МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра геометрии

Кольца представлений алгебры Ли sl(2)

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 227 группы
направления 02.04.01 Математика и компьютерные науки
механико-математического факультета

Филиной Татьяны Максимовны

Научный руководитель
профессор, д.ф.-м.н., доцент ____________________ А.Н. Сергеев
подпись, дата

И.о. зав. кафедрой
к.п.н., доцент ____________________ А.В. Букушева
подпись, дата

Саратов 2024

ВВЕДЕНИЕ

Актуальность работы. Алгебры Ли занимают значительное место в современной математике. Их теория отличается исключительной полнотой в понимании структурных аспектов, особенно в классе конечномерных алгебр Ли. Простые алгебры Ли над полем характеристики нуль используются в криптографии для создания криптосистем с открытым ключом. Эти системы полагаются на сложность задачи факторизации целых чисел, а их безопасность обеспечивается структурой алгебр Ли.

Цель работы:

1) рассмотреть полупростые алгебры;

2) рассмотреть основные свойства алгебр Ли;

3) изучить $sl(2)$-модули;

4) изучить представление кольца Ли sl_2.

Описание структуры работы. Выпускная квалификационная работа состоит из введения, семи глав, заключения, списка использованных источников, содержащего 23 наименований. Работа содержит 40 страниц.

Краткая характеристика материалов работы. Работа носит реферативный характер и основана на источниках, указанных в списке литературы. Часть результатов доказана самостоятельно.

Научная новизна и значимость работы. Научная значимость работы состоит в кодировании, где Алгебры Ли используются для разработки кодов с открытым и закрытым ключом, обеспечивающих безопасную передачу информации.

Положения, выносимые на защиту. На защиту выносится следующий результат - самостоятельное доказательство ряда результатов, приведенных в работе.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

1 Ассоциативные алгебры

Определение 1.1. Ассоциативная алгебра над полем $\mathbb{C}$, это вектор-ное пространство над C вместе с билинейным отображением A×A →A и элементом $1 \in A$ таким, что

$$(ab)c = a(bc)$$
$$1a = a1 = a$$

То есть мы всегда рассматриваем алгебры с единицей.

Пример 1.1. Алгебра матриц.

Пример 1.2. Пусть A - алгебра матриц и $X \in A$. Рассмотрим множество всех матриц которые коммутируют с матрицей X. Показать, что такие матрицы образуют алгебру.

Пример 1.3. Пусть $A = Mat_2(R)$ и $X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ Показать, что в этом случае множество матриц коммутирующих с X, это множество матриц вида

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \ a, b \in \mathbb{R}$$

Пример 1.4. Вычислить централизатор диагональной матрицы и Жордановой клетки при разных разметрах и значениях параметров.

Пример 1.5. Аналогичным образом можно описать алгебру кватернионов как централизатор, двух 4×4 матриц.

Пример 1.6. Алгебра линейных преобразований векторного пространства.

Замечание 1.1. Примеры с матрицами можно перевести на языклинейных операторов. Полезно также привести примеры множеств с умножением которые не удовлетворяют аксиомам алгебры.

2 Обертывающая алгебра алгебры Ли sl(2)

Определение 2.1 Универсальной обертывающей алгеброй алгебры Ли sl(2), называется алгебра обозначаемая $U(sl(2))$, которая порождена образующими X, H, Y и соотношениями:

$$XY - YX = H, HY - YH = 2Y, HX - XH = 2X$$

Лемма 2.2 (Универсальное свойство). Пусть A - ассоциативная алгебра и A, B, C три элемента таких, что

$$AC - CA = B, BC - CB = 2A, BA - AB = 2A,$$

тогда существует и единственный гомоморфизм ассоциативных алгебр

$$\phi : U(sl(2)) \to A$$

такой, что

$$\phi(X) = A, \phi(X) = B, \phi(Y) = C$$

3 Алгебры Ли

Определение 3.1. Алгеброй Ли называется векторное пространство V наделенное умножением, которое обозначается $[a, b]$ и обладает свойствами:

1) Билинейность.

$$[\lambda a, b] = [a, \lambda b] = \lambda[a, b]$$
$$[a_1 + a_2, b] = [a_1, b] + [a_2, b]$$
$$[a, b_1 + b_2] = [a, b_1] + [a, b_2],$$

где λ - комплексное число.

2) Кососимметричность.

$$[b, a] = -[a, b]$$

3) Тождество Якоби.

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$$

Полезно рассмотреть все основные свойства алгебр Ли на простейшем нетривиальном примере алгебры Ли $sl(2)$.

Определение 3.2. Алгеброй Ли $sl(2)$ называется трехмерная алгебра Ли с таблицей умножения

$$[XY] = H, [HY] = -2Y, [HX] = 2X.$$

Лемма 3.1. Алгебра Ли $sl(2)$ изоморфна подалгебре в алгебре матриц 2×2 имеющих след нуль (сумма диагональных элементов равна нулю).

Доказательство. Изоморфизм задается по правилу

$$X \to \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, Y \to \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, H \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

□

Лемма 3.2. Алгебра Ли $sl(2)$ изоморфна алгебре векторов трехмерного пространства с векторным умножением.

Доказательство. Напомним таблицу умножения векторов

$$[e_1, e_2] = e_3, [e_1, e_3] = -e_2, [e_2, e_3] = e_1.$$

Изоморфизм задается по правилу

$$X \to ie_2 - e_1, Y \to ie_2 + e_1, H \to -2ie_3.$$

□

4 sl(2) - модули

В этом разделе будем считать, что $\mathbb{K}$ - произвольное поле характеристики нуль. Векторное пространство g называется *алгеброй Ли*, если на нём задана билинейная операция «скобка» [*,*] : $g \times g \to g$, удовлетворяющая тождеству Якоби:

$$\forall X, Y, Z : [X, [Y, Z]] = [[X, Y], Z] + [Y, [X, Z]].$$

Например, на любой ассоциативной алгебре A над полем $\mathbb{K}$ имеется структура алгебры Ли, задаваемая коммутатором $[a, b] = ab - ba$.

Эта алгебра Ли называется коммутаторной алгеброй ассоциативной алгебры A. Наоборот, для любой алгебры Ли g имеется единственная ассоциативная алгебра $\Psi(g)$ и линейное отображение $v : g \to \Psi(g)$, для любых

$X, Y \in g$ переводящее $[X, Y]$ в $v(X)v(Y) - v(Y)v(X)$, такие что каждое линейное отображение $\psi : g \to A$ в ассоциативную алгебру, переводящее скобку в коммутатор, однозначно представляется в виде $\psi = \tilde{\psi} \cdot v$, где $\tilde{\psi} : \Psi(g) \to A$ — гомоморфизм ассоциативных алгебр.

Ассоциативная алгебра $\Psi(g)$ называется *универсальной обёртывающей* алгеброй алгебры Ли g. Её можно построить как фактор тензорной алгебры $T(g)$ по двустороннему идеалу, порождённому всевозможными разностями

$$X \otimes Y - Y \otimes X - [X, Y] \in g^{\otimes 2} \otimes g.$$

Линейное отображение $\sigma : g \to End(V)$ называется представлением алгебры Ли g, если оно переводит скобку в коммутатор, т. е. $\sigma([A, B]) = [\sigma(A), \sigma(B)]$. Пространство V называется в этой ситуации g-модулем. В силу универсального свойства универсальной обёртывающей алгебры, линейные представления алгебры Ли $\sigma : g \to End(V)$ биективно соответствуют гомоморфизмам ассоциативных алгебр $\tilde{\sigma} : \Psi(g) \to End(V)$, т. е. линейным представлениям ассоциативной алгебры $\Psi(g)$. Представление $\tilde{\sigma}$ отображает класс тензора $A_1 \otimes A_2 \otimes ... \otimes A_m$ в композицию $\sigma(A_1) \cdot \sigma(A_2) \cdot ... \cdot \sigma(A_m)$, и его образ совпадает с ассоциативной оболочкой

$$Ass(\sigma(g)) \subset End(V).$$

5 Теория представлений алгебры sl(2)

Рассмотрим алгебру Ли sl_2 матриц 2×2 со следом 0. Эта алгебра трехмерна.

Стандартный базис:

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Коммутационные соотношения:

$$[e, f] = h, [h, e] = 2e, [h, f] = -2f. \tag{4}$$

Замечание 5.1. Пусть g — алгебра Ли. $0 \neq e, f, h \in g$ и удовлетворяют соотношениям (4). $\Longrightarrow e, f, h$ линейно независимы.
Кроме того, $g \subseteq \langle e, f, h \rangle \simeq sl_2$. ($sl_2$–тройка).

Пусть $K = C$. Пусть $\rho : sl_2 \to gl(v)$ — C–линейное представление. Элемент h полупрост $\Longrightarrow \rho(h)$ полупрост $\Longrightarrow V = \oplus_\lambda V_\lambda$, где V_λ - собственное подпространство для $\rho(h)$ с собственным значением $\lambda \in C$.

Лемма 5.1. Имеем $\rho(e)V_\lambda \subseteq V_{\lambda+2}$, $\rho(f)V_\lambda \subseteq V_{\lambda-2}$ ($\rho(e)$ — повышающий оператор, а $\rho(f)$ — понижающий оператор).

Доказательство. Доказательство проводится непосредственной проверкой. $v \in V_\lambda$, $\omega = \rho(e)v$.

$$\rho(e)\omega = \rho(h)\rho(e)v = \rho(e)\rho(h)v + [\rho(h), \rho(e)]v = \rho(e)\lambda v + \rho([h, e])v = (\lambda + 2)\omega$$

$\Longrightarrow \omega \in V_{\lambda+2}$. Аналогично для $\rho(f)$. □

Следствие 5.1. Существует $v \in V, v \neq 0$ такой, что $\rho(h)v = \lambda v, \rho(e)v = 0$. Этот вектор называется старшим вектором. Аналогично, младший вектор — собственный для $\rho(h)$, аннулируется $\rho(f)$.

Лемма 5.2. Пусть v - старший вектор,

$$v' = \rho(f)v, v'' = \rho(f)v', ..., v^{(k)} = \rho(f)v^{(k-1)}, ...$$

Тогда
1. $\rho(h)v^{(k)} = (\lambda - 2k)v^{(k)}$,
$\rho(e)v^{(k)} = k(\lambda - k + 1)v^{(k-1)}$,
$\rho(f)v^{(k)} = v^{(k+1)}$.
2. $\exists n \geq 0 : v, v', ..., v^{(n)}$ - линейно независимы, $v^{(n+1)} = v^{(n+2)} = ... = 0$.
3. $\lambda = n$
4. $U = \langle v, v', ..., v^{(n)} \rangle$ - неприводимое инвариантное подпространство в V.

Доказательство.

1. Нетривиально только второе равенство. Докажем, что $\rho(e)v^{(k)} = c_{k-1}v^{(k-1)}$ индукцией по k.

База $k = 1$:

$$\rho(e)v' = \rho(e)\rho(f)v = \rho(f)\rho(e)v + \rho([e, f])v = \lambda v, c_0 = \lambda$$

Шаг (от k к $k + 1$):

$$\rho(e)v^{(k+1)} = \rho(e)\rho(f)v^{(k)} = \rho(f)\rho(e)v^{(k)} + \rho(h)v^{(k)} = (c_{k-1} + \lambda - 2k)v^{(k)} = c_k v^{(k)}.$$

Итак, $c_k = \lambda + (\lambda - 2) + (\lambda - 4) + ... + (\lambda - 2k) = (k + 1)(\lambda - k)$. Делая сдвиг на единицу, получим формулу из условия леммы.

2. Существует такое n, что $v, v', ..., v^{(n)} \neq 0, v^{(n+1)} = v^{(n+2)} = ... = 0$. А все ненулевые векторы — это собственные векторы для $\rho(h)$ с разными собственными значениями $\Longrightarrow$ линейно независимы.

3. $0 = \rho(e)v^{(n+1)} = (n + 1)(\lambda - n)v^{(n)}, \Longrightarrow \lambda - n = 0 \Longrightarrow \lambda = n.$

4. Любое ненулевое инвариантное подпространство $W \subseteq U$ содержит собственный вектор для $\rho(h)$. А собственные векторы для $\rho(h)$ в U — это только векторы из цепочки $v, v', ..., v^{(n)}$ и их линейные комбинации. $\exists k : v^{(k)} \in W$. Следовательно, в W содержатся и остальные векторы, так как их можно получить с помощью понижающих и повышающих операторов $\rho(e)$ и $\rho(f)$ из $v^{(k)} \Longrightarrow W = U$, и тем самым доказана неприводимость. □

6 Категория ϑ

Определение 6.1. Множество объектов $M \in \vartheta$ тогда и только тогда, когда:

1) M конечномерное, порожденное как $U(sl(2))$;

2) M полупросто как H;

3) $\forall v \in M$, $dim\langle v, xv, ..\rangle < +\infty$.

Лемма 6.1. Справедливо следующее утверждение:

1) $\forall \lambda \in \mathbb{C}$ пространство $M^\lambda = \{v \in M | Hv = \lambda v\}$ - конечномерно.

2) Множество $\lambda : M^\lambda \neq 0$ содержится в конечном объединении множеств $\bigcup_{i=1}^n (\lambda_i - 2z)$.

Теорема 6.1. 1) Любой простой модуль в ϑ изоморфен $L(\lambda), \lambda \in \mathbb{C}$.

2) Если $\lambda \in \mathbb{Z}_{\geq 0}$, то $M(\lambda)$ приводим $M(\lambda) \supset M(-\lambda - 2)$ и $L(\lambda) = M(\lambda)/M(-\lambda - 2)$.

Лемма 6.2. пространство $How(M, N)$ - конечномерно.

Все конечномерные неприводимые представления алгебры Ли $sl_2(C)$ (или $sl_2(C)$-модули) обладают следующим свойством:

1) Оператор $\rho(h)$ действует полупросто, т.е. пространство представления имеет базис из собственных веторов оператора $\rho(h)$.

2) Оператор $\rho(e)$ действует локально нильпотентно, т.е. для любого вектора v существует такое натуральное число k, что $\rho(e)^k v = 0$.

Категория конечнопорожденных $sl_2(C)$-модулей с такими свойствами называется категорией ϑ.

Примером бесконечномерного объекта этой категории является модуль Верма со старшим весом λ: это векторное пространство с базисом $v_\lambda^{(k)}$, $k = 0, 1, 2, ...$, в элементы алгебры Ли действуют следующим образом:

$$\rho(e)v_\lambda^{(k)} = (k\lambda - k(k-1))v_\lambda^{(k-1)}, \rho(f)v_\lambda^{(k)} = v_\lambda^{(k+1)}, \rho(h)v_\lambda^{(k)} = (\lambda - 2k)v_\lambda^{(k)}.$$

7 Представления кольца Ли $sl_2(Z)$

Рассматриваются конечномерные $sl_2(Z)$ - модули.

Положим $R = sl_2(Z)$. Обозначим через ϑ категорию $sl_2(Z)$ - модулей конечного типа без кручения. Пусть $M \in \vartheta$, тогда $M_Q = M \otimes_Z Q$ будет конечномерным $sl_2(Q)$ - модулем, причем $dimM = dim_Q(M_Q)$. Определим также $sl_2(Z_p)$ - модуль $M_p = M \otimes_Z Z_p$, где Z_p - кольцо целых p - адических чисел.

Зафиксируем в R стандартный базис $\{e, h, f\}$, где

$$eh = 2e, ef = h, fh = -f.$$

Введем обозначение: $M = \langle \omega_0, ..., \omega_k \rangle$, если элементы $\omega_0, ..., \omega_k$ образуют базис модуля M.

Пусть V - $sl_2(Q)$. Выберем в нем некоторый базис $\langle \omega_0, ..., \omega_k \rangle$ так, чтобы действие e, h, f определялось с целыми коэффициентами. Тогда мы можем рассмотреть R - модуль $V_Z = \langle \omega_0, ..., \omega_k \rangle$, который будем называть редукцией модуля V по базису $\omega_0, ..., \omega_k$.

R - модуль M будем называть неприводимым, если соответствующий $sl_2(Q)$ - модуль $M_Q = M \otimes_Z Q$ неприводим.

Хорошо известно, что существует единственный неприводимый $(m+1)$ - мерный M_Q - модуль V_Q, который можно задать, например, следующим образом: $V_Q = \langle v_0, ..., v_m \rangle$, где

$$v_i e = v_{i+1}, v_m e = 0, v_i h = (m-2i)v_i, v_i f = -i(m-i+1)v_{i-1}.$$

Редукцию модуля V_Q по этому базису обозначим буквой V и назовем стандартным R - модулем размерности $m+1$. Пусть $M \in \vartheta$ произвольный неприводимый $(m+1)$ - мерный модуль, тогда $M_Q \cong V_Q$.

Модуль D назовем диагональным, если он имеет базис из собственных векторов h, т.е. $D = \langle d_0, ..., d_s | \exists k_i \in Z : d_i h = k_i d_i \rangle$. Заметим, что если M неприводимый, то M_d также неприводим.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Сергеев А.Н. Алгебры Ли / Сергеев А.Н. // Учебное пособие (2014).

2 Серр Ж.П. Алгебры Ли и группы Ли / Ж.П. Серр // – М.: «Мир». – 1969. - 376 с.

3 Бахтурин Ю.А. Тождества в алгебрах Ли / Ю.А. Бахтурин // – М.: «Наука». – 1985. 450 с.

4 Хамрис Дж. Введение в теорию алгебр Ли и их представление / Дж. Хамрис // – М.: «МЦНМО». – 2003. - 216с.

5 Бурбаки Н. Группы и алгебры Ли / Н. Бурбаки // – М.: «Мир». 1976. 495 с.

6 Джекобсон Н. Алгебры Ли / Н. Джекобсон // – М.: «Мир». 1964. - 358 с.

7 Капланский И. Алгебры Ли и локально компактные группы / И. Капланский // – М.: «Мир». 1974. - 152 с.

8 Размыслов Ю.П. Тождества алгебр и их представления / Ю.П. Размыслов // – М.: «Наука». – 1989. - 433 с.

9 Скорняков Л.А. Элементы теории структур / Л.А. Скорняков // – М.: «Наука». – 1970. - 150 с.

10 Березин Ф.А. Введение в алгебру и анализ с антикоммутирующими переменными / Ф.А. Березин // М.: «Издательство МГУ». – 1983. 205 с.

11 Готто М., Гроссханс Ф. Полупростые алгебры Ли / М. Готто, Ф. Гроссханс // - М.: Мир, 1981. — 171 с.

12 Пирс Р. Ассоциативные алгебры / Пирс Р.// – М.: Мир, 1986. – 541 с.