Правительство Российской Федерации

Федеральное государственное автономное
образовательное учреждение
высшего профессионального образования
“Национальный исследовательский университет
Высшая школа экономики”

Факультет математики

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
на тему

“Максимальные Порядки в Алгебрах Кватернионов и Фуксовы Группы”

Студентка группы 4.11.1
Пащевская Софья Александровна

Руководитель ВКР
Доктор физико-математических наук, профессор,
Шварцман Осип Владимирович

Москва, 2013

Содержание

1 Алгебры кватернионов и максимальные порядки в них

Определение 1. *Алгеброй кватернионов A над $\mathbb{Q}$ называется четырехмерное пространство над $\mathbb{Q}$ с базисом $1, i, j, k$, где умножение определяется следующим образом:* 1 *является единицей, так что выполнено*

$$i^2 = a1, \quad j^2 = b1, \quad ij = -ji = k$$

для каких-то $a, b \in \mathbb{Q}^*$; умножение продолжается линейно, так что A становится ассоциативной алгеброй над $\mathbb{Q}$.

Таким образом сконструированная алгебра будет обозначаться символом Гильберта

$$\left(\frac{a, b}{\mathbb{Q}}\right).$$

Заметим, что

$$k^2 = (ij)^2 = -ab.$$

Очевидно, что любые два базисных вектора i, j и k анти-коммутируют.

Определение 2. *Обозначим за A_0 подпространство в A, натянутое на векторы i, j и k. Элементы из A_0 называются чистыми кватернионами.*

Ясно, что это определение не зависит от выбора базиса.

Рассмотрим $\mathbb{Q}-$линейный автоморфизм

$$x = (1, i, j, k) \mapsto \bar{x} = (1, -i, -j, -k).$$

Он определяет анти-инволюцию в A:

$$\bar{xy} = \bar{y}\bar{x} \quad \text{и} \quad \bar{\bar{x}} = x.$$

Определение 3. *След и норма кватерниона x — это элементы*

$$T(x) = x + \bar{x} \in \mathbb{Q}$$

и $n(x) = x\bar{x} \in \mathbb{Q}^2$, соответственно.

След является $\mathbb{Q}-$линейным отображением $A \longrightarrow \mathbb{Q}$, и легко проверяется, что $\mathbb{Q}-$билинейная форма

$$(x, y) \mapsto T(x\bar{y}),$$

симметрична и невырожденна. Норма определяет квадратичную форму от 4 переменных над $\mathbb{Q}$, которая равна

$$2n(\alpha + \beta i + \gamma j + \delta k) = 2\left[\alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2\right],$$

и тоже невырожденна. Ниже, при нахождении группы автоморфизмов решетки, нам будет удобнее работать без множителя 2, который в нашем случае не играет роли.

Роль, которую играет кольцо целых ($\mathbb{Z}$ в нашем случае) в числовом поле, заменяет понятие порядка в алгебрах кватернионов.

Определение 4.

- *Порядок $\mathfrak{O}$ в алгебре A над полем $\mathbb{Q}$ — это подкольцо в A, являющееся $\mathbb{Z}-$решеткой полного ранга.*
- *Порядок $\mathfrak{O}$ называется максимальным, если он максимальный по включению.*

Теперь мы можем сформулировать необходимую теорему:

Теорема 5. *Пусть A — $\mathbb{Q}-$алгебра ранга 4, тогда следующие утверждения эквивалентны:*

- *A — алгебра кватернионов над $\mathbb{Q}$,*
- *A имеет центр и является простой (то есть не имеет нетривиальных двусторонних идеалов),*
- *$A \otimes_{\mathbb{Q}} \bar{\mathbb{Q}} \cong M_2(\bar{\mathbb{Q}})$.*

Если эти свойства выполняются, то либо $A \cong M_2(\mathbb{Q})$, либо A является алгеброй с делением.

Алгебра кватернионов, изоморфная $M_2(\mathbb{Q})$, называется расщепимой (или тривиальной) алгеброй кватернионов.

2 Постановка задачи и основной результат

Определение 6. *Нормализатором порядка $\mathfrak{O}$ называется группа*

$$N(\mathfrak{O}) = \left\{x \in A^* : x\mathfrak{O}x^{-1} = \mathfrak{O}\right\}.$$

Нормализатор можно изучать локально, а именно:

Лемма 7. $N(\mathfrak{O}) = \{x \in A^* : x \in N(\mathfrak{O}_\mathfrak{p})$*для любого конечного* $p\}$. *При этом в случае нерасщепимой алгебры максимальный порядок единственный, и нормализатор $N(\mathfrak{O}_\mathfrak{p}) = A^*$, где алгебра определена над соответствующим $\mathbb{Q}_p$. В противном случае, нормализатор есть $\mathbb{Q}^*\mathfrak{O}_\mathfrak{p}^*$.*

Нормализатор $N(\mathfrak{O})$ действует на решетке $\mathfrak{O}$ сопряжениями, сохраняя при этом решетку $\mathfrak{O} \cap A_0 = M$. Известно, что сопряжения с помощью элементов $a \in A^*$ индуцируют на M ортогональные в смысле формы $n(x)$ преобразования с определителем 1. В частности, группа $N(\mathfrak{O})$ действует автоморфизмами гиперболической решетки M. Ее образ в группе $Aut^+(M)$ автоморфизмов решетки с определителем 1 будем обозначать $\Gamma(\mathfrak{O})$. Возникает естественный вопрос: чему равен индекс $[Aut^+(M) : \Gamma(\mathfrak{O})]$? Известно, что он конечен. Равносильный вопрос - это вопрос об индексе группы $\Gamma(\mathfrak{O}) \cup \langle -E \rangle$ в группе $Aut(M)$. Ответ на этот вопрос в общем виде нам неизвестен, но в частном случае мы докажем совпадение этих групп, используя технику групп отражений. Точнее, мы докажем совпадение фуксовых групп $\mathbb{P}(Aut(M))$ и $\mathbb{P}(\Gamma(\mathfrak{O}))$ в группе автоморфизмов плоскости Лобачевского.

3 Нахождение максимального порядка алгебры $A = \left(\frac{-1,p}{\mathbb{Q}}\right)$

Начнем со следующего определения:

Определение 8. *Пусть есть локальное поле ($p-$адические числа $\mathbb{Q}_p$ в нашем случае), тогда символом Гильберта называется функция* $(*,*)$: $\mathbb{Q}_p^* \times \mathbb{Q}_p^* \longrightarrow \{-1, 1\}$, *определенная следующим образом:*

$$(a,b) = \begin{cases} 1, & \text{если } z^2 = ax^2 + by^2 \text{ имеет ненулевое решение } (x,y,z) \in \mathbb{Q}_p^3; \\ -1, & \text{иначе.} \end{cases}$$

Для рациональных чисел ν и a, b, пусть $(a, b)_\nu$ обозначает значение символа Гильберта в соответствующем пополнении $\mathbb{Q}_\nu$. Если ν есть простое число p, то соответствующее пополнение — $p-$адическое поле, а если ν равно бесконечности, то пополнение есть $\mathbb{R}$.

Над $\mathbb{R}$, $(a, b)_\infty = +1$, если хотя бы одно число из a и b положительно, и -1, если оба отрицательны. Над $p-$адическими числами с нечетным p, записав $a = p^\alpha u$ и $b = p^\beta v$, где u и v — целые, взаимно простые с p, имеем

$$(a, b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha,$$

где $\epsilon(p) = (p-1)/2$ и выражение включает в себя два символа Лежандра. Для 2−адических чисел, снова записывая $a = 2^\alpha u$ и $b = 2^\beta v$, где u и v — нечетные, мы имеем

$$(a, b)_2 = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)},$$

где $\omega(x) = (x^2 - 1)/8$.

Вопрос о том, является алгебра расщепимой или нет, сводится к вычислению символа Гильберта, а именно: пусть $A = \left(\frac{a,b}{\mathbb{Q}_p}\right)$, тогда если $(a, b) = -1$, то A — алгебра с делением; и A изоморфна алгебре 2 на 2 матриц, если $(a, b) = +1$. Рассмотрев алгебру A над $\mathbb{Q}_p$ для всех p, мы можем посчитать символы Гильберта, что позволит нам посчитать дискриминант:

Определение 9. *Дискриминантом $d(A)$ алгебры кватернионов A над $\mathbb{Q}$ называется произведение простых чисел p, для которых A является алгеброй с делением над $\mathbb{Q}_p$.*

Дискриминант $d(\mathfrak{O})$ кватернионного порядка является очень важным инвариантом и определяется следующим образом:

Определение 10. *Дискриминант $d(\mathfrak{O})$ кватернионного порядка — это целое число $\det(T(x_i\bar{x}_j)), 1 \leq i, j \leq 4$, где x_i — базис порядка*

Дискриминант позволяет нам найти максимальный порядок в алгебре кватернионов, применяя следующую теорему:

Теорема 11. *Пусть d — дискриминант алгебры A, тогда максимальные порядки в A — это такие порядки в A, которые имеют дискриминант, равный d^2.*

Теперь рассмотрим пример нахождения максимального порядка в алгебре кватернионов $A = \left(\frac{-1,p}{\mathbb{Q}}\right)$, где p — простое число: прежде всего, посчитаем дискриминант алгебры A. Из вышенаписанного следует, что нам необходимо посчитать символ Гильберта для всех простых чисел и ∞. Из формул для подсчета символа Гильберта очевидно, что $(-1,p)_2 = -1$ и $(-1,p)_p = -1$, а для остальных простых чисел и для бесконечности значение символа Гильберта есть 1. Тогда $d(A) = 2p$. Таким образом, наша задача состоит в том, что бы найти $\mathbb{Z}-$решетку с дискриминантом $2p = 4p^2$, которая и будет максимальным порядком в A.

Рассмотрим решетку $\mathfrak{O} = \mathbb{Z}[i,j,k,\frac{1+i+j+k}{2}]$, и заметив, что элемент $\frac{1+i+j+k}{2}$, умноженный на себя, равен $1 + \frac{1+i+j+k}{2}$, и при умножении его на i, j или k, мы не выходим за пределы решетки $\mathfrak{O}$, заключим, что это порядок. Посчитав следы всех элементов вида $x_i\bar{x}_j$, найдем дискриминант порядка:

$$\det\begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & -2p & 0 & -p \\ 0 & 0 & -2p & -p \\ 1 & -p & -p & 1-p \end{pmatrix} = 4p^2,$$

откуда следует, что найденный порядок максимален.

4 Описание нормализатора

В нашем примере алгебры $A = \left(\frac{-1,p}{\mathbb{Q}}\right)$ имеет место

Лемма 12. *Для всех простых чисел p справедливо*

$$\mathbb{Q}_p^*\mathfrak{O}_p^* = \left\{\text{элементы вида } qx, \text{ где } q \in \mathbb{Q}_p^* \text{ и } n(x) \text{ не делится на } p.\right\}$$

Доказательство. В доказательстве мы пользуемся тем, что $p \neq 2$, и в этом случае $\mathfrak{O}_p = \{a + bi + cj + dk, \text{где } a,b,c,d \in \mathbb{Z}_p\}$. Одно включение очевидно, так как если норма не делится на p, то она обратима в $\mathbb{Z}_p$. Докажем второе включение: пусть $n(x) = p^k\lambda$, где $k \geq 1$ и λ не делится на p. Пусть $x = a + bi + cj + dk$, где $a,b,c,d \in \mathbb{Z}_p$. Если $x^{-1} \in \mathfrak{O}_p$, то $\bar{x} = n(x)\alpha$, где $\alpha \in \mathfrak{O}_p$, и тогда a,b,c,d делятся на p^k, а $n(x)$ — на p^{2k}, чего не может быть. $\square$

Теперь нам нужно пересечь все локальные нормализаторы по всем простым числам, кроме 2 и p, откуда мы получим, что нормализатор максимального порядка равен

$$\mathbb{Q}^* \left\{ \text{элементы из } \mathfrak{O}\text{, норма которых делится только на 2 и } p \right\}.$$

5 Метод отражений

У группы автоморфизмов, о которой шла речь выше, есть фундаментальный многоугольник, стороны которого являются зеркалами отражений r_i. Ниже мы покажем, что сопряжения чистыми кватернионами задают отражения, и тогда, если нам удастся найти элементы $a_1, \dots a_n$ из нормализатора, так что $-(a_i x a_i^{-1}) = r_i$, то равенство групп, очевидно, имеет место. Ниже мы найдем фундаментальный многоугольник для конкретной алгебры и соответствующей квадратичной формы.

Рассмотрим в алгебре $A = \left(\frac{-1,3}{\mathbb{Q}}\right)$ решетку $M = \mathbb{Z}[i,j,k]$, состоящую из линейных комбинаций базисных чистых кватернионов с целыми коэффициентами. Норма элемента $x = ai + bj + ck \in M$, индуцированная нормой из алгебры A, есть квадратичная форма $a^2 - 3b^2 - 3c^2$. Рассмотрим группу линейных преобразований трехмерного пространства чистых кватернионов, которые сохраняют эту норму и переводят решетку в себя. Чистые кватернионы нормы 1 образуют гиперболоид в трехмерном пространстве (его уравнение — $x^2 - 3y^2 - 3z^2 = 1$), каждая компонента связности которого служит моделью для плоскости Лобачевского. Поскольку мы рассматриваем линейные преобразования, сохраняющие норму, то наша группа действует на плоскости Лобачевского. Мы докажем, что это дискретная подгруппа, и найдем ее фундаментальную область. Линейные преобразования, сохраняющие интересующую нас норму, можно задавать с помощью сопряжения кватернионов: пусть s — сопряжение, действующее по правилу $s(y)x = \pm y x y^{-1}$ для $x, y \in A^*$. Имеет место следующая

Лемма 13. *Любое линейное преобразование трехмерного пространства, сохраняющее норму, задается как сопряжение с помощью некоторого обратимого кватерниона.*

Перейдем теперь к необходимым утверждениям:

6 Технические леммы

Лемма 14. *Для сопряжения с помощью чистых кватернионов справедливо $s(y)x = -r_y$, где r_y — отражение в векторе y.*

Доказательство. Заметим, что для чистых кватернионов справедливо $y^* = -y$ и $y^{-1} = \frac{-y}{n(y)}$. Тогда можем записать $s(y)x = yxy^{-1} = -(yxy)\frac{1}{n(y)}$. Далее,

$$n(x+y) = (x^*+y^*)(x+y) = x^*x + x^*y + y^*x + y^*y = n(x) + n(y) - xy - yx,$$

откуда $xy + yx = -2\frac{1}{2}(n(x+y) - n(x) - n(y)) = -2(x,y)$, где (x,y) — скалярное произведение. Отсюда получаем

$$-(yxy)\frac{1}{n(y)} = \frac{1}{n(y)}(y(2(x,y) + yx)) = -x + \frac{2(x,y)}{n(y)}y = -r_y,$$

и все доказано. □

Лемма 15. *Сопряжение посредством чистого кватерниона задает на плоскости Лобачевского отражение тогда и только тогда, когда норма кватерниона отрицательна.*

Доказательство. Достаточно заметить, что тот факт, что норма отрицательна, равносилен тому, что соответствующая плоскость отражения пересекает гиперболоид. □

Лемма 16. *Теорема о взаимном базисе решеток. Для пары решеток L и M найдутся базис $e_1, \dots, e_n$ в M и числа $k_1, \dots, k_n$ такие, что $k_1|k_2|\dots|k_n$ и $k_1 r_1, \dots k_n r_n$ — базис в L, причем k_i определены однозначно.*

7 Нахождение фундаментального многоугольника для алгебры $A = \left(\frac{-1,3}{\mathbb{Q}}\right)$

Во-первых, сли в качестве пары взять решетку M и двойственную к ней $M^* = \{x : (x, M) \in \mathbb{Z}\}$, то из леммы будет следовать, что норма элемента y, которым мы сопрягаем, должна делить k_n, что в нашем случае означает, что $n(y)$ может принимать значения $-1, -2, -3, -6$. Во вторых, у любого фундаментального многоугольника для нашей группы углы могут быть только вида π/n.

Найдем фундаментальный многоугольник.

Сопряжение с помощью элемента k сохраняет решетку, следовательно, принадлежит нашей группе. Рассмотрим прямую на плоскости Лобачевского, соответствующую элементу k, и прямую, соответствующую элементу $i + j$. Легко проверить, что отражения относительно них принадлежат нашей группе. Эти прямые ортогональны.

Докажем, что через точку пересечения этих прямых не может проходить никакая прямая, отражение относительно которой лежит в нашей группе. Действительно, такая прямая записывается уравнением $a(i+j)+bk$ для каких-то целых a, b. Но по условию на норму $a^2 - 3a^2 - 3b^2 = -1, -2, -3, -6$. Ясно, что такое выражение может принимать только два из этих значений, а именно: $-2, -3$, откуда либо $a = 0, b = 1$, либо $a = 1, b = 0$, а это и есть наши k и $i + j$.

Из доказанного следует, что существует фундаментальный многоугольник, для которого стороны, задаваемые нормалями k и $i + j$, являются соседними. Определим теперь все прямые, перпендикулярные прямой, задаваемой элементом k, отражения относительно которых лежат в нашей группе. Этим прямым будут отвечать кватернионы вида $ai + bj$ для целых a, b. Норма кватерниона такого вида есть $a^2 - 3b^2$ и легко видеть, что это выражение не может принимать значения -1 и -6 по модулю 3.

Опишем, как устроены кватернионы такого вида с нормой -2 и -3. Для этого используем теорию уравнений Пелля: в поле $\mathbb{Q}[\sqrt{3}]$ норма элемента $a + b\sqrt{3}$ есть $a^2 - 3b^2$. Известен следующий факт:

Лемма 17.

- *Элемент $a + b\sqrt{3}$ с целыми a, b имеет норму 1 тогда и только тогда, когда $a + b\sqrt{3} = (2 + \sqrt{3})^m$ для некоторого целого m.*

- *Элемент $a + b\sqrt{3}$ имеет норму -2 тогда и только тогда, когда $a + b\sqrt{3} = \pm(1 + \sqrt{3})(2 + \sqrt{3})^m$ для некоторого целого m.*

- *Элемент $a + b\sqrt{3}$ имеет норму -3 тогда и только тогда, когда $a + b\sqrt{3} = \pm\sqrt{3}(2 + \sqrt{3})^m$ для некоторого целого m.*

Теперь рассмотрим на прямой, отвечающей кватерниону k, точки пересечения, отвечающие отражениям с помощью кватернионов $ai + bj$, где $a^2 - 3b^2 = -2, -3$. Из леммы следует, что это две бесконечных серии точек, занумерованных целыми числами. Нетрудно проверить, что ближайшей точкой пересечения к точке пересечения прямых, отвечающих k и $i + j$, будет точка пересечения k и j. Заметим, что норма $i + j$ равна -2 а норма j равна -3. Элемент $j + k$ проходит через точку пересечения k и $i + j$, поэтому образует с k угол $\pi/4$.

Докажем что фундаментальный многоугольник имеет стороны $i + j, k, j + k$. Рассмотрим сторону фундаментальной области, лежащую на прямой, отвечающей k. Пусть угол при второй вершине равен pi/n. После n последовательных отражений образ прямой, задаваемой $i + j$, снова будет перпендикулярен к прямой, задаваемой k. Отсюда видно, что точка пересечения прямых, отвечающих k и $j+k$, является вершиной исходного фундаментального многоугольника; и прямая, отвечающая $j + k$ — его сторона. При этом

$$\cos(i + j, j + k) = \frac{\sqrt{3}}{2},$$

откуда третий угол треугольника есть $\pi/6$. Заметим, что сумма углов равна $90 + 45 + 30 = 165 < 180$ и это действительно треугольник в пространстве Лобачевского. Таким образом, фундаментальный многогранник - это треугольник с нормалями к сторонам $k, i + j, j + k$, чьи нормы суть $-3, -2, -6$ соответственно, и с углами $\pi/2, \pi/4, \pi/6$.

Список литературы

[1] Gaчtan Chenevier, course trimestre Galoisien 2010, lecture notes.

[2] Stefan Johansson, “A Description of Quaternion Algebras”.

[3] Maclachlan, Colin; Reid, Alan W. (2003), The arithmetic of hyperbolic 3-manifolds, Graduate Texts in Mathematics, 219, Berlin, New York.

[4] Serr J.P. A course in arithmetic (Springer, 1996).