда v имеет следующее строение:

(1) $[16^1\, 0^9]$, (2) $[8^2\, 0^8]$, (3) $[8^1\, 4^1\, 0^8]$, (4) $[7^1\, 1^9]$,
(5) $[4^4\, 0^6]$, (6) $[4^3\, 2^2\, 0^5]$, (7) $[4^2\, 2^4\, 0^4]$, (8) $[4^2\, 1^8]$,
(9) $[4^1\, 2^6\, 0^3]$, (10) $[4^1\, 2^3\, 1^6]$, (11) $[2^8\, 0^2]$, (12) $[2^6\, 1^4]$.

В случае 1 ненулевая координата делится на $2\bar{\zeta}$ (по свойству 2) и на ζ^2 (по свойству 4). Тогда она делится на $\zeta^2\bar{\zeta}^2 = 4$, и следовательно, равна ± 4. Число таких векторов — $10 \cdot 2 = 20$. В случае 2 коэффициенты при ζ чётны и обе ненулевые координаты делятся на ζ^2 (по свойству 4), следовательно, они равны $\pm 2\zeta$. Число таких векторов — $C_{10}^2 \cdot 4 = 180$. В случае 3 коэффициенты при ζ чётны, поэтому координата с нормой 4 равна ± 2, что противоречит условию 4.

Пусть имеет место случай 4, и координата с нормой 7 равна $\lambda = 1 + 2\zeta$. По свойству 4 множество координат, равных -1, должно образовывать множество из $\mathcal{C}_{10}$. С другой стороны, любой такой вектор можно получить, вычтя из вектора $(\lambda^1\, 1^9)$ вектор $(2^4\, 0^6)$, следовательно, все такие векторы лежат в L. Умножая

их на -1, получаем, что вектор вида $[7^1\,1^9]$ лежит в L тогда и только тогда, когда он отличается от $(\lambda^1\,1^9)$ знаками координат, образующих элемент $\mathcal{C}_{10}$. Число таких векторов — $10\cdot 2^5 = 320$.

В случае 5 получаем вектор вида $\big((\pm\zeta^2)^4\,0^6\big)$ или $\big((\pm 2)^4\,0^6\big)$. В первом случае носитель должен быть элементом $\mathcal{C}_{10}^*$ и число минусов должно быть чётно, а во втором носитель является элементом $\mathcal{C}_{10}$ и выбор знаков любой. Число таких векторов — $15\cdot 2^3 + 15\cdot 2^4 = 360$.

В случае 6 вектор имеет вид $\big((\pm 2)^1(\pm\zeta^2)^2(\pm\zeta)^2\,0^5\big)$ и условие 4 не выполнено. В случае 7 вектор имеет вид $\big((\pm\zeta^2)^2(\pm\zeta)^4\,0^4\big)$ или $\big((\pm 2)^2(\pm\zeta)^4\,0^4\big)$. В первом случае носитель лежит в $\mathcal{C}_{10}^*$, координаты, равные $\pm\zeta$, образуют элемент $\mathcal{C}_{10}$ и число минусов нечётно. Во втором случае носитель лежит в $\mathcal{C}_{10}$, координаты, равные $\pm\zeta$, образуют элемент $\mathcal{C}_{10}^*$ и число координат, равных $-\zeta$, чётно. Итого получаем $15\cdot 3\cdot 2^5 + 15\cdot 3\cdot 2^5 = 2\,880$ векторов (каждое слово веса 4 в $\mathcal{C}_{10}$ тремя способами дополняется до слова веса 6 в $\mathcal{C}_{10}^*$ и наоборот).

В случае 8 вектор имеет вид $\big((\pm\bar\zeta^2)^2(\pm 1)^8\big)$, что невозможно, поскольку ровно две координаты имеют нечётный коэффициент при ζ. В случае 9 получаем вектор $\big((\pm 2)^1(\pm\zeta)^6\,0^3\big)$, что невозможно по условию 4.

Изучим векторы типа 10. Такой вектор имеет вид $\big((\pm\bar\zeta^2)^1(\pm\bar\zeta)^3(\pm 1)^6\big)$. Без ограничения общности пусть координата с нормой 4 равна $\bar\zeta^2 = -1+\zeta$. Пусть k — число координат, равных $-\bar\zeta = 1+\zeta$, и m — число координат, равных 1. Тогда по условиям 2, 3

$$\begin{aligned} m(v) &= \frac{1}{2\bar\zeta}\big(-1+\zeta+k(1+\zeta)-(3-k)(1+\zeta)+m-(6-m)\big) = \\ &= \frac{2(k+m)-10+(2k-2)\zeta}{2\bar\zeta} = \frac{k+m-5+(k-1)\zeta}{\bar\zeta} = \\ &= -k+\frac{m-4}{\bar\zeta}+1 = 1-k+\Big(\frac{m}{2}-2\Big)\zeta \equiv 1 \pmod{\zeta}. \end{aligned}$$

Это равносильно тому, что числа k, m чётны. Из условия 4 следует, что множество координат, равных $1+\zeta$ и -1, лежит в $\mathcal{C}_{10}$, в то время как множество координат с нормой 4 и 2 лежит в $\mathcal{C}_{10}^*$ по условию 5. Таким образом, в предположении, что координата с нормой 4 равна $-1+\zeta$, получаем $15\cdot 4\cdot 16 = 960$ векторов (элемент $\mathcal{C}_{10}^*$ веса 4 выбирается пятнадцатью способами, в нём четырьмя способами выбирается координата $-1+\zeta$ и оставшиеся координаты определяются выбором элемента из $\mathcal{C}_{10}$, состоящего из координат $1+\zeta$, -1, т. е. не содержащего координату нормы 4 — таких элементов 16). Изменяя знак всего вектора, получаем 1 920 векторов типа 10.

Случай 11 невозможен, так как такой вектор имеет вид $\big((\pm\zeta)^8\,0^2\big)$, что противоречит условию 4. В случае 12 рассуждениями из предыдущего абзаца получаем, что вектор имеет вид $\big((\pm\bar\zeta)^6(\pm 1)^4\big)$, координаты с нормой 2 образуют элемент из $\mathcal{C}_{10}^*$, а координаты $1+\zeta$ и -1 образуют элемент $\mathcal{C}_{10}$. Таким образом, получаем $15\cdot 2^5 = 480$ векторов типа 12.

Итого, число векторов нормы 16 в L равно $20 + 180 + 320 + 360 + 2880 + + 1920 + 480 = 6\,160$. □

Обозначим через L_0 множество векторов в L нормы 16. В таблице 2 приведена классификация этих векторов по нормам координат.

Таблица 2. Классификация L_0

Обозн.	Тип	Структура	Описание	Количество
L_0^{16}	$[16^1\,0^9]$	$\big((\pm 4)^1 0^9\big)$	Любой такой вектор лежит в L	$10 \cdot 2 = 20$
L_0^{8}	$[8^2\,0^8]$	$\big((\pm 2\zeta)^2\,0^8\big)$	Любой такой вектор лежит в L	$C_{10}^2 \cdot 4 = 180$
L_0^{71}	$[7^1\,1^9]$	$\big((\pm\lambda)^1(\pm 1)^9\big)$	Отличие от вектора $(\lambda^1\,1^9)$ в координатах, образующих элемент $\mathcal{C}_{10}$	$10 \cdot 2^5 = 320$
L_0^{4a}	$[4^4\,0^6]$	$\big((\pm 2)^4\,0^6\big)$	Носитель лежит в $\mathcal{C}_{10}$	$15 \cdot 2^4 = 240$
L_0^{4b}	$[4^4\,0^6]$	$\big((\pm\zeta^2)^4\,0^6\big)$	Носитель лежит в $\mathcal{C}_{10}^*$, число минусов чётно	$15 \cdot 2^3 = 120$
L_0^{42a}	$[4^2 2^4\,0^4]$	$\big((\pm 2)^2(\pm\zeta)^4\,0^4\big)$	Носитель лежит в $\mathcal{C}_{10}$, координаты $\pm\zeta$ образуют элемент $\mathcal{C}_{10}^*$, число координат $-\zeta$ чётно	$15 \cdot 3 \cdot 2^5 = 1440$
L_0^{42b}	$[4^2 2^4\,0^4]$	$\big((\pm\zeta^2)^2(\pm\zeta)^4\,0^4\big)$	Носитель лежит в $\mathcal{C}_{10}^*$, координаты $\pm\zeta$ образуют элемент $\mathcal{C}_{10}$, число минусов нечётно	$15 \cdot 3 \cdot 2^5 = 1440$
L_0^{421}	$[4^1 2^3 1^6]$	$\big((\pm\bar\zeta^2)^1(\pm\bar\zeta)^3(\pm 1)^6\big)$	Координаты $\pm\bar\zeta^2$, $\pm\bar\zeta$ образуют элемент $\mathcal{C}_{10}^*$; отличие от вектора $\big((\bar\zeta^2)^1(\bar\zeta)^3\,1^6\big)$ в координатах, образующих элемент $\mathcal{C}_{10}$	$15 \cdot 4 \cdot 2^5 = 1920$
L_0^{21}	$[2^6\,1^4]$	$\big((\pm\bar\zeta)^6(\pm 1)^4\big)$	Координаты $\pm\bar\zeta$ образуют элемент $\mathcal{C}_{10}^*$; отличие от вектора $\big((\bar\zeta)^6\,1^4\big)$ в координатах, образующих элемент $\mathcal{C}_{10}$	$15 \cdot 2^5 = 480$

5.6. Фактор-решётка $L/\bar\zeta L$

Подрешётка $\bar\zeta L \leqslant L$ является $\mathcal{E}$-подмодулем, поэтому можно рассмотреть $\mathcal{E}$-фактор-модуль $\hat L = L/\bar\zeta L$. Он имеет порядок $|\hat L| = (|\bar\zeta|^2)^{10} = 2^{10}$. Заметим,

что, так как 2 делится на $\bar\zeta$ в $\mathcal{E}$, любой вектор в L содержится в одном смежном классе по $\bar\zeta L$ вместе со своим противоположным.

Лемма 5.9. *Пусть* $u, v \in L_0$, $u \neq \pm v$, $u + \bar\zeta L = v + \bar\zeta L$. *Тогда* $\operatorname{Re}(u, v) = 0$ *и* $(u - v)/\bar\zeta \in L_0$.

Доказательство. Поскольку $v + \bar\zeta L = -v + \bar\zeta L$, условия останутся в силе при замене v на $-v$, поэтому можно считать, что $\operatorname{Re}(u, v) \geqslant 0$. По условию $(u - v)/\bar\zeta = w \in L$, и $w \neq 0$. Тогда

$$(u - v, u - v) = (u, u) + (v, v) - 2\operatorname{Re}(u, v) \leqslant 16 + 16 + 0 = 32,$$
$$(u - v, u - v) = (\bar\zeta w, \bar\zeta w) = 2(w, w) \geqslant 2 \cdot 16 = 32,$$

так как в L нет ненулевых векторов с нормой меньше 16. Отсюда следует, что $\operatorname{Re}(u, v) = 0$ (второе утверждение леммы ещё не доказано, поскольку производилась замена v на $-v$). Написав с учётом этого ту же цепочку неравенств для $u + v$ вместо $u - v$, получим, что $(u + v)/\bar\zeta \in L_0$, что доказывает второе утверждение. □

Лемма 5.10. *Пусть* $u = 4e_1$, $v = 2\zeta e_1 + 2\zeta e_2$. *Тогда*

$$(u + \bar\zeta L) \cap L_0 = \{\pm 4e_p,\ p = 1, \dots, 10\} = L_0^{16}$$

и

$$\begin{aligned}(v + \bar\zeta L) \cap L_0 = \{&\pm(2\zeta, 2\zeta, 0, 0, 0, 0, 0, 0, 0, 0),\ \pm(0, 0, 2\zeta, 2\zeta, 0, 0, 0, 0, 0, 0),\\ &\pm(0, 0, 0, 0, 2\zeta, 0, 0, 2\zeta, 0, 0),\ \pm(0, 0, 0, 0, 0, -2, 2, 0, 2, 2),\\ &\pm(0, 0, 0, 0, 0, 2, -2, 0, 2, 2),\ \pm(0, 0, 0, 0, 0, 2, 2, 0, -2, 2),\\ &\pm(0, 0, 0, 0, 0, 2, 2, 0, 2, -2)\}.\end{aligned}$$

Доказательство. Все координаты вектора u делятся на $\bar\zeta$, поэтому если $w \in (u + \bar\zeta L) \cap L_0$, то все координаты вектора w также должны делиться на $\bar\zeta$. Этому условию удовлетворяют только классы векторов L_0^{16}, L_0^8, L_0^{4a}. Если $w \neq \pm u$, то по лемме 5.9 первая координата вектора w равна нулю. Теперь нетрудно видеть, что $w \notin L_0^8$, $w \notin L_0^{4a}$, следовательно, $(u + \bar\zeta L) \cap L_0 = L_0^{16}$.

Аналогично получаем, что если $w \in (v + \bar\zeta L) \cap L_0$, то все координаты w делятся на $\bar\zeta$. Пусть $w \neq \pm v$. По первому абзацу $w \notin L_0^{16}$. Учитывая лемму 5.9, нетрудно заметить, что если $w \in L_0^8$, то $w = \pm(2\zeta e_3 + 2\zeta e_4)$ или $w = \pm(2\zeta e_5 + 2\zeta e_8)$. Пусть теперь $w \in L_0^{4a}$. Тогда $\operatorname{supp} w \cap \operatorname{supp} u = \varnothing$, следовательно, $\operatorname{supp} w \in \mathcal{C}_{10}$, $\operatorname{supp}(v - w) = \operatorname{supp} v + \operatorname{supp} w \in \mathcal{C}_{10}^*$, $(v - w)\bar\zeta \in L_0^{42b}$, и число минусов в w нечётно. Таким образом, надо исследовать, сколькими способами данное двухэлементное подмножество $X \subset \Omega = \{1, \dots, 10\}$ можно дополнить четырёхэлементным множеством из $\mathcal{C}_{10}$ до шестиэлементного множества из $\mathcal{C}_{10}^*$. Так как это число не зависит от X и каждое четырёхэлементное множество из $\mathcal{C}_{10}$ тремя способами дополняется двухэлементным множеством до шестиэлементного множества из $\mathcal{C}_{10}^*$, то искомое число равно $(15 \cdot 3)/C_{10}^2 = 1$. Следовательно, $\operatorname{supp} w$ определено однозначно, и лемма доказана. □

5.7. Автоморфизмы решётки L. Двойное накрытие $2\cdot(M_{22}:2)$

Для каждого $X\subseteq\{1,\dots,10\}$ обозначим через ε_X преобразование $\mathbb{C}^{10}$, действующее по правилу

$$\varepsilon_X e_i=\begin{cases}e_i, & i\notin X,\\ -e_i, & i\in X.\end{cases}$$

Для каждого $\sigma\in S_{10}$ будем обозначать той же буквой σ преобразование $\mathbb{C}^{10}$, действующее по правилу $\sigma e_i=e_{\sigma(i)}$.

Лемма 5.11.

1. *Для всех $C\in\mathcal{C}_{10}$, $\sigma\in\operatorname{Aut}\mathcal{C}_{10}\cong S_6$ преобразования ε_C, σ являются автоморфизмами решётки L.*
2. *Автоморфизмы ε_C, $C\in\mathcal{C}_{10}$, образуют подгруппу 2^5, которая нормализуется подгруппой автоморфизмов σ, изоморфной S_6.*
3. *Пусть N обозначает полупрямое произведение подгрупп из пункта 2. Тогда N совпадает с подгруппой всех мономиальных автоморфизмов L.*
4. *N действует транзитивно на каждом классе векторов из таблицы 2, кроме L_0^{42a}, на котором N имеет две орбиты порядка $15\cdot3\cdot2^4$.*

Доказательство. Первое утверждение проверяется непосредственно применением указанных автоморфизмов к порождающим элементам решётки L (лемма 5.6) с использованием того факта, что автоморфизм $\mathcal{C}_{10}$ является и автоморфизмом $\mathcal{C}_{10}^*$, так как эти коды двойственны. Для $C\in\mathcal{C}_{10}$, $\sigma\in S_6$ имеем

$$\sigma\varepsilon_C\sigma^{-1}e_i=\sigma\varepsilon_C e_{\sigma^{-1}(i)}=$$
$$=\begin{cases}\sigma e_{\sigma^{-1}(i)}, & \sigma^{-1}(i)\notin C,\\ -\sigma e_{\sigma^{-1}(i)}, & \sigma^{-1}(i)\in C\end{cases}=\begin{cases}e_i, & i\notin\sigma(C),\\ -e_i, & i\in\sigma(C)\end{cases}=\varepsilon_{\sigma(C)}e_i,$$

что доказывает второе утверждение.

Пусть $g\in G=\operatorname{Aut}L$ — мономиальный автоморфизм, т. е. $g=d\sigma$, где d — диагональное преобразование, $\sigma\in S_{10}$. Так как $g,\sigma\in\mathrm{U}_{10}(\mathbb{C})$, то $d\in\mathrm{U}_{10}(\mathbb{C})$. Пусть $d=\operatorname{diag}(d_1,\dots,d_{10})$. Так как $g\bigl(4e_{\sigma^{-1}(i)}\bigr)=4de_i=4d_ie_i\in L$, то $d_i\in\mathcal{E}$, и так как $|d_i|=1$, то $d_i=\pm1$, т. е. $d=\varepsilon_X$ для некоторого $X\subset\{1,\dots,10\}$. Применяя автоморфизм g к элементу $(\lambda,1,\dots,1)$, получаем, что $X\in\mathcal{C}_{10}$, и следовательно, $d\in G$, $\sigma\in G$. Применяя σ ко всем векторам вида $(2^4\,0^6)$, получаем, что $\sigma\in S_6$.

Докажем пункт 4. Для начала выведем некоторые простые факты о классах блоков $\mathcal{B}_1$, $\mathcal{B}_2$, порождающих коды $\mathcal{C}_{10}$, $\mathcal{C}_{10}^*$.

— Из построения $\mathcal{B}_1$, $\mathcal{B}_2$ через силовские 3-подгруппы S_6 видно, что любое двухэлементное подмножество $\Omega=\{1,\dots,10\}$ содержится в двух блоках из $\mathcal{B}_1$ и в двух блоках из $\mathcal{B}_2$.

— S_6 действует 2-транзитивно на Ω, и стабилизатор двух точек действует на оставшихся восьми точках двумя орбитами порядка 4. Отсюда следует, что для любого двухэлементного подмножества $X \subset \Omega$ найдётся блок $B \in \mathcal{B}_1$, пересекающий X по любому наперёд заданному подмножеству.

— S_6 действует транзитивно на $\mathcal{B}_1$, стабилизатор $K = \mathrm{St}_{S_6}(B)$, $B \in \mathcal{B}_1$, изоморфен $S_4 \times 2$ и индуцирует на B всю группу S_4. Отсюда следует, что так как существуют два блока в $\mathcal{B}_1$, пересекающиеся в одной точке, то каждая точка x любого блока B содержится в некотором блоке B', пересекающем B по x.

— Стабилизатор K действует транзитивно на $\Omega \setminus B$. Это можно доказать, воспользовавшись построением $\mathcal{B}_1$, $\mathcal{B}_2$ через проективную прямую над полем порядка 9. Пусть i — корень неприводимого многочлена $x^2 + 1$ над полем $\mathbb{F}_3$ (комплексная единица редко будет использоваться в рассуждениях, поэтому здесь не возникнет путаницы) и $\mathbb{F} = \mathbb{F}_3[i]$. Стабилизатором блока $B_0 = \{\infty, 0, 1, -1\}$ в $\mathrm{PGL}_2(9)$ является подгруппа $\mathrm{PGL}_2(3) \cong S_4$, содержащаяся в $\mathrm{PSL}_2(9) \cong A_6$. Нетрудно проверить, что стабилизатором точки $i \notin B_0$ в $\mathrm{PGL}_2(3)$ является подгруппа преобразований $\{x \mapsto (ax - b)/(bx + a),\ a, b \in \mathbb{F}_3\}$. Она циклическая порядка 4, следовательно, орбита точки i при действии $\mathrm{PGL}_2(3)$ имеет порядок 6 и совпадает с $\Omega \setminus B_0$. Множество $\Omega \setminus B$ разбивается на три блока импримитивности при действии K — это три пары точек, дополняющих B до слова веса 6 из $\mathcal{C}_{10}^*$. Складывая попарно эти слова веса 6, получаем, что попарные объединения этих трёх пар точек являются блоками из $\mathcal{B}_2$.

— Пусть A — носитель слова веса 6 из $\mathcal{C}_{10}$, $B \in \mathcal{B}_2$, $B \subset A$, $X = A \setminus B$. Если P_1, P_2 — два блока из $\mathcal{B}_2$, содержащих X, то $P_i \cap B \neq \varnothing$ и $|P_i \cap A|$ чётно, следовательно, $|P_i \cap B| = 2$. Тогда два блока из $\mathcal{B}_1$, содержащих X, пересекают A по X.

Теперь транзитивность N на классах L_0^{16}, L_0^8, L_0^{71}, L_0^{4a}, L_0^{4b} очевидна. Перестановками из S_6 можно зафиксировать вектор из L_0^{42a} с точностью до изменения знаков в координатах. Для любых двух координат $\pm\zeta$ найдётся блок из $\mathcal{B}_1$, пересекающий множество координат $\pm\zeta$ по выбранным двум, поэтому можно считать, что все координаты $\pm\zeta$ имеют знак $+$. Наконец, выбирая блок из $\mathcal{B}_1$, содержащий координаты ± 2 и две нулевые координаты, можно зафиксировать знак одной из двоек. Но знак второй двойки зафиксировать невозможно, так как не существует элемента из $\mathcal{C}_{10}$, носитель которого пересекает носитель вектора из L_0^{42a} в одной точке. Таким образом, на L_0^{42a} имеем две орбиты одного порядка.

В векторах из класса L_0^{42b} снова можно зафиксировать расположение координат без учёта знаков при помощи перестановок из S_6. Пусть A — носитель такого вектора; он имеет порядок 6 и является элементом $\mathcal{C}_{10}^*$. Он естественным образом разбивается на три пары, дополняющие $\Omega \setminus A$ до шестёрки из $\mathcal{C}_{10}$. Если X — одна из этих пар, то можно поменять знаки координат X, изменив знаки в $X \cup (\Omega \setminus A) \in \mathcal{C}_{10}$. Если же $X \subset A$ — двухэлементное подмножество,

не совпадающее ни с одной из пар, то два блока из $\mathcal{B}_1$, содержащие X, не могут одновременно содержаться в A и, так как они должны пересекать A по чётному числу точек, один из них пересекает A по X. Следовательно, в этом случае тоже можно поменять знаки в X автоморфизмом из N. Таким образом, действие N на L_0^{42b} транзитивно.

Транзитивность действия на остальных двух классах очевидна, так что лемма доказана. □

Для дальнейшего изучения автоморфизмов будет удобно использовать реализацию кодов $\mathcal{C}_{10}$, $\mathcal{C}_{10}^*$ на проективной прямой $\Omega = \mathbb{F} \cup \{\infty\}$, где $\mathbb{F} = \mathbb{F}_3[i]$ — поле порядка 9. Пронумеруем элементы Ω следующим образом.

∞	0	1	-1	i	$1+i$	$-1+i$	$-i$	$1-i$	$-1-i$
1	2	3	4	5	6	7	8	9	10

Если $B_0 = \{\infty, 0, 1, -1\}$, $S = \mathrm{PSL}_2(9)$, $\tilde{S} = \mathrm{PGL}_2(9)$, то S-орбита множества B_0 состоит из пятнадцати четвёрок, порождающих один из кодов — для определённости $\mathcal{C}_{10}^*$. В $\tilde{S}$-орбите B_0 содержатся оставшиеся пятнадцать четвёрок, порождающие $\mathcal{C}_{10}$, которые вместе с первыми пятнадцатью задают на Ω структуру системы Штейнера $S(3, 4, 10)$. Ниже по строкам выписаны все слова веса 4 обоих кодов. Первые пять строк каждой таблицы образуют базис соответствующего кода.

1	2	3	4	5	6	7	8	9	10
×	×				×				×
	×	×		×	×				
		×	×		×	×			
				×	×		×	×	
					×	×		×	×
×		×		×					×
×	×					×		×	
	×		×	×		×			
	×	×					×	×	
×			×		×		×		
		×	×					×	×
				×		×	×		×
×			×	×				×	
×		×				×	×		
	×		×				×		×

$\mathcal{C}_{10}$

1	2	3	4	5	6	7	8	9	10
×	×	×	×						
	×	×				×			×
		×	×	×			×		
			×	×	×				×
			×			×	×	×	
×			×			×			×
×	×			×			×		
		×		×		×		×	
		×			×		×		×
	×		×		×			×	
	×			×			×		×
×		×			×			×	
×				×	×	×			
×							×	×	×
	×			×				×	×
	×				×	×	×		

$\mathcal{C}_{10}^*$

Рассмотрим матрицу

$$U = \frac{1}{4}\begin{pmatrix} -\lambda & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & \lambda & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & \lambda & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & \lambda & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & \lambda \\ 1 & 1 & -1 & -1 & \lambda & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & \lambda & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & \lambda & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & \lambda & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & -1 & \lambda & 1 & 1 \end{pmatrix}.$$

С помощью [3] можно проверить, что $U\bar{U}^T = E$, т. е. $U \in \mathrm{U}_{10}(\mathbb{C})$. Заметим, что векторы в строках матрицы $4U$ лежат в L_0, следовательно, векторы $4e_p$, $p = 1, \ldots, 10$, остаются в L при действии матрицей U (действие матрицы на вектор осуществляется умножением вектор-строки слева на матрицу). Нетрудно проверить, что остальные порождающие векторы L тоже остаются в L при действии этой матрицей, следовательно, $U \in G$. (Для упрощения вычислений нужно заметить, что в пункте 3 леммы 5.6 достаточно брать по пять векторов вида $(2^4\,0^6)$ и $\big((\zeta^2)^4\,0^6\big)$ с носителями в базисных векторах соответствующих кодов.)

Лемма 5.12. *Пусть T_1, T_2 — две N-орбиты на L_0^{42a}, причём T_1 содержит векторы вида $(2^2\,\zeta^4\,0^4)$. Группа G имеет две орбиты при действии на L_0:*

$$\Phi = L_0^{16} \cup L_0^{71} \cup L_0^{21} \cup T_2,$$
$$\Psi = L_0^{8} \cup L_0^{4a} \cup L_0^{4b} \cup L_0^{42b} \cup L_0^{421} \cup T_1.$$

Они имеют порядки $|\Phi| = 1540 = 2^2 \cdot 5 \cdot 7 \cdot 11$ и $|\Psi| = 4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

Доказательство. Достаточно показать, что автоморфизм U сливает между собой классы векторов в Φ и Ψ. При проверке того, что U — автоморфизм L, уже получено, что сливаются между собой N-орбиты L_0^{16}, L_0^{71}, N-орбиты L_0^{8}, L_0^{42b} и N-орбиты L_0^{4a}, L_0^{421}, T_1. Непосредственно проверяется, что

$$(1,1,1,1,\bar\zeta,\bar\zeta,\bar\zeta,\bar\zeta,\bar\zeta,\bar\zeta) \in L_0^{21} \xrightarrow{U} (-\lambda,-1,1,1,1,1,-1,1,-1,1) \in L_0^{71},$$
$$(\zeta,\zeta,\zeta,\zeta,2,0,0,-2,0,0) \in T_2 \xrightarrow{U} (-\bar\zeta,\bar\zeta,-1,1,-1,\bar\zeta,\bar\zeta,1,\bar\zeta,-\bar\zeta) \in L_0^{21},$$
$$(\zeta^2,\zeta^2,\zeta^2,\zeta^2,0,0,0,0,0,0) \in L_0^{4b} \xrightarrow{U} (-2,2,0,0,0,0,2,0,2,0) \in L_0^{4a},$$
$$(\zeta,\zeta,0,0,0,\zeta,\zeta^2,0,-\zeta^2,\zeta) \in L_0^{42b} \xrightarrow{U} (-\bar\zeta,-1,-\bar\zeta^2,-1,-1,\bar\zeta,1,-1,\bar\zeta,1) \in L_0^{421}.$$

Таким образом, слиты между собой все N-орбиты в Φ и все N-орбиты в Ψ.

Осталось показать, что Φ и Ψ не сливаются в одну орбиту. Так как подрешётка $\bar\zeta L$ инвариантна при автоморфизмах L, то они действуют на смежных

классах по $\bar\zeta L$. По лемме 5.10 в смежных классах векторов $4e_1 \in \Phi$ и $2\zeta e_1 + 2\zeta e_2 \in \Psi$ содержится разное количество векторов из L_0, следовательно, они не могут быть переставлены автоморфизмом L.

Порядки орбит Φ и Ψ вычисляются непосредственно. □

Теорема 7. $|G| = 2^9 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 1\,774\,080 = 4 \cdot |M_{22}|$.

Доказательство. Обозначим через $\hat\Phi$ множество смежных классов по $\bar\zeta L$, содержащих векторы из Φ. Тогда $|\Phi| = 1540/20 = 77$, и группа G действует на Φ транзитивно. Стабилизатор $K = \mathrm{St}_G(\hat x)$, где $\hat x = 4e_1 + \bar\zeta L$, переставляет между собой векторы $\pm 4e_p$, $p = 1, \ldots, 10$, т. е. состоит из мономиальных преобразований. По лемме 5.11 $K = N$, следовательно, $|G| = 77 \cdot |N| = 77 \cdot 2^5 \cdot 720 = 2^9 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$. □

Лемма 5.13. *Подгруппа $N = \mathrm{St}_G(\hat x)$ имеет две орбиты на $\hat\Phi \setminus \{\hat x\}$ порядков* 16 *и* 60.

Доказательство. Применяя матрицу U к $\hat x$, получаем, что строки матрицы $4U$ лежат в одном смежном классе по $\bar\zeta L$. Кроме того, нетрудно видеть, что векторы

$$(\bar\zeta, \bar\zeta, 1, 1, -1, \bar\zeta, -\bar\zeta, -1, \bar\zeta, -\bar\zeta) \in L_0^{21}, \quad (-2, 2, \zeta, \zeta, \zeta, 0, 0, \zeta, 0, 0) \in T_2$$

лежат в одном смежном классе по $\bar\zeta$. Так как N действует транзитивно на L_0^{71}, L_0^{21}, T_2, то L_0^{71} целиком состоит из наборов из двадцати векторов, лежащих в одном смежном классе, а остальные смежные классы из $\hat\Phi$ распределены по орбитам L_0^{21}, T_2. Таким образом, N имеет две орбиты на $\hat\Phi \setminus \{\hat x\}$ порядков $|L_0^{71}|/20 = 16$ и $77 - 1 - 16 = 60$. □

Обозначим N-орбиты на $\hat\Phi$ через Γ, Δ так, что $|\Gamma| = 16$, $|\Delta| = 60$. Найдём ядро K действия G на $\hat\Phi$. Ясно, что оно содержится в $\mathrm{St}_G(\hat x) = N$. Пусть $B = \{6, 7, 9, 10\} \in \mathcal{C}_{10}$. Тогда $\varepsilon_B \in N$, и

$$V = U\varepsilon_B U^{-1} = \frac{1}{4}\begin{pmatrix} 2 & -2 & -\zeta & -\zeta & -\zeta & 0 & 0 & -\zeta & 0 & 0 \\ -2 & 2 & -\zeta & -\zeta & -\zeta & 0 & 0 & -\zeta & 0 & 0 \\ -\bar\zeta & -\bar\zeta & -1 & -1 & 1 & -\bar\zeta & \bar\zeta & 1 & -\bar\zeta & \bar\zeta \\ -\bar\zeta & -\bar\zeta & -1 & -1 & 1 & \bar\zeta & -\bar\zeta & 1 & \bar\zeta & -\bar\zeta \\ -\bar\zeta & -\bar\zeta & 1 & 1 & -1 & -\bar\zeta & -\bar\zeta & -1 & \bar\zeta & \bar\zeta \\ 0 & 0 & -\zeta & \zeta & -\zeta & 2 & 0 & \zeta & 0 & 2 \\ 0 & 0 & \zeta & -\zeta & -\zeta & 0 & 2 & \zeta & 2 & 0 \\ -\bar\zeta & -\bar\zeta & 1 & 1 & -1 & \bar\zeta & \bar\zeta & -1 & -\bar\zeta & -\bar\zeta \\ 0 & 0 & -\zeta & \zeta & \zeta & 0 & 2 & -\zeta & 2 & 0 \\ 0 & 0 & \zeta & -\zeta & \zeta & 2 & 0 & -\zeta & 0 & 2 \end{pmatrix} \in G.$$

Отсюда следует, что строки матрицы $4V$ лежат в одном смежном классе из Δ. Все четыре вектора типа $[2^6\,1^4]$ в этом смежном классе имеют единицы в одних и тех же координатах, образующих элемент $\mathcal{C}_{10}^*$. Так как подгруппа N транзитивна на Δ, то это верно для всех смежных классов в Δ. Следовательно, элемент $g \in K$, действуя на координатах, оставляет на месте все блоки

из $\mathcal{B}_2$. Группа автоморфизмов S_6 кода $\mathcal{C}_{10}^*$ действует на нём без ядра, поэтому $g \in 2^5 \leqslant N$, т. е. g действует только изменением знаков координат. Теперь, рассмотрев первую строку матрицы $4U$, получаем, что $g = \pm E$, т. е. $K = \{\pm E\}$.

Теорема 8. *$G \cong 2 \cdot (M_{22} : 2)$, и расширение $2 \cdot M_{22}$ не расщепляется.*

Доказательство. Фактор-группа $\hat{G} = G/K$ является примитивной группой перестановок на $\hat{\Phi}$ ранга 3, причём порядок $|\hat{G}|$ чётный. По лемме 2.2 на $\hat{\Phi}$ можно задать структуру сильно регулярного графа $\mathrm{srg}(77, 16, \lambda, \mu)$ для некоторых $\lambda, \mu \geqslant 0$, сохраняющуюся при действии G. По лемме 2.1

$$(77 - 16 - 1)\mu = 16(16 - \lambda - 1), \quad 60\mu = 240 - 16\lambda, \quad 15\mu = 60 - 4\lambda.$$

Отсюда следует, что λ делится на 15 и $\lambda \leqslant 15$. Если $\lambda = 15$, то $\mu = 0$, т. е. две несоседние вершины не имеют общих соседей. Тогда между Γ и Δ нет рёбер, и $\Gamma \cup \{\hat{x}\}$ — полный граф, являющийся компонентой связности графа $\hat{\Phi}$. Но так как группа G транзитивна на $\hat{\Phi}$, то $\hat{\Phi}$ разбивается на компоненты связности одного порядка, что невозможно, так как 77 не делится на 17. Таким образом, $\lambda = 0$, $\mu = 4$, $\hat{\Phi} = \mathrm{srg}(77, 16, 0, 4)$. По теореме 5 группа автоморфизмов этого графа изоморфна $M_{22} : 2$. Так как $|\hat{G}| = |M_{22}| \cdot 2$, то $\hat{G} \cong M_{22} : 2$.

Осталось показать, что расширение $G \cong 2 \,.\, (M_{22} : 2)$, и даже расширение $2 \,.\, M_{22}$, не расщепляется. Пусть $N_0 = 2^5 : A_6 \leqslant N$. По лемме 5.4 $2^5 \leqslant N_0'$, следовательно, $N_0' = N_0$, в частности, N_0 не содержит подгрупп индекса 2. Тогда $N_0 \leqslant 2 \,.\, M_{22}$, и так как расширение $\mathbb{F}_2 A_6$-модулей $\langle \Omega \rangle \leqslant \mathcal{C}_{10}$ не расщепляется, то и расширение $2 \,.\, M_{22}$ не расщепляется. □

5.8. Фактор-решётка $L/\lambda L$. Построение группы $4 \cdot M_{22}$

Будем обозначать факторизацию по λL и по $\lambda\mathcal{E}$ тильдой. Фактор-решётка $\tilde{L} = L/\lambda L$ имеет порядок $(|\lambda|^2)^{10} = 7^{10}$. Она может быть рассмотрена как векторное пространство над полем $\tilde{\mathcal{E}} = \mathcal{E}/\lambda\mathcal{E} \cong \mathbb{F}_7$. Определим на $\tilde{L}$ билинейную форму $f\colon \tilde{L} \times \tilde{L} \to \tilde{\mathcal{E}}$ по формуле

$$f(\tilde{u}, \tilde{v}) = \widetilde{(u, v)}, \quad u, v \in L.$$

Это определение корректно:

$$\begin{aligned}(u + \lambda a, v + \lambda b) &= (u, v) + \lambda(a, v) + \bar{\lambda}(u, b) + 7(a, b) = \\ &= (u, v) + \lambda(a, v) - \lambda(u, b) + 7(a, b) \equiv (u, v) \pmod{\lambda}, \quad a, b \in L.\end{aligned}$$

Здесь существенно, что λ — чисто мнимое число. Билинейность f следует из того, что для любого $r = m + n\zeta \in \mathcal{E}$ $r - \bar{r} = n(\zeta - \bar{\zeta}) = \lambda n \in \lambda\mathcal{E}$, т. е. $\tilde{r} = \bar{\tilde{r}}$.

Лемма 5.14. *Билинейная форма f невырожденна, симметрична и имеет тип $-$.*

Доказательство. Докажем, что векторы $\tilde{x}_p = 4e_p + \lambda L$, $p = 1, \ldots, 10$, образуют базис $\tilde{L}$. Действительно, матрица Грама формы f на векторах $\tilde{x}_p$ равна

$16E$, её определитель равен $16^{10} = 2^{40} \not\equiv 0 \pmod{\lambda}$. Следовательно, эти векторы линейно независимы, и f невырожденна. Симметричность f следует из свойства $r \equiv \bar{r} \pmod{\lambda}$ для всех $r \in \mathcal{E}$.

Знак невырожденной симметрической билинейной формы f на векторном пространстве размерности $2n$ над полем $\mathbb{F}_q$ порядка q определяется формулой $\operatorname{sgn} f = \varepsilon^n \delta$, где $\varepsilon, \delta \in \{\pm 1\}$, $q \equiv \varepsilon \pmod{4}$ и $\delta = 1$ тогда и только тогда, когда $\det f$ является квадратом в $\mathbb{F}_q$. Так как $\det f = (2^{20})^2$ и $7 \equiv -1 \pmod{4}$, то $\operatorname{sgn} f = (-1)^5 \cdot 1 = -1$. □

Наконец, докажем основной результат данного раздела.

Теорема 9. *Группа M_{22} допускает четверное накрытие $4 \cdot M_{22}$.*

Доказательство. Докажем, что группа G действует на $\tilde{L}$ без ядра. Если K — ядро этого действия, то $-E \notin K$, и так как расширение $2 \cdot M_{22}$ не расщепляется, то $K \cap (2 \cdot M_{22}) = 1$. Тогда $|K| \leqslant 2$, и так как $M_{22} : 2 \ncong M_{22} \times 2$, то $K = 1$.

Так как G при действии на $\tilde{L}$ сохраняет форму f, то G вкладывается в полную ортогональную группу $\mathrm{O}_{10}^-(7)$, а так как $2 \cdot M_{22}$ не содержит подгрупп индекса 2, то $2 \cdot M_{22}$ вкладывается в $\Omega_{10}^-(7)$. Центральная инволюция в $2 \cdot M_{22}$ при этом вложении переходит в скалярное преобразование $-E \in \Omega_{10}^-(7)$. В спинорной группе $2\,.\,\Omega_{10}^-(7)$ элемент $-E$ поднимается до элемента порядка 4, следовательно, подгруппа $2\,.\,(2 \cdot M_{22}) \leqslant 2\,.\,\Omega_{10}^-(7)$ изоморфна $4 \cdot M_{22}$. Так как в группе M_{22} нет подгрупп индекса 2, то циклическая подгруппа порядка 4 является центральной.

Теорема доказана. □

Мультипликатор Шура этой группы является циклической группой порядка 12 [1]. Оставшаяся 3-часть этого мультипликатора может быть построена путём вложения группы M_{22} в $\mathrm{U}_6(2)$ и расширения её до группы $\mathrm{SU}_6(2) = 3 \cdot \mathrm{U}_6(2)$. В группе Янко J_4 содержится шестерное накрытие $6 \cdot M_{22}$ — ещё один способ построить 3-часть мультипликатора Шура M_{22}.

6. Заключение

Описанные в данной работе построения являются далеко не единственными примерами применения теории решёток к построению накрытий простых групп. Так, например, при помощи 24-мерной вещественной решётки Лича строится двойное накрытие спорадической простой группы Конвея Co_1. В действительности эта группа определяется именно как фактор-группа группы автоморфизмов Co_0 решётки Лича по подгруппе $\{\pm E\}$. Конструкция 12-мерной комплексной решётки Лича (изоморфной предыдущей как вещественная решётка) над кольцом целых эйзенштейновых чисел ведёт к построению шестерного накрытия спорадической простой группы Судзуки Suz, а некоторые шестимерные решётки над

кольцом икосианов в алгебре кватернионов позволяют построить двойное накрытие группы Янко J_2 и исключительное двойное накрытие группы типа Ли $G_2(4)$.

Существование накрытий групп можно доказывать также методами теории когомологий. Однако представленный в данной работе метод позволяет не только доказать их существование, но и получить несколько транзитивных перестановочных представлений этих групп (на векторах фиксированной нормы), а также несколько неприводимых линейных представлений, как в положительной характеристике — на фактор-решётках по различным подрешёткам, так и в характеристике 0 — на самом пространстве $\mathbb{R}^n$ или $\mathbb{C}^n$.

Литература

[1] Atlas of Finite Group Representations. Version 3. — `https://brauer.maths.qmul.ac.uk/Atlas/v3/`.

[2] Brouwer A. E. The uniqueness of the strongly regular graph on 77 points // J. Graph Theory. — 1983. — Vol. 7, no. 4. — P. 455—461.

[3] Matrix calculator. — `https://matrixcalc.org/ru/`.

[4] Wilson R. A. The Finite Simple Groups. — Springer, 2007.