МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

АЛГЕБРА-4

ТИМАШЕВ
ДМИТРИЙ АНДРЕЕВИЧ

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

Оглавление

Лекция 1. Теория полей. ... 6
Теория полей ... 6
Некоторые факты о расширениях полей ... 8
Предложение 1 ... 8
Автоморфизмы расширения полей ... 9
Упражнение ... 9
Теорема ... 9
Лекция 2. Автоморфизмы расширения полей. ... 10
Теорема 1 ... 10
Предложение 1 ... 10
Предложение 2 ... 11
Предложение 3 ... 11
Расширения Галуа ... 13
Лекция 3. Основная теорема теории Галуа. ... 14
Теорема 1 ... 14
Теорема 2 ... 15
Основная теорема теории Галуа ... 15
Теорема о примитивном элементе ... 17
Решение алгебраических уравнений в радикалах ... 17
Теорема Галуа ... 17
Лекция 4. Теорема Галуа. ... 18
Теорема Галуа ... 18
Лемма 1 ... 18
Лемма 2 ... 18
Лемма 3 ... 18
Лемма 4 ... 19
Решение общего уравнения степени n в радикалах ... 21
Лекция 5. Кольца, алгебры, модули. ... 22
Кольца, алгебры, модули ... 22
Примеры модулей ... 25
Лекция 6. Общие теоретико-модульные конструкции. ... 28
Универсальное свойство прямой суммы ... 28

Предложение 1 ... 29
Предложение 2 ... 30
Примеры и свойства тензорного произведения ... 32
Лекция 7. Свойства тензорного произведения. ... 35
Свойства тензорного произведения (продолжение) ... 35
Универсальное свойство тензорного произведения ... 35
Структура колец / модулей ... 39
Нётеровы модули ... 39
Предложение 1 ... 39
Предложение 2 ... 40
Лекция 8. Нётеровы кольца. ... 42
Предложение 1 ... 42
Предложение 2 ... 42
Теорема Гильберта о базисе идеала ... 42
Теорема ... 44
Конечно порожденные модули над кольцами главных идеалов ... 45
Предложение 3 ... 45
Лекция 9. Основная теорема о структуре конечно порожденных модулей над кольцом главных идеалов. ... 47
Теорема ... 48
Приложения теоремы ... 51
Лекция 10. Теория представлений. ... 53
Нормальная форма Фробениуса линейного оператора ... 53
Теория представлений ... 54
Терминология ... 55
Предложение ... 57
Теорема ... 58
Лекция 11. Лемма Шура. Тензорное произведение представлений групп. ... 60
Лемма Шура ... 60
Предложение 1 ... 61
Предложение 2 ... 62
Тензорное произведение представлений групп ... 63
Предложение 3 ... 64
Лекция 12. Конечномерные ассоциативные алгебры и их представления. ... 66

Нильпотентные алгебры ... 66
Лемма 1 ... 67
Лемма 2 ... 67
Радикал ... 68
Стандартное скалярное умножение ... 68
Лемма 3 ... 68
Теорема ... 69
Лемма 4 ... 69
Лекция 13. Структура полупростых алгебр. Теорема Бернсайда. ... 71
Предложение 1 ... 71
Полупростые алгебры ... 71
Структура полупростых алгебр ... 72
Предложение 2 ... 73
Теорема Бернсайда ... 74
Лекция 14. Структура простых и полупростых алгебр. ... 76
Теорема Веддербёрна ... 76
Теорема Веддербёрна - Артина ... 76
Предложение 1 ... 77
Представления групп с точки зрения ассоциативных алгебр ... 78
Предложение 2 ... 79
Теорема Машке ... 80
Лекция 15. Группы Ли и алгебры Ли. ... 82
Примеры групп Ли ... 83
Предложение 1 ... 83
Примеры групп Ли ... 86
Лекция 16. Свойства групп Ли. ... 88
Предложение 1 ... 88
Теорема 1 ... 88
Предложение 2 ... 90
Алгебра Ли ... 91
Теорема 2 ... 92
Примеры касательных алгебр Ли ... 93
Лекция 17. Экспоненциальное отображение. ... 94
Экспоненциальное отображение ... 94

Теорема ... 96
Предложение 1 ... 96
Предложение 2 ... 96
Предложение 3 ... 97
Линейные представления групп Ли ... 98
Предложение 4 ... 98
Лекция 18. Линейные представления алгебр Ли. ... 99
Линейные представления алгебр Ли ... 99
Присоединенное представление ... 99
Теорема 1 ... 100
Теорема 2 ... 102
Предложение ... 103
Лекция 19. Линейные представления компактных групп Ли. ... 104
Линейные представления компактных групп Ли ... 104
Теорема 1 ... 104
Выпуклые множества ... 104
Свойства выпуклых тел ... 104
Предложение 1 ... 107
Предложение 2 ... 110
Лекция 20. Представления $SL2(\mathbb{C})$ и $\mathfrak{sl}2(\mathbb{C})$. ... 111
Унитарный трюк Г. Вейля ... 111
Представления $SL2(\mathbb{C})$ и $\mathfrak{sl}2(\mathbb{C})$ (над $\mathbb{C}$) ... 111
Теорема 1 ... 113
Гармонический анализ на сфере ... 116
Лекция 21. Универсальная обертывающая алгебра. ... 117
Гармонический анализ на сфере (продолжение) ... 117
Универсальная обертывающая алгебра ... 118
Предложение ... 119
Лекция 22. Теорема Пуанкаре-Бирхгофа-Витта. Алгебра Клиффорда. ... 122
Теорема Пуанкаре–Бирхгофа–Витта ... 122
Алгебра Клиффорда ... 124
Предложение 1 ... 125
Соотношения в алгебре Клиффорда ... 126
Лекция 23. Свойства алгебры Клиффорда. Спинорная группа. ... 128

Предложение 1 128
Теорема 1 129
Теорема 2 131
Пространство спиноров 132
Модель спинорного представления 133
Спинорная группа 134
Предложение 2 135
Спинорная норма 136
Теорема 3 136

Лекция 1. Теория полей.

Этот курс читается на мехмате, на потоке “Фундаментальная математика и математическая физика”, и отличается от стандартного курса алгебры, обычно читающегося на мехмате. Содержание будет ближе скорее к спецкурсу “Дополнительные главы алгебры” кафедры Высшей алгебры мехмата.

Рекомендуемая литература:

1. Винберг Э.Б. Курс алгебры. – М.: МЦНМО, 2017.
2. Кострикин А.И. Введение в алгебру, ч. III: Основные структуры. – М.: Физматлит, 2001.
3. Бахтурин Ю.А. Основные структуры современной алгебры. – М.: Наука, 1990.
4. Ленг С. Алгебра. – М.: Мир, 1968.
5. Ван дер Варден Б.Л. Алгебра. – М.: Мир, 1976.

Информацию по курсу можно найти на следующих ресурсах:

- http://halgebra.math.msu.su/wiki/doku.php/%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0_3_%D0%BA%D1%83%D1%80%D1%81_%D1%84%D0%BC%D0%BC%D1%84_%D0%BE%D1%81%D0%B5%D0%BD%D1%8C_2022
- https://fmmp.math.msu.ru/courses/algebra-1

Чтобы сохранить преемственность с курсом “Алгебра-3” https://teach-in.ru/course/algebra-letctures-p2-timashev, начнем с продолжения темы, которой мы закончили прошлый семестр – теории полей.

Теория полей

Определение. *Поле* – это коммутативное ассоциативное кольцо K с 1, в котором любой ненулевой элемент обратим (и в котором больше одного элемента).

Примеры полей: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ (p-простое), конечные поля $\mathbb{F}_q$ ($q = p^n$, p-простое).

Определение. *Характеристика* поля $char\, K$ – это наименьшее $p \in \mathbb{N}$, такое что $\underbrace{1 + \cdots + 1}_{p \text{ слагаемых}} = 0$, или 0, если такого p не существует.

Примеры: $char\, \mathbb{Q} = char\, \mathbb{R} = char\, \mathbb{C} = 0$, $char\, \mathbb{F}_q = p$ при $q = p^n$, p-простое.

Имеет место следующий факт: если $char\, K = p > 0$, то p-простое. Отметим, что поля положительной характеристики p (к которым, в частности, относятся все конечные поля)

обладают одним необычным свойством – в таких полях операция возведения в степень p является гомоморфизмом (т.е. переводит не только произведение в произведение, но и сумму в сумму). Этот гомоморфизм называется гомоморфизмом (эндоморфизмом) Фробениуса.

Свойство (эндоморфизм Фробениуса). Пусть $char\ K = p > 0$. Тогда $\forall a, b \in K$:

- $(a \pm b)^p = a^p \pm b^p$
- $(ab)^p = a^p b^p$

- *эндоморфизм Фробениуса:*

$$\Phi\colon\ K \to K$$
$$a \mapsto a^p$$

Отметим, что Φ инъективен:

$$a^p = b^p \Longrightarrow a^p - b^p = 0 \Longrightarrow (a-b)^p = 0 \Longrightarrow a - b = 0 \Longrightarrow a = b$$

А если K – конечное поле, то Φ – автоморфизм (так как инъективное отображение конечного множества в себя является также и сюръективным).

Определение 1. Поле K *совершенно*, если либо $char\ K = 0$, либо $char\ K = p > 0$, и $\forall a \in K\ \ \exists b \in K\colon\ b^p = a$.

Пример. $\mathbb{F}_q$ совершенно (так как инъективное отображение $\Phi\colon\ \mathbb{F}_q \to \mathbb{F}_q$ автоматически сюръективно).

Пусть L – поле, $K \subset L$ – подполе. Говорят, что L – *расширение* поля K. В этом случае L – векторное пространство над K. Расширение полей $K \subset L$ называется конечным, если L конечномерно над K. *Степень расширения* $(L\colon K) = dim_K L$.

Наряду с конечными расширениями в теории полей рассматриваются *конечно порожденные расширения*. Пусть $K \subset L$ – расширение полей и $a_1, \dots, a_s \in L$. Расширение поля K, порожденное элементами $a_1, \dots, a_s$ – это наименьшее подполе $M \subset L$, такое что $M \supseteq K$ и $M \ni a_1, \dots, a_s$ (иными словами, это пересечение всех подполей, содержащих K и $a_1, \dots, a_s$). Обозначение: $M = K(a_1, \dots, a_s)$.

Конструктивное описание:

$$K(a_1, \dots, a_n) = \left\{ \frac{f(a_1, \dots, a_s)}{g(a_1, \dots, a_s)} \mid f, g \in K[x_1, \dots, x_s],\ \ g(a_1, \dots, a_s) \neq 0 \right\}$$

Простое расширение: $L = K(a)$, a – примитивный элемент расширения.

Примеры простого расширения полей:

1) $\mathbb{C} = \mathbb{R}(i)$, степень расширения: $(\mathbb{C}:\mathbb{R}) = 2$

2) $\mathbb{F}_q \supseteq \mathbb{F}_p \simeq \mathbb{Z}_p$ $(q = p^n,\ p = char\ \mathbb{F}_q)$ – конечное расширение, степень расширения: $(\mathbb{F}_q:\mathbb{F}_p) = n$. Это простое расширение: мультипликативная группа $\mathbb{F}_q^\times = < a >$ - циклическая, поэтому $\mathbb{F}_q = \mathbb{F}_p(a)$

3) Поле рациональных дробей $L = K(t)$ (t - переменная) – бесконечное расширение K (так как $1, t, t^2, \dots, t^n, \dots$ линейно независимы над K)

Некоторые факты о расширениях полей

1) $(K(a):K) < \infty \Leftrightarrow a$ *алгебраичен* над K, т.е. $\exists f \in K[x]$, $\deg f > 0$, $f(a) = 0$.

2) В этом случае $(K(a):K) = n$ – степень минимального многочлена $\mu_a(x) \in K[x]$ и $\{1, a, a^2, \dots, a^n\}$ – базис $K(a)$ над K. При этом $\mu_a(x)$ неприводим в $K[x]$.

3) Обратно, $\forall$ неприводимого $f \in K[x]$ $\exists$ простое расширение $L = K(a) \supset K$, $f(a) = 0$. При этом $f = c\mu_a$ $(c \in K^\times)$. L единственно с точность до изоморфизма.

Конструкция: $L = K[x]/f \cdot K[x]$, $\quad a = x + f \cdot K[x]$ (*присоединение корня*).

Расширение $L \supset K$ *алгебраично*, если $\forall a \in L$ алгебраичен над K.

Предложение 1. Следующие условия эквивалентны:
1) $L \supseteq K$ – конечное расширение,
2) $L \supseteq K$ – конечно порожденное алгебраическое расширение,
3) $L = K(a_1, \dots, a_s)$, где $a_1, \dots, a_s$ алгебраичны над K.

Доказательство.
1) $\Longrightarrow$ 2): пусть $b_1, \dots, b_n$ – базис L над K, тогда $L = K(b_1, \dots, b_n)$, т.е. всякое конечное расширение является конечно порожденным. Также оно является алгебраическим: $\forall a \in L$: $K \subseteq K(a) \subseteq L \Longrightarrow K(a)$ – векторное подпространство в L над K, откуда следует, что $(K(a):K) \leq (L:K) = n < \infty \Longrightarrow a$ алгебраичен над K.

2) $\Longrightarrow$ 3): тривиально.

3) $\Longrightarrow$ 1): введем обозначения:

$$K_0 = K, K_1 = K(a_1), \dots, K_i = K(a_1, \dots, a_i) = K_{i-1}(a_i), \dots, K_s = L$$

Башня простых расширений $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i = K_{i-1}(a_i) \subseteq \cdots \subseteq K_s = L$, a_i алгебраичен над $K_i \Longrightarrow$ и над $K_{i-1} \Longrightarrow (K_i : K_{i-1}) < \infty$. Из теоремы о башне расширений следует, что $(L:K) = (K_s : K_{s-1}) \cdot \ldots \cdot (K_i : K_{i-1}) \cdot \ldots \cdot (K_1 : K_0) < \infty$. ■

Автоморфизмы расширения полей.

Для изучения любой алгебраической структуры полезно знать, как устроены ее автоморфизмы. Расширение полей не является исключением. Пусть $L \supseteq K$ – расширение полей.

Определение. *Автоморфизм расширения* – это такой изоморфизм $\varphi\colon L \twoheadrightarrow L$, что $\varphi(a) = a, \forall a \in K$. Группа автоморфизмов расширения полей:

$$Aut\ (L/K) = \{\varphi\colon\ L \twoheadrightarrow L \mid \varphi(a) = a, \forall a \in K\}$$

Пример. $Aut\ (\mathbb{C}/\mathbb{R}) = \{id, \sigma\}$, где σ- комплексное сопряжение: $\sigma(z) = \bar{z}$.

Действительно, $\mathbb{C} = \mathbb{R}(i)$, поэтому любой элемент $\varphi \in Aut\ (\mathbb{C}/\mathbb{R})$ полностью определяется своим действием на i. Но $-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$, т.е. $\varphi(i)$ является корнем из -1 и равно либо i (и тогда $\varphi = id$), либо $-i$ (и тогда $\varphi = \sigma$).

Упражнение. Вычислить $Aut\ (\mathbb{R}/\mathbb{Q})$.

Далее будем рассматривать конечные расширения полей: $(L:K) = n < \infty$. Введем некоторые полезные обозначения:

- Группу автоморфизмов такого расширения для краткости обозначим $Aut\ (L/K) = G$.
- $\forall H \subseteq G$ обозначим $L^H = \{a \in L \mid h(a) = a,\ \forall h \in H\}$ – множество элементов L, которые остаются неподвижными под действием автоморфизмов из H (*поле инвариантов* H). Это подполе в L, содержащее K.

Теорема. Пусть $L \supseteq K$ – конечное расширение полей, $(L:K) = n$, $Aut\ (L/K) = G$. Тогда:
1) $|G| \leq n$,
2) $|G| = n \Leftrightarrow L^G = K$.

Определение. *Расширение Галуа* – это конечное расширение $L \supseteq K$, для которого $|Aut\ (L/K)| = (L:K)$. В этом случае группа $Aut\ (L/K)$ называется группой Галуа расширения и обозначается $Gal\ (L/K)$.

Пример. $\mathbb{C} \supset \mathbb{R}$ - расширение Галуа.

Лекция 2. Автоморфизмы расширения полей.

Теорема 1. Пусть $L \supseteq K$ – конечное расширение полей, $(L:K) = n$, $Aut\,(L/K) = G$. Тогда:
1) $|G| \leq n$,
2) $|G| = n \Leftrightarrow L^G = K$.

Доказательство.

Лемма 1. Пусть $F \subset F(a)$ – простое алгебраическое расширение и $\mu(x) = x^n + \mathrm{c}_1 x^{n-1} + \cdots + \mathrm{c}_n \in F[x]$ – минимальный многочлен a. Тогда любой гомоморфизм φ: $F \to E$ продолжается до гомоморфизма $\tilde{\varphi}$: $F(a) \to E$ столькими способами, сколько корней в поле E имеет многочлен ${}^{\varphi}\mu(x) = x^n + \varphi(\mathrm{c}_1)x^{n-1} + \cdots + \varphi(\mathrm{c}_n)$.

Набросок доказательства леммы.
$\forall b \in F(a)$ имеет вид $b = f(a) = a_0 + a_1 a + \cdots + a_m a^m$ для некоторого многочлена $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in F[x]$. Следовательно,

$$\tilde{\varphi}(b) = \tilde{\varphi}(a_0 + a_1 a + \cdots + a_m a^m) =$$
$$= \varphi(a_0) + \varphi(a_1)\tilde{\varphi}(a) + \cdots + \varphi(a_m)\tilde{\varphi}(a)^m = {}^{\varphi}f\big(\tilde{\varphi}(a)\big),$$

Т.е гомоморфизм $\tilde{\varphi}$: $F(a) \to E$ однозначно задается образом элемента a. С другой стороны, $\mu(a) = 0$, следовательно, $\tilde{\varphi}\big(\mu(a)\big) = {}^{\varphi}\mu\big(\tilde{\varphi}(a)\big) = 0$, т.е. $\tilde{\varphi}(a)$ – корень ${}^{\varphi}\mu$.

Обратно, для любого корня $\tilde{a} \in E$ многочлена ${}^{\varphi}\mu$ продолжение $\tilde{\varphi}$ корректно определяется формулой $\tilde{\varphi}\big(f(a)\big) = {}^{\varphi}f(\tilde{a})$. ■

Предложение 1. $|G| \leq n$.

Доказательство предложения 1.
Рассмотрим башню простых расширений $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i = K_{i-1}(a_i) \subseteq \cdots$ $\cdots \subseteq K_s = L$ и поймем, сколько существует автоморфизмов φ: $L \xrightarrow{\sim} L$, которые на поле K действуют тождественно (другими словами, нас интересуют автоморфизмы поля L, которые продолжают тождественный автоморфизм поля K).

Будем продолжать id: $K \xrightarrow{\sim} K$ до автоморфизма φ: $L \xrightarrow{\sim} L$ постепенно. Количество продолжений φ_{i-1}: $K_{i-1} \to L$ до φ_i: $K_i \to L$ по лемме 1 равно числу корней в L многочлена ${}^{\varphi_{i-1}}\mu_i$, где $\mu_i \in K_{i-1}[x]$ – минимальный многочлен a_i над K_{i-1}, т.е. не превосходит $\deg({}^{\varphi_{i-1}}\mu_i) = \deg \mu_i = (K_i : K_{i-1})$.

Отсюда следует, что количество продолжений id_K до $\varphi \in G$, т.е. $|G|$, не превосходит $(K_1:K_0)(K_2:K_1)\cdots(K_s:K_{s-1}) = (L:K) = n$. ■

Предложение 2. Если $|G| = n$, то $L^G = K$.

Доказательство предложения 2.
Заметим, что $G = Aut\ (L/K) = Aut\ (L/L^G)$. Тогда (по предложению 1), $|G| \leq (L:L^G)$. Так как $(L:L^G) \leq (L:K) = n$, получаем, что $|G| \leq (L:K) = n$. Получаем цепочку неравенств:

$$|G| \leq (L:L^G) \leq n = (L:K) = (L:L^G)(L^G:K)$$

Так как $|G| = n$, то все неравенства можно заменить на равенства, тогда из того, что $(L:L^G) = (L:K)$, следует, что $(L:L^G) = n$, поэтому $(L^G:K) = 1$, т.е. $L^G = K$. ■

Лемма 2. Пусть $H \supseteq G$ – подгруппа и $L^H = K$. Для $\forall a \in L$ рассмотрим орбиту $Ha = \{a_1, \dots, a_m\}$. Тогда многочлен $\mu(x) = (x - a_1)\cdots(x - a_m) \in K[x]$ – минимальный многочлен a над K.

Доказательство леммы 2.
Из теоремы Виета следует, что $\mu(x) = x^m + c_1x^{m-1} + \cdots + c_m$, где $c_k = (-1)^k\sigma_k(a_1, \dots, a_m)$, σ_k – элементарный симметрический многочлен. Заметим, что $\forall h \in H$ переставляет $a_1, \dots, a_m$, откуда следует, что $\forall k$: $c_k \in L^H = K$.

Теперь докажем, что μ – минимальный многочлен a над K: пусть $f \in K[x]$, $f(a) = 0$. Тогда $\forall h \in H$: $h(f(a)) = f(h(a)) = 0$, следовательно, $f(a_1) = \cdots = f(a_m) = 0$, и $f \vdots \mu$. ■

Следствие. В условиях леммы $\forall a \in L$ многочлен $\mu_a \in K[x]$ не имеет кратных корней и разлагается на линейные множители над L.

Это следствие оказывается ключевым для завершения доказательства теоремы 1.

Предложение 3. Пусть $H \supseteq G$ – подгруппа и $L^H = K$. Тогда $H = G$ и $|G| = n$.

Доказательство предложения 3.
1) Поймем, сколькими способами можно продолжить тождественный автоморфизм поля K до автоморфизма поля L. Рассмотрим башню простых расширений $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i = K_{i-1}(a_i) \subseteq \cdots \subseteq K_s = L$. Из следствия леммы 2: $\forall i$: $\mu_{a_i} \in K[x]$ имеет $\deg \mu_{a_i}$ различных корней в L.

Рассмотрим μ_i – минимальный многочлен a_i над K_{i-1}. Имеем: $\mu_i \mid \mu_{a_i}$, откуда следует, что количество различных корней μ_i в L равно $\deg \mu_i$. Обозначим $\deg \mu_i = (K_i : K_{i-1}) = n_i$. По лемме 1, существует n_i способов продолжить любой гомоморфизм φ_{i-1}: $K_{i-1} \to L$ до гомоморфизма φ_i: $K_i \to L$ (воспользовались тем, что $\mu_i, \mu_{a_i} \in K_{i-1}[x]$ и ${}^{\varphi_{i-1}}\mu_i, {}^{\varphi_{i-1}}\mu_{a_i} \in \varphi_{i-1}(K_{i-1})[x]$, и ${}^{\varphi_{i-1}}\mu_{a_i} = \mu_{a_i}$, если $\varphi_{i-1}|_K = id$, откуда следует, что ${}^{\varphi_{i-1}}\mu_i$ имеет $\deg \mu_i$ корней в L). Следовательно, $|G| = n_1 n_2 \cdots n_s = n$ (по теореме о башне расширений).

2) Пусть $g \in G$. Тогда $\forall a \in L$: $\mu_a(x) = (x - a_1) \cdots (x - a_m)$, где $\{a_1, \dots, a_m\} \in Ha$ (по лемме 2). Так как $\mu_a(a) = 0$, то и $\mu_a\big(g(a)\big) = 0$ – другими словами, образ элемента $a \in L$ при любом автоморфизме расширения поля тоже будет корнем минимального многочлена a. Но если $g(a)$ – корень, тогда $g(a) \in \{a_1, \dots, a_m\}$, т.е. $\exists h \in H$: $h(a) = g(a) \Leftrightarrow g^{-1}h(a) = a$. Следовательно,

$$L = \bigcup_{h \in H} L^{g^{-1}h}$$

Докажем, что $\exists h$: $L^{g^{-1}h} = L$. Рассмотрим два случая – конечных и бесконечных полей.

- Случай конечных полей. В этом случае $L^{\times} = < a >$ для некоторого $a \in L$ (мультипликативная группа конечного поля является циклической). Имеем: $\exists h \in H$: $a \in L^{g^{-1}h}$, откуда следует, что $L^{g^{-1}h} = L$.
- Случай бесконечных полей. Докажем вспомогательную лемму:

Лемма 3. Векторное пространство V над бесконечным полем K нельзя представить в виде объединения конечного числа собственных подпространств.

Доказательство леммы 3.
Докажем от противного – пусть $V = V_1 \cup \dots \cup V_k$. Без ограничения общности можно считать, что ни одно из этих подпространств не содержится в объединении остальных: $\forall i$: $V_i \nsubseteq \bigcup_{j \neq i} V_j$. Выберем $v_i \in V_i \setminus \bigcup_{j \neq i} V_j$. Рассмотрим векторы $v_1 + cv_2$ $(c \in K)$ – их бесконечно много, значит, $\exists i$, $\exists c, c' \in K$, $c \neq c'$, такие что $v_1 + cv_2, v_1 + c'v_2 \in V_i$. Следовательно, $(c - c')v_2 \in V_i \Longrightarrow v_2 \in V_i \Longrightarrow v_1 \in V_i$. Противоречие. ■

$L^{g^{-1}h}$ - подпространство в L над K и утверждение $\exists h$: $L^{g^{-1}h} = L$ для случая бесконечных полей следует из леммы 3.

Итак, $\forall g \in G$ $\exists h \in H$: $L^{g^{-1}h} = L$, откуда следует, что $g^{-1}h = id$, т.е $g = h$. Следовательно, $H = G$. Предложение 3 доказано. ■

Теорема 1 следует из предложений 1,2,3. Итак, теорема 1 полностью доказана. ■

Расширения Галуа.

Таким образом, мы выделили класс конечных расширений полей, которые обладают свойством “максимальной подвижности” по отношению к своим автоморфизмам – расширения Галуа. Возникает несколько естественных вопросов – например:

- какое место занимают расширения Галуа среди всех конечных расширений полей
- как проверить, является ли данное расширение расширением Галуа

и т.д. Далее мы ответим на эти и другие вопросы. Начнем с нескольких определений.

Определение. Многочлен $f \in K[x]$ *сепарабелен*, если f не имеет кратных корней ни в каком расширении поля K. Эквивалентно: $(f, f') = 1$.

Определение. Элемент $a \in L \supseteq K$ *сепарабелен* над K, если a – корень сепарабельного многочлена f над K. Эквивалентно: μ_a сепарабелен.

Определение. Расширение $L \supseteq K$ *сепарабельно*, если $\forall a \in L$ сепарабелен над K.

Замечания.

1) Если $char\ K = 0$, то все неприводимые многочлены над K сепарабельны (если f – неприводимый многочлен, то f' - многочлен ненулевой степени, и условие $(f, f') = 1$ выполнено всегда). Следовательно, если $char\ K = 0$, то все алгебраические расширения сепарабельны.

2) Если K совершенно, то все неприводимые многочлены над K сепарабельны и все алгебраические расширения сепарабельны.

Доказательство.
Если $char\ K = 0$, то рассуждаем как в п.1. Если $char\ K > 0$: пусть $f \in K[x]$ неприводимый, не сепарабельный, тогда $f \mid f'$, откуда следует, что $f' \equiv 0$. Тогда f имеет вид $f = a_0 + a_1x^p + a_2x^{2p} + \cdots a_mx^{mp}$, где $p = char\ K > 0$. Так как K совершенно, то $f = (b_0 + b_1x + \cdots + b_mx^m)^p$, где $b_i \in K,\ b_i^p = a_i$ – противоречит неприводимости. ■

Пример-упражнение. Рассмотрим $K = \mathbb{F}_p(t)$ – поле рациональных дробей. Доказать, что многочлен $f(x) = x^p - t \in K[x]$ неприводим над K и не сепарабелен.

3) Расширения Галуа сепарабельны.

Лекция 3. Основная теорема теории Галуа.

На прошлой лекции мы ввели класс сепарабельных алгебраических расширений, которые характеризуются тем, что любой элемент такого расширения является корнем многочлена, который не имеет кратных корней в своем поле разложения. Введем еще один класс алгебраических расширений – нормальные расширения.

Определение 1. Алгебраическое расширение $K \subseteq L$ *нормально*, если любой неприводимый многочлен $f \in K[x]$, имеющий корень в L, разлагается на линейные множители над L.
Эквивалентно: $\forall a \in L$: минимальный многочлен $\mu_a(x) \in K[x]$ разлагается на линейные множители над L.

Приведем теорему, которая характеризует расширения Галуа, не используя автоморфизмы расширения полей.

Теорема 1. Конечное расширение $K \subseteq L$ – расширение Галуа $\Leftrightarrow$ оно нормально и сепарабельно.

Доказательство.
По определению, алгебраическое расширение $K \subseteq L$ нормально и сепарабельно $\Leftrightarrow$ $\forall a \in L$: минимальный многочлен $\mu_a(x) \in K[x]$ не имеет кратных корней и разлагается на линейные множители над L (т.е. имеет ровно $\deg \mu_a$ различных корней в L) – обозначим для краткости это условие $(*)$.

Для расширений Галуа свойство $(*)$ выполнено по следствию леммы 2 из прошлой лекции. Обратно, если свойство $(*)$ выполнено, то тогда мы можем продолжить тождественный автоморфизм id: $K \nrightarrow K$ до автоморфизма φ: $L \nrightarrow L$ ровно $(L{:}K)$ способами (доказательство этого факта аналогично доказательству первой части предложения 3 из прошлой лекции). Таким образом, $|Aut\ (L/K)| = (L{:}K)$, т.е. $(L \supset K)$ – расширение Галуа. ■

Конечно, проверить нормальность и сепарабельность расширения по определению не так просто, однако существует легко проверяемый критерий того, что данное расширение является расширением Галуа.

Напоминание: пусть K – поле, $f \in K[x]$, $\deg f > 0$. *Поле разложения* многочлена f над полем K – это расширение $L = K(a_1, \dots, a_n) \supseteq K$, причем $f(x) = c(x - a_1) \cdots (x - a_n)$.

Для любого многочлена $f \in K[x]$, $\deg f > 0$ существует единственное с точностью до изоморфизма поле разложения f над K. Обозначение: $L = K(f)$.

Теорема 2. Расширение $L \supseteq K$ – расширение Галуа $\Leftrightarrow L = K(f)$, $f \in K[x]$ сепарабелен.

Доказательство.
$\Rightarrow$:
Пусть $L = K(a_1, \dots, a_s)$, тогда можно взять $f = (\mu_{a_1} \cdots \mu_{a_s})_{red}$ (т.е. возьмем произведение минимальных многочленов элементов $a_1, \dots, a_s$ и каждый кратный неприводимый множитель на K заменим на однократный).
$\Leftarrow$:
Пусть $f(x) = c(x - a_1) \cdots (x - a_n)$, где $c \in K$, $a_1, \dots, a_n \in L$. Рассмотрим башню расширений $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i = K_{i-1}(a_i) \subseteq \cdots \subseteq K_n = L$ и снова воспользуемся тем, что мы можем продолжить тождественный автоморфизм $id\colon K \xrightarrow{\sim} K$ до автоморфизма $\varphi\colon L \xrightarrow{\sim} L$ ровно $(L\colon K)$ способами (доказательство этого факта аналогично доказательству первой части предложения 3 из прошлой лекции). Следовательно, $L \supseteq K$ – расширение Галуа. ■

Следствие. Для любого конечного сепарабельного расширения $K \subseteq M$ существует расширение Галуа $K \subseteq L$, $L \supseteq M$.

Доказательство.
$M = K(a_1, \dots, a_s)$, a_i сепарабельны над K. Возьмем $f = (\mu_{a_1} \cdots \mu_{a_s})_{red}$, тогда $L = K(f) \supseteq M$. ■

Пример. Рассмотрим расширение $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$. Это расширение сепарабельно, но не нормально: в самом деле, комплексные корни $\pm i\sqrt[4]{2}$ многочлена $\mu_{\sqrt[4]{2}}(x) = x^4 - 2$ не содержатся в $\mathbb{Q}(\sqrt[4]{2})$. Но $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ уже будет расширением Галуа.

Теперь мы готовы к тому, чтобы доказать основную теорему теории Галуа. Расширения Галуа имеют максимально богатую группу автоморфизмов, поэтому совершенно естественно, что структура расширения Галуа тесно связана со структурой этой группы автоморфизмов. Основная теорема раскрывает эту связь.

Основная теорема теории Галуа. Пусть $K \subseteq L$ – расширение Галуа, $G = Aut\ (L/K)$ – его группа Галуа. Тогда:

- 1) Имеется биекция (*соответствие Галуа*) между множеством подгрупп $H \subseteq G$ и множеством подполей $M \subseteq L$, $M \supseteq K$: каждой подгруппе сопоставим поле ее инвариантов, а каждому подполю сопоставим подгруппу, состоящую из автоморфизмов расширения, оставляющих на месте все элементы подполя:

$$H \mapsto M = L^H$$
$$M \mapsto H = \{g \in G \mid g(a) = a, \forall a \in M\} = Aut\ (L/M)$$

- 2) Если $K \subseteq M \subseteq L$, M – подполе, то $L \supseteq M$ – расширение Галуа, и соответствующая подгруппа $H \subseteq G$ – его группа Галуа.
- 3) Если $K \subseteq M \subseteq L$, M – подполе, то $M \supseteq K$ – расширение Галуа $\Leftrightarrow H \lhd G$. При этом $Aut\ (M/K) \cong G/H$.

Доказательство.
2) Так как $K \subseteq L$ – расширение Галуа, т.е. нормально и сепарабельно, то $\forall a \in L$ его минимальный многочлен над K не имеет кратных корней и разлагается на линейные множители в $L[x]$. Следовательно, минимальный многочлен a над M тоже имеет это свойство (так как делит минимальный многочлен над K). Следовательно, $L \supseteq M$ нормально и сепарабельно, т.е. расширение Галуа. Утверждение, гласящее, что соответствующая подгруппа $H \subseteq G$ – его группа Галуа, является тривиальным.

1) Докажем, что соответствия $H \mapsto M = L^H$ и $M \mapsto H = Aut\ (L/M)$ взаимно обратны. Из предложения 3 из прошлой лекции следует, что если $M = L^H$, то $Aut\ (L/M) = H$. Обратно, если $H = Aut\ (L/M)$, то $M = L^H$ по свойству расширений Галуа $L \supseteq M$.

3) Пусть $K \subseteq M \subseteq L$, найдем $Aut\ (M/K)$. Разложим $L \supseteq M$ в цепочку простых алгебраических расширений: $M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_i = M_{i-1}(a_i) \subseteq \cdots \subseteq M_s = L$.

Продолжим $\varphi \in Aut\ (M/K)$ до автоморфизма $g \in G$ постепенно по этажам башни простых алгебраичеких расширений. Для продолжаемости $\varphi_{i-1}\colon M_{i-1} \to L$ до $\varphi_i\colon M_i \to L$ нужно, чтобы ${}^{\varphi_{i-1}}\mu_i(x)$ имел корень в L, где $\mu_i(x)$ – минимальный многочлен a_i над M_{i-1}. Но μ_i делит минимальный многочлен μ_{a_i} над K, который разлагается на попарно различные линейные множители над L. Следовательно, μ_i и ${}^{\varphi_{i-1}}\mu_i$ такие же, и ${}^{\varphi_{i-1}}\mu_i$ также делит минимальный многочлен μ_{a_i} над K, в частности, ${}^{\varphi_{i-1}}\mu_i$ имеет корень в L, и продолжить φ_{i-1} можно.

Далее, пусть $M = L^H$, тогда $\forall g \in G$ выполнено: $g(M) = L^{gHg^{-1}}$. В самом деле:

$$a \in g(M) \Leftrightarrow g^{-1}(a) \in M \Leftrightarrow hg^{-1}(a) = g^{-1}(a),\ \ \forall h \in H \Leftrightarrow ghg^{-1}(a) = a,\ \ \forall h \in H$$

Тогда из биективности соответствия Галуа следует, что $g(M) = M \Leftrightarrow gHg^{-1} = H$. Следовательно, $Aut\ (M/K) \simeq N_G(H)/H$, где $N_G(H)$ – нормализатор H в G.

С другой стороны, по теореме о башне расширений, $(L\colon K) = (L\colon M) \cdot (M\colon K)$. Так как $(L\colon K)$ и $(L\colon M)$ – расширения Галуа, то $(L\colon K) = |G|$ и $(L\colon K) = |H|$, поэтому $(M\colon K) = \frac{|G|}{|H|}$. Как мы знаем, $M \supseteq K$ – расширение Галуа $\Leftrightarrow |Aut\ (M/K)| = (M\colon K)$. Но $|Aut\ (M/K)| = \frac{|N_G(H)|}{|H|}$, а $(M\colon K) = \frac{|G|}{|H|}$, поэтому $|Aut\ (M/K)| = (M\colon K) \Leftrightarrow |N_G(H)| = |G| \Leftrightarrow H \lhd G$. ■

В качестве применения основной теоремы теории Галуа проиллюстрируем, как можно с ее помощью доказать т.н. теорему о примитивном элементе.

Теорема о примитивном элементе. Любое конечное сепарабельное расширение $K \subseteq M$ является простым.

Доказательство.
Вложим в расширение Галуа: $K \subseteq M \subseteq L$. $G = Aut\,(L/K)$ – конечная группа порядка $(L{:}K)$. Из основной теоремы теории Галуа следует, что любое подполе $F \subseteq L$, $F \supseteq K$ взаимно-однозначно соответствует подгруппе $H \subseteq G$. Но подгрупп в G конечное число, значит, и подполей F конечное число. В частности, подполей F, для которых $K \subseteq F \subseteq M$ тоже конечное число. Рассмотрим два случая – конечных и бесконечных полей.

- Случай бесконечных полей: по лемме 3 из прошлой лекции $\exists a \in M$: $F \subset M, F \supseteq K$: $a \notin F$. Следовательно, $K(a) = M$.
- Случай конечных полей: в этом случае $M^{\times} = < a >$ для некоторого $a \in M$ (мультипликативная группа конечного поля является циклической). Следовательно, $M = K(a)$.

■

Решение алгебраических уравнений в радикалах

Пусть $f \in K[x]$. В поле разложения: $f(x) = c(x - a_1) \cdots (x - a_n)$.

Вопрос: можно ли выразить $a_1, \dots, a_n$ через элементы поля K путем последовательного применения арифметических операций и операций извлечения корней?

Определение 2. Расширение полей $K \subseteq F$ называется *радикальным*, если существует башня расширений $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i = K_{i-1}(b_i) \subseteq \cdots \subseteq K_s = F$, где $b_i^{n_i} \in K_{i-1}$ для некоторого $n_i \in \mathbb{N}$.

Уравнение $f(x) = 0$ *разрешимо в радикалах* над K, если $K(f) \subseteq F$, $F \supseteq K$ – радикальное расширение поля K.

Сформулирем теорему, ради доказательства которой Галуа и создал свою теорию.

Теорема Галуа. Пусть $char\,K = 0$, $f \in K[x]$, $L = K(f)$, $G = Aut\,(L/K)$. Тогда: уравнение $f(x) = 0$ разрешимо в радикалах $\Leftrightarrow G = Aut\,(L/K)$ разрешима.

Лекция 4. Теорема Галуа.

Теорема Галуа. Пусть $char\, K = 0$, $f \in K[x]$, $L = K(f)$, $G = Aut\,(L/K)$. Тогда: уравнение $f(x) = 0$ разрешимо в радикалах $\Leftrightarrow$ $G = Aut\,(L/K)$ разрешима.

Лемма 1. Всякое радикальное расширение $K \subseteq F$ содержится в некотором радикальном расширении Галуа $K \subseteq E$, $E \supseteq F$.

Доказательство.
Рассмотрим башню расширений $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i = K_{i-1}(b_i) \subseteq \cdots \subseteq K_s = F$, где $b_i^{n_i} \in K_{i-1}$ для некоторого $n_i \in \mathbb{N}$. Докажем индукцией по i, что $K_i \hookrightarrow E_i$ для некоторого радикального расширения Галуа $E_i \supseteq K$.

База индукции: $i = 0$ – можно взять $E_0 = K$.

Шаг индукции: предположим, что $E_{i-1} \supseteq K_{i-1}$ и продолжим E_{i-1} до $E_i \supseteq K_i$. Пусть $\mu(x)$ – минимальный многочлен $c_i = b_i^{n_i}$ над K, тогда $\mu(x) = (x - c_i)(x - c_i')(x - c_i'') \cdots$ над E_{i-1}. Также $E_i = E_{i-1}(\mu(x^{n_i}))$ – радикальное расширение Галуа поля K. Осталось заметить, что вложение $K_i \hookrightarrow E_i$ существует по лемме 1 из лекции 2.

При $i = s$ получаем утверждение леммы. ■

Лемма 2. Пусть $f(x) = x^n - 1$. Тогда $G = Aut\,(L/K)$ абелева.

Доказательство.
Рассмотрим $\Gamma = \{\gamma \in L \mid \gamma^n = 1\}$ – это циклическая группа порядка n (как циклическая подгруппа мультипликативной группы поля), т.е. $\Gamma = <\varepsilon>$. Отсюда следует, что $L = K(\varepsilon)$.

Далее, $\forall g \in G$ выполнено: $g(\varepsilon) = \varepsilon^k$ для некоторого k (и этим автоморфизм g полностью определяется). Пусть $h \in G$: $h(\varepsilon) = \varepsilon^l$, тогда $gh(\varepsilon) = g(\varepsilon^l) = \big(g(\varepsilon)\big)^l = (\varepsilon^k)^l = \varepsilon^{kl} = hg(\varepsilon)$. Таким образом, на порождающем элементе ε любые два автоморфизма из G коммутируют. Так как любой автоморфизм полностью определяется своим действием на ε, то $gh = hg$, $\forall g, h \in G$, т.е. группа G абелева. ■

Лемма 3. Пусть поле K содержит n различных корней степени n из 1. Пусть также $F = K(b)$, $b^n = c \in K$. Тогда $F = L$ – поле разложения $f(x) = x^n - c$, а G – циклическая группа порядка, делящего n.

Доказательство.

Любой корень $f(x)$ имеет вид γb, где $\gamma^n = 1$, следовательно, все корни f лежат в F, т.е. $F = L$.

Для любого $g \in G$ выполнено: $g(b) = \gamma b$ для некоторого $\gamma \in K$, где $\gamma^n = 1$, также для любого $h \in G$ выполнено: $h(b) = \delta b$ для некоторого $\delta \in K$, где $\delta^n = 1$. Следовательно, $gh(b) = g(\delta b) = \delta g(b) = \delta\gamma b = (\gamma\delta)b$. Так как автоморфизмы g и h однозначно определяются своим действием на γ и δ соответственно, получаем вложение:

$$G \hookrightarrow \Gamma = \{\gamma \in K \mid \gamma^n = 1\} \simeq \mathbb{Z}_n$$
$$g \mapsto \gamma = \frac{g(b)}{b}$$

Это гомоморфизм, следовательно, G – циклическая группа порядка, делящего n (так как $\mathbb{Z}_n$ – циклическая группа порядка n). ■

Лемма 4. Пусть $|G| = p$ – простое число, и K содержит p корней степени p из 1. Тогда $L = K(b)$, $b^p \in K$.

Доказательство.
Так как $|G| = p$ – простое число, то $G = < g >$. Мы можем рассматривать g как линейный оператор в p-мерном векторном пространстве L над полем K, причем $g^p = id$, $g \neq id$. Все собственные значения такого оператора являются корнями степени p из 1, следовательно, все собственные значения g лежат в K. Поэтому существует собственный вектор $b \in L$: $g(b) = \varepsilon b$, $\varepsilon \neq 1$, $\varepsilon^p = 1$.

Тогда $\forall k$ выполнено: $g(b^k) = (g(b))^k = \varepsilon^k b^k$, откуда следует, что $1, b, b^2, \dots, b^{p-1}$ – собственные векторы для g с попарно различными собственными значениями $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$. Следовательно, $1, b, b^2, \dots, b^{p-1}$ линейно независимы и образуют базис L над K, т.е. $L = K(b)$. Также $g(b^p) = b^p \Longrightarrow b^p \in L^G = K$. ■

Теперь все готово для доказательства теоремы Галуа.

Доказательство теоремы Галуа.
$\Longrightarrow$:
По лемме 1 можно считать, что $K \subseteq L \subseteq F$, а $K \subseteq F$ – радикальное расширение Галуа. Тогда из основной теоремы теории Галуа (см. предыдущую лекцию) следует, что $G = Aut\,(F/K)/Aut\,(F/L)$, поэтому для разрешимости группы $G = Aut\,(L/K)$ достаточно доказать, что группа $Aut\,(F/K)$ разрешима. Таким образом, можно считать, что $L = F$ и $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_i = K_{i-1}(b_i) \subseteq \dots \subseteq K_s = F = L$, где $b_i^{n_i} \in K_{i-1}$ для некоторого $n_i \in \mathbb{N}$.

Положим $n = \text{НОК}(n_1, \dots, n_s)$. Нетрудно видеть, что $L \subseteq L(x^n - 1) = L(f(x) \cdot (x^n - 1))$. Так как $L(x^n - 1) = L(\varepsilon)$ и $K \subseteq K(\varepsilon)$ – поле разложения $x^n - 1$ (ε – первообразный корень степени n из 1), получаем следующую башню расширений:

$$K(\varepsilon) \subseteq K_1(\varepsilon) \subseteq \dots \subseteq K_{i-1}(\varepsilon) \subseteq K_i(\varepsilon) \subseteq \dots \subseteq L(\varepsilon)$$

Так как $L(\varepsilon)$ – расширение Галуа поля K, а L – его подрасширение, то

$$G = Aut\ (L(\varepsilon)/K)/Aut\ (L(\varepsilon)/L),$$

и для разрешимости группы $G = Aut\ (L/K)$ достаточно доказать, что группа $\tilde{G} = Aut\ (L(\varepsilon)/K)$ разрешима. Имеем: $\tilde{G} \rhd H_0 \rhd \dots \rhd H_{i-1} \rhd H_i \rhd \dots \rhd H_s = \{id\}$. Действительно, каждая подгруппа в этой цепочке будет нормальна в предыдущей, так как $K_{i-1}(\varepsilon) \subseteq K_i(\varepsilon)$ – расширение Галуа (это поле разложения многочлена $x^{n_i} - b_i^{n_i}$).

Далее, группа $\tilde{G}/H_0$ абелева (по лемме 2), а H_{i-1}/H_i – циклическая, порядка, делящего n_i (по лемме 3). Следовательно, по критерию разрешимости для групп, $\tilde{G}$ разрешима.

$\Leftarrow$:
Если G разрешима, то можно построить ряд: $G = H_0 \rhd \dots \rhd H_{i-1} \rhd H_i \rhd \dots \rhd H_s = \{id\}$, где $H_{i-1}/H_i \simeq \mathbb{Z}_{p_i}$, p_i-простое (если группа разрешима, то ее коммутант является собственной нормальной подгруппой, и факторгруппа по коммутанту абелева. Факторизуя по максимальной нормальной подгруппе в факторгруппе по коммутанту, получаем простую абелеву группу, т.е. циклическую, простого порядка).

По основной теореме теории Галуа, этому ряду подгрупп в группе G соответствует ряд подполей в поле L: $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{i-1} \subseteq K_i \subseteq \dots \subseteq K_s = L$. Положим $n = \text{НОК}(p_1, \dots, p_s)$ и присоединим к полю K корни степени n из 1 (достаточно присоединить ε – первообразный корень степени n из 1): $K_0 \subseteq K_0(\varepsilon)$. Получим следующую башню расширений:

$$K_0(\varepsilon) \subseteq K_1(\varepsilon) \subseteq \dots \subseteq K_{i-1}(\varepsilon) \subseteq K_i(\varepsilon) \subseteq \dots \subseteq L(\varepsilon) = F$$

Каждое расширение в этом ряду является расширением Галуа (так как каждое расширение в ряду $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{i-1} \subseteq K_i \subseteq \dots \subseteq K_s = L$ – расширение Галуа, и $K_i \subseteq K_i(\varepsilon)$, $i = 0, \dots, s$), причем $Aut\ (K_i(\varepsilon)/K_{i-1}(\varepsilon)) \hookrightarrow Aut\ (K_i/K_{i-1}) \simeq H_{i-1}/H_i \simeq \mathbb{Z}_{p_i}$.

Следовательно, $Aut\ (K_i(\varepsilon)/K_{i-1}(\varepsilon))$ либо тривиальна, либо также изоморфна $\mathbb{Z}_{p_i}$, тогда по лемме 4, $K_i(\varepsilon) = K_{i-1}(\varepsilon, b_i)$, где $b_i^{p_i} \in K_{i-1}(\varepsilon)$. Таким образом, $K \subseteq F$ – радикальное расширение. ■

Решение общего уравнения степени n в радикалах

Пусть $f(x) = x^n + c_1 x^{n-1} + \cdots + c_n$ – произвольный многочлен степени n (будем считать, что характеристика основного поля равна нулю).

Вопрос: существуют ли общие формулы, выражающие корни f через его коэффициенты $c_1, \dots, c_n$ с помощью арифметических операций и операций извлечения корней?

Будем рассматривать $c_1, \dots, c_n$ как независимые переменные, и считать, что $f \in K(c_1, \dots, c_n)[x]$. Если уравнение $f(x) = 0$ над полем $K(c_1, \dots, c_n)$ разрешимо в радикалах, то решение даст нам общие формулы, выражающие корни f через его коэффициенты. Применим теорему Галуа – для этого нам нужно знать поле разложения многочлена f и вычислить его группу Галуа.

Построим поле разложения для f над $K(c_1, \dots, c_n)$. Рассмотрим поле $L = K(x_1, \dots, x_n)$, где $x_1, \dots, x_n$ – независимые переменные. На этом поле действует группа S_n перестановками переменных. Поле инвариантов L^{S_n} этого действия – поле симметрических рациональных дробей. Но любая симметрическая рациональная дробь есть отношение двух симметрических многочленов – в самом деле, пусть $f = \frac{p}{q}$ симметрическая дробь. Рассмотрим многочлены

$$\tilde{q} = \prod_{\sigma \in S_n} \sigma(q), \qquad \tilde{p} = p \prod_{\sigma \neq id} \sigma(q)$$

$\tilde{q}$ – симметрический многочлен, при этом $f = \frac{\tilde{p}}{\tilde{q}}$, т.е. $\tilde{p} = f\tilde{q}$ тоже симметрический.

Так как любой симметрический многочлен можно представить в виде многочлена от элементарных симметрических многочленов, то

$$L^{S_n} = K(\sigma_1, \dots, \sigma_n),$$

где $\sigma_1, \dots, \sigma_n$ – элементарные симметрические многочлены от $x_1, \dots, x_n$. Их можно принять за независимые переменные (в силу основной теоремы о симметрических многочленах). Таким образом, существует изоморфизм

$$K(c_1, \dots, c_n) \simeq L^{S_n}$$
$$c_i \leftrightarrow (-1)^i \sigma_i$$

По теореме Виета, $x_1, \dots, x_n$ – все корни f. Следовательно, L – поле разложения f над $K(c_1, \dots, c_n)$. При этом $Aut\ (L/K(c_1, \dots, c_n)) = S_n$. Но S_n разрешима $\Leftrightarrow n \leq 4$.

Таким образом, общее алгебраическое уравнение степени n разрешимо в радикалах $\Leftrightarrow$ $n \leq 4$.

Лекция 5. Кольца, алгебры, модули.

Кольца, алгебры, модули

Определение. *Кольцо* – это множество A с двумя бинарными операциями $A \times A \to A$ (сложением и умножением), для которых выполнены следующие аксиомы:

1) $(A, +)$ – абелева группа,
2) дистрибутивность умножения:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

$\forall a, b, c \in A$.

Определение. *Алгебра* над полем K – это кольцо A, являющееся векторным пространством над K, так что отображение умножения $A \times A \to A$ билинейно, т.е. выполнены следующие аксиомы:

1) $(A, +)$ – абелева группа,
2) дистрибутивность умножения:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

$\forall a, b, c \in A$.
3) однородность: $\forall a, b \in A,\ \forall \lambda \in K$:

$$(\lambda a) \cdot b = a \cdot (\lambda b) = \lambda \cdot (ab)$$

Может возникнуть вопрос целесообразности введения понятия алгебры, так как понятия алгебры и кольца довольно близки между собой. Дело в том, что алгебра является линейным пространством, к которому мы можем применить хорошо разработанный аппарат линейной алгебры. Например, если выбрать в алгебре A базис (как в векторном пространстве над K), то произведение любых двух элементов A сводится к произведению базисных элементов (см. структурные константы).

В зависимости от дополнительных свойств умножения, выделяют разные классы колец и алгебр: коммутативные, ассоциативные, с единицей, лиевские, йордановы и т.д. Нужно отметить, что многие классы колец так или иначе сводятся к ассоциативным кольцам, поэтому в дальнейшем мы будем рассматривать в основном ассоциативные кольца. Напомним некоторые основные определения.

Определение. *Гомоморфизм* колец (алгебр) – это отображение φ: $A \to B$ (где A и B – кольца/алгебры), для которого: $\forall a, a' \in A$:

- $\varphi(a + a') = \varphi(a) + \varphi(a')$
- $\varphi(a \cdot a') = \varphi(a) \cdot \varphi(a')$

для алгебр добавляется еще одно свойство: $\forall \lambda \in K$:

- $\varphi(\lambda \cdot a) = \lambda \cdot \varphi(a)$

для колец/алгебр с единицей требуется выполнения еще одного условия (единица в A переходит в единицу в B):

- $\varphi(1_A) = 1_B$

Определение. Пусть A – кольцо/алгебра. *Идеалом* в A называется подмножество $I \subseteq A$, для которого:
1) I – аддитивная подгруппа (для колец),
– векторное подпространство (для алгебр).

2) $a \in A, b \in I \Longrightarrow ab \in I$ – *левый* идеал,
$a \in A, b \in I \Longrightarrow ba \in I$ – *правый* идеал.

Если идеал одновременно является левым и правым, то говорят, что он *двусторонний*. Именно двусторонние идеалы являются полным аналогом нормальных подгрупп в теории групп. В коммутативном кольце/алгебре все идеалы – двусторонние.

Обозначение для двустороннего идеала: $I \lhd A$.

В теории групп нормальные подгруппы используются для построения новых групп – мы можем строить по ним факторгруппы. Аналогичная конструкция есть и в теории колец и в теории алгебр.

Определение. Пусть A – кольцо или алгебра, $I \lhd A$. *Факторкольцо/факторалгебра*:

$$A/I = \{a + I \mid a \in A\}$$

- аддитивная факторгруппа/факторпространство с операцией умножения по правилу: $\forall a, b \in A,\ \forall \lambda \in K$:

$$(a + I)(b + I) = ab + I$$
$$\lambda(a + I) = \lambda a + I$$

Для любого гомоморфизма колец/алгебр φ: $A \to B$:

- $Im\ \varphi \subseteq B$ – подкольцо/подалгебра
- $Ker\ \varphi \lhd A$ – двусторонний идеал

Таким образом, идеалы естественно возникают как ядра гомоморфизмов колец/алгебр. Верно и обратное. Пусть $I \lhd A$, тогда, как и для групп, можно рассмотреть каноническую проекцию из A в факторкольцо/факторалгебру A/I, которая каждому элементу ставит в соответствие его смежный класс (класс вычетов) по модулю идеала I.

Каноническая проекция:

$$\pi\colon A \to A/I$$
$$a \mapsto a + I$$

Каноническая проекция – гомоморфизм (следует из определения операций в A/I: операции над смежными классами определяются через операции над представителями этих смежных классов). Ядром этого гомоморфизма является сам идеал I, а образ совпадает с A/I:

$$Ker\,\pi = I$$
$$Im\,\pi = A/I$$

Таким образом, двусторонние идеалы = ядра гомоморфизмов. По аналогии с теорией групп, существует и следующая теорема.

Основная теорема о гомоморфизмах колец/алгебр. Пусть $\varphi\colon A \to B$ – гомоморфизм колец/алгебр. Тогда ∃! изоморфизм

$$\bar{\varphi}\colon A/\,Ker\,\varphi \xrightarrow{\sim} Im\,\varphi,$$

для которого $\varphi = \bar{\varphi} \circ \pi$, где $\pi\colon A \to A/\,Ker\,\varphi$ – каноническая проекция. Другими словами,

$$\varphi(a) = \bar{\varphi}(a + Ker\,\varphi)$$

Еще короче теорему можно сформулировать с помощью коммутативной диаграммы:

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "\pi"'] & B \arrow[d, phantom, "\cup\!\!\!|"] \\
A\,/\,Ker\,\varphi \arrow[r, "\bar{\varphi}", "\sim"'] & Im\,\varphi
\end{tikzcd}$$

Пусть A – ассоциативное кольцо/алгебра. Дадим определение модуля.

Определение 1. *Левый модуль* над A (A-модуль) – это абелева группа (в аддитивной записи) / векторное пространство M вместе с операцией

$$A \times M \to M$$
$$(a, m) \mapsto am,$$

удовлетворяющая аксиомам:
$\forall a, b \in A,\ \ m, n \in M$:

- $a \cdot (m + n) = a \cdot m + a \cdot n$
- $(a + b) \cdot m = a \cdot m + b \cdot m$
- $(a \cdot b) \cdot m = a \cdot b \cdot m$

для алгебр добавляется еще одно свойство: $\forall \lambda \in K$:

- $(\lambda \cdot a) \cdot m = a \cdot (\lambda \cdot m)$

для колец/алгебр с единицей требуется выполнения еще одного условия:

- $1 \cdot m = m$

Правый модуль над A определяется аналогично – это абелева группа (в аддитивной записи) / векторное пространство M вместе с операцией

$$M \times A \to M$$
$$(m, a) \mapsto ma,$$

при этом все аксиомы, кроме третьей, остаются без изменений (меняется лишь порядок сомножителей), а третья акисома выглядит так:

- $m \cdot (a \cdot b) = (m \cdot a) \cdot b$

Замечание. Правый A-модуль = левый модуль над *противоположным кольцом/алгеброй* A^{op}. При этом $A^{op} = A$ как аддитивная группа/векторное пространство, но с новым умножением: $a * b = b \cdot a$.

Определение. (A, B)-*бимодуль* – это левый A- и правый B-модуль M, удовлетворяющий аксиоме согласованности: $\forall a \in A, b \in B,\ \ \forall m \in M$:

- $(a \cdot m) \cdot b = a \cdot (m \cdot b)$

Как видно из определения, неформально можно сказать, что модуль – это векторное пространство над кольцом.

Примеры модулей:

1) Векторное пространство – это модуль над полем.

2) Абелева группа (аддитивная) – это модуль над $\mathbb{Z}$.

3) Пусть V – векторное пространство над полем K, и $\mathcal{A}\colon V \to V$ – линейный оператор. Тогда на V можно ввести структуру $K[x]$-модуля (над алгеброй многочленов): $fv = f(\mathcal{A})v, \quad \forall f \in K[x], \forall v \in V$.

4) $Mat_{m,n}(A)$ – это $\big(Mat_m(A), Mat_n(A)\big)$-бимодуль.
Частный случай: $m = n = 1$. В этом случае A есть (A, A)-бимодуль, который называют *регулярным*.

5) Пусть $\mathcal{R}\colon\ G \longrightarrow GL_n(V)$ – линейное представление группы G в векторном пространстве V над полем K (т.е. гомоморфизм из группы G в группу невырожденных линейных операторов над V). Тогда задание линейного представления означает задание KG-модуля над V (где KG – групповая алгебра):

$$\left(\sum_i \lambda_i g_i\right) \cdot v = \sum_i \lambda_i \cdot \mathcal{R}(g_i)v$$

6) Пусть X – гладкое многообразие. Пространство векторных полей $Vect(X)$ – левый модуль над $C^\infty(X)$.

7) $C^\infty(X)$ – левый модуль над алгеброй дифференциальных операторов $Diff(X)$. Элементы пространства $Diff(X)$ – дифференциальные операторы $\partial\colon\ C^\infty(X) \longrightarrow C^\infty(X)$, задаваемые в локальных координатах $x_1, \dots, x_n$ формулой:

$$\partial = \sum_{0 \le k_1, \dots, k_n \le N} f_{k_1, \dots, k_n}(x) \cdot \frac{\partial^{k_1}}{\partial x_1^{k_1}} \cdots \frac{\partial^{k_n}}{\partial x_n^{k_n}}$$

Замечание. Задать на абелевой группе M структуру (левого) A-модуля $\Leftrightarrow$ задать гомоморфизм $A \longrightarrow End(M)$, где $End(M)$ – кольцо эндоморфизмов M (т.е. гомоморфизмов M в себя). Если M – векторное пространство, то задать на M структуру (левого) A-модуля $\Leftrightarrow$ задать гомоморфизм $A \longrightarrow L(M)$, где $L(M)$ – алгебра линейных операторов на M.

Другие структуры кольца/алгебры на $End(M)$ или $L(M)$ позволяют определить понятие модуля над кольцами других типов (примеры этого мы увидим далее).

Определение 2. Пусть M – модуль над A. *Подмодуль* $N \subseteq M$ – аддитивная подгруппа /подпространство, удовлетворяющая условию: $a \in A, \ \ n \in N \Longrightarrow an \in N$.

Фактормодуль M/N – аддитивная факторгруппа / факторпространство с операцией умножения на A по правилу: $a(m + N) = am + N, \forall a \in A, \ \forall m \in N$.

Примеры подмодулей.

- подмодули в левом регулярном A-модуле – это левые идеалы в A,
- подмодули в правом регулярном A-модуле – это правые идеалы в A,
- подмодули в регулярном (A, A)-бимодуле – это двусторонние идеалы в A.

Определение 3. *Гомоморфизм* A-модулей – это отображение $\varphi\colon M \to N$, которое является гомоморфизмом аддитивных групп / линейных отображений векторных пространств и $\varphi(am) = a\varphi(m), \forall a \in A,\ \forall m \in M$.

Ядро $Ker\ \varphi = \{m \in M \mid \varphi(m) = 0\}$ – подмодуль в M. *Образ* $Im\ \varphi$ – подмодуль в N. По аналогии с теорией групп, верна основная теорема о гомоморфизме: $Im\ \varphi \simeq M/Ker\ \varphi$.

Лекция 6. Общие теоретико-модульные конструкции.

В сегодняшней лекции мы рассмотрим некоторые теоретико-модульные конструкции, которые позволяют строить новые модули из имеющихся. Начнем с прямой суммы.

Определение 1. *Прямая сумма* колец/алгебр

$$A = A_1 \oplus \cdots \oplus A_s$$

- прямая сумма аддитивных групп (если A – кольцо), или векторных пространств (если A – алгебра) с умножением по правилу: $\forall a_i, b_i \in A_i$ $(i = 1, \dots, s)$:

для внутренней прямой суммы: если

$$a = a_1 + \cdots + a_s$$
$$b = b_1 + \cdots + b_s$$

то

$$ab = a_1 b_1 + \cdots + a_s b_s$$

для внешней прямой суммы: если

$$a = (a_1, \dots, a_s)$$
$$b = (b_1, \dots, b_s)$$

то

$$ab = (a_1 b_1, \dots, a_s b_s)$$

Прямая сумма (левых) A-модулей

$$M = M_1 \oplus \cdots \oplus M_s$$

- прямая сумма аддитивных групп / векторных пространств со следующим умножением на элементы A: если $a \in A$ и $m = m_1 + \cdots + m_s$, то $am = am_1 + \cdots + am_s$.

Введем еще несколько стандартных понятий:

- Вложения ε_i: $M_i \to M$
- Проекции π_i: $M \to M_i$

- гомоморфизмы модулей (аналогично для колец/алгебр).

Универсальное свойство прямой суммы.

а) Для любого набора гомоморфизмов модулей φ_i: $M_i \to N$ существует единственный гомоморфизм φ: $M \to N$, такой что $\varphi|_{M_i} = \varphi \circ \varepsilon_i = \varphi_i$. Обозначение: $\varphi = \varphi_1 \oplus \cdots \oplus \varphi_s$.

б) Для любого набора гомоморфизмов модулей $\psi_i\colon N \to M_i$ существует единственный гомоморфизм $\psi\colon N \to M$, такой что $\pi_i \circ \psi = \psi_i$. Обозначение: $\psi = \psi_1 \times \cdots \times \psi_s$.

$$\begin{tikzcd}
M_1 \arrow[dr, "\varepsilon_1"] \arrow[drr, bend left, "\varphi_1"] & & \\
\vdots & M \arrow[r, dashed, "\exists!\,\varphi"] & N \\
M_s \arrow[ur, "\varepsilon_s"'] \arrow[urr, bend right, "\varphi_s"'] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& & M_1 \\
N \arrow[r, dashed, "\exists!\,\psi"] \arrow[urr, bend left, "\psi_1"] \arrow[drr, bend right, "\psi_s"'] & M \arrow[ur, "\pi_1"] \arrow[dr, "\pi_s"'] & \vdots \\
& & M_s
\end{tikzcd}$$

Рис. 6.1. Универсальное свойство прямой суммы

Доказательство.

Единственность.

а) Так как φ – гомоморфизм, то $\varphi(m_1 + \cdots + m_s) = \varphi(m_1) + \cdots + \varphi(m_s)$, а так как φ должен продолжать φ_i, то должно быть выполнено $\varphi(m_i) = \varphi_i(m_i)$. Таким образом, $\varphi(m_1 + \cdots + m_s) = \varphi_1(m_1) + \cdots + \varphi_s(m_s)$ – этой формулой φ определяется однозначно.

б) Пусть $\psi(n) = m = m_1 + \cdots + m_s$, тогда должно быть выполнено $m_i = \pi_i\,\psi(n) = \psi_i(n)$, т.е. $\psi(n) = \psi_1(n) + \cdots + \psi_s(n)$ – этой формулой ψ определяется однозначно.

Существование. Определим φ и ψ по вышеприведенным формулам. Легко проверить, что это гомоморфизмы, подходящие под условия. ■

Приведем еще одно полезное утверждение, касающееся прямой суммы колец/алгебр.

Предложение 1. Кольцо/алгебра A разлагается в прямую сумму колец/алгебр: $A \simeq A_1 \oplus \cdots \oplus A_s$ тогда и только тогда, когда $A \simeq I_1 \oplus \cdots \oplus I_s$, где $I_i \lhd A$ и $I_i \simeq A_i$ как кольцо/алгебра.

Доказательство.

$\Longrightarrow$:

Можно считать, что $A \simeq A_1 \oplus \cdots \oplus A_s$ – внутренняя прямая сумма. Так как $A_iA_j = \{0\}$ при $i \neq j$, то $A_iA = A_iA_i \subseteq A_i$ и $AA_i = A_iA_i \subseteq A_i$, откуда следует, что $A_i \lhd A$.

$\Longleftarrow$:

Так как $I_i, I_j \lhd A$, то $I_iI_j \subseteq I_i$, также $I_iI_j \subseteq I_j$, т.е. $I_iI_j \subseteq I_i \cap I_j = \{0\}$. Следовательно, умножение в $I_1 \oplus \cdots \oplus I_s$ покомпонентно. ■

Определение 2. Пусть A – ассоциативное кольцо/алгебра над K с единицей, M – правый A-модуль, N – левый A-модуль, P – аддитивная абелева группа / векторное пространство над K. Отображение $\Phi\colon M \times N \to P$ называется *A-билинейным*, если $\forall m, m' \in M$, $\forall n, n' \in M$:

- $\Phi(m+m',n)=\Phi(m,n)+\Phi(m',n)$
- $\Phi(m,n+n')=\Phi(m,n)+\Phi(m,n')$

для алгебр добавляется еще одно свойство: $\forall\lambda\in K$:

- $\Phi(\lambda m,n)=\Phi(m,\lambda n)=\lambda\Phi(m,n)$

Условия 1-3 – условия билинейности отображения векторных пространств, для A-билинейности требуется выполнения еще одного условия: $\forall a\in A$:

- $\Phi(ma,n)=\Phi(m,an)$

Возникает вопрос – если рассматривать все A-билинейные отображения для фиксированных A-модулей M и N, будет ли среди них универсальное отображение (т.е. со свойствами, аналогичными универсальному свойству прямой суммы)? Следующее утверждение дает ответ на этот вопрос.

Предложение 2.
1) Существует единственная (с точностью до изоморфизма) абелева группа / векторное пространство U вместе с A-билинейным отображением Φ_{uni}: $M\times N\longrightarrow U$, такая что для любого A-билинейного отображения Φ: $M\times N\longrightarrow P$ существует единственный гомоморфизм групп / линейное отображение векторных пространств φ: $U\longrightarrow P$, такой что $\Phi=\varphi\circ\Phi_{uni}$.

$$\begin{tikzcd} M\times N \arrow[rr, "\Phi"] \arrow[dr, "\Phi_{uni}"'] & & P \\ & U \arrow[ur, dashed, "\exists!\,\varphi"'] & \end{tikzcd}$$

Обозначение: $U=M\underset{A}{\otimes}N$ – тензорное произведение модулей, $\Phi_{uni}=m\otimes n$.
Таким образом, $\Phi(m,n)=\varphi(m\otimes n)$.

2) Любой $u\in U$ представим в виде $u=m_1\otimes n_1+\cdots+m_s\otimes n_s$, где $m_i\in M$, $n_i\in N$.

3) Если M – (B,A)-бимодуль, а N – (A,C)-бимодуль, то $M\underset{A}{\otimes}N$ – (B,C)-бимодуль с умножением $b(m\otimes n)=bm\otimes n$, $(m\otimes n)c=m\otimes nc$.

Доказательство.

1) Единственность. Пусть U' - другое тензорное произведение M и N. Воспользуемся языком коммутативных диаграмм:

$$\begin{tikzcd}
 & U \arrow[d, dashed, shift right, "\exists!\,\varphi"'] \arrow[loop right, dashed, "\exists!\,\varphi'\varphi = id"] \\
M \times N \arrow[ur, "\Phi_{uni}"] \arrow[dr, "\Phi'_{uni}"'] & \\
 & U' \arrow[uu, dashed, shift right, "\exists!\,\varphi'"'] \arrow[loop right, dashed, "\exists!\,\varphi\varphi' = id"]
\end{tikzcd}$$

По свойству универсальности для U существует единственное отображение φ: $U \longrightarrow U'$, которое делает эту диаграмму коммутативной. Аналогично, для U' существует единственное отображение φ': $U' \longrightarrow U$, которое делает эту диаграмму коммутативной.

Рассмотрим композицию $\varphi' \circ \varphi$: $U \longrightarrow U$. Имеем: $\varphi' \circ \varphi \circ \Phi_{uni} = \varphi' \circ \Phi'_{uni} = \Phi_{uni}$, откуда следует, что $\varphi' \circ \varphi = id$. Аналогично получаем, что $\varphi \circ \varphi' = id$. Отсюда следует, что φ и φ' - два взаимно обратных друг другу изоморфизма, т.е. $U \simeq U'$.

2) Прежде чем доказывать существование в п.1., докажем пункт 2. Рассмотрим подмножество

$$U \supseteq U_0 = \{\sum_i m_i \otimes n_i \mid m_i \in M, n_i \in N\}$$

Легко видеть, что U_0 – подгруппа / подпространство: $\lambda(m \otimes n) = \lambda m \otimes n$, $\forall \lambda \in \mathbb{Z}$ или K (для векторных пространств над K это просто одно из условий билинейности, а для колец это следует из аддитивности и того, что $m \otimes n + (-m) \otimes n = \big(m + (-m)\big) \otimes n = 0 \otimes n = (0+0) \otimes n = 0 \otimes n + 0 \otimes n = 0$).

Рассмотрим отображение $M \times N \xrightarrow{\Phi_{uni}} U \xrightarrow{\pi} U/U_0$, где π – каноническая проекция. Тогда $\pi \circ \Phi_{uni} = 0$. Но $\pi \circ \Phi_{uni} = 0 = 0 \circ \Phi_{uni}$, поэтому $\pi = 0$. Следовательно, $U = U_0$.

<u>Существование</u>. Рассмотрим множество формальных линейных комбинаций следующего вида:

$$F = \{\sum_i \lambda_i(m_i, n_i) \mid \lambda_i \in \mathbb{Z} \text{ или } K,\ m_i \in M,\ n_i \in N\}$$

Это аддитивная абелева группа / векторное пространство над K. Рассмотрим $F_0 \subseteq F$ – подгруппа / подпространство, порожденное элементами вида:

- $(m + m', n) - (m, n) - (m', n)$
- $(m, n + n') - (m, n) - (m, n')$
- $\lambda(m, n) - (\lambda m, n)$

- $\lambda(m,n) - (m,\lambda n)$
- $(ma,n) - a(m,n)$, $a \in A$

Положим $U = F/F_0$ и рассмотрим

$$M \times N \xrightarrow{\Phi_{uni}} F/F_0$$
$$\Phi_{uni}(m,n) = (m,n) + F_0$$

Проверка универсального свойства: $\Phi\colon M \times N \longrightarrow P$ однозначно продолжается до гомоморфизма / линейного отображения $\tilde{\varphi}\colon F \longrightarrow P$. Из A-билинейности Φ следует, что $Ker\ \tilde{\varphi} \supseteq F_0$, поэтому $\tilde{\varphi} = \varphi \circ \pi$, где $\pi\colon F \longrightarrow F/F_0$ – каноническая проекция, $\varphi\colon F/F_0 \longrightarrow P$. Следовательно, $\Phi = \varphi \circ \Phi_{uni}$. Единственность φ вытекает из того, что F/F_0 порождается элементами вида $(m,n) + F_0$.

3) $\forall b \in B$ рассмотрим отображение

$$\Phi\colon M \times N \longrightarrow M \otimes N$$
$$\Phi(m,n) = bm \otimes n$$

Это отображение A-билинейно, следовательно, по универсальному свойству, $\exists!\ \varphi\colon M \otimes N \longrightarrow M \otimes N$, такой что $\varphi(m \otimes n) = \Phi(m,n) = bm \otimes n$.

$$\begin{tikzcd}
M \times N \arrow[r, "\Phi"] \arrow[d, "\Phi_{uni}"'] & M \otimes N \\
M \otimes N \arrow[ur, dashed, "\exists!\ \varphi"'] &
\end{tikzcd}$$

Определим умножение на B слева по правилу: $bu = \varphi(u)$, $\forall u \in M \otimes N$. Тогда $b(m \otimes n) = bm \otimes n$. Аналогично определяется умножение на C справа. Аксиомы (B,C)-бимодуля достаточно проверить на элементах вида $u = m \otimes n$, что легко. ■

Примеры и свойства тензорного произведения.

1) $M \underset{A}{\otimes} A \simeq M$, $A \underset{A}{\otimes} N \simeq N$

Доказательство.
Достаточно доказать первое свойство (второе доказывается аналогично). Рассмотрим произвольное билинейное отображение $\Phi\colon M \times A \longrightarrow P$. Имеем: $\Phi(m,a) = \Phi(ma,1)$, тогда определим φ как $\varphi(m) = \Phi(m,1)$ и $\Phi_{uni}(m,a) = ma$. Тогда $\Phi = \varphi \circ \Phi_{uni}$:

$$\begin{tikzcd} M \times A \arrow[r, "\Phi"] \arrow[d, "\Phi_{uni}"'] & P \\ M \arrow[ur, dashed, "\exists!\,\varphi"'] & \end{tikzcd}$$

Единственность φ:

$$\varphi(m) = \varphi \circ \Phi_{uni}(m, 1) = \Phi(m, 1)$$

Итак, отображение φ существует и единственно, следовательно, M удовлетворяет свойству универсальности, а значит, $M \simeq M \underset{A}{\otimes} A$. ■

2)

- $(M_1 \oplus \cdots \oplus M_s) \otimes N \simeq (M_1 \otimes N) \oplus \cdots \oplus (M_s \otimes N)$
- $M \otimes (N_1 \oplus \cdots \oplus N_s) \simeq (M \otimes N_1) \oplus \cdots \oplus (M \otimes N_s)$

Доказательство.
Достаточно доказать первое свойство (второе доказывается аналогично). Рассмотрим произвольное билинейное отображение Φ: $(M_1 \oplus \cdots \oplus M_s) \otimes N \longrightarrow P$.

$$\begin{tikzcd} (M_1 \oplus \cdots \oplus M_s) \otimes N \arrow[r, "\Phi"] \arrow[dd, bend right=60, "\Phi_{uni}(m_1 + \cdots + m_s, n) = m_1 \otimes n + \cdots + m_s \otimes n"'] & P & \\ M_i \times N \arrow[u, hook] \arrow[r, "\otimes"'] & M_i \otimes N \arrow[u, "\exists!\,\varphi_i"] \arrow[r, hook] & (M_1 \otimes N) \oplus \cdots \oplus (M_s \otimes N) \arrow[ul, "\exists!\,\varphi = \varphi_1 \oplus \cdots \oplus \varphi_s"'] \end{tikzcd}$$

Единственный способ сделать приведенную диаграмму коммутативной – это положить $\Phi_{uni}(m_1 + \cdots + m_s, n) = m_1 \otimes n + \cdots + m_s \otimes n$. ■

3) $L \underset{B}{\otimes} \left(M \underset{A}{\otimes} N\right) \simeq \left(L \underset{B}{\otimes} M\right) \underset{A}{\otimes} N$

Доказательство.
Рассмотрим отображение

$$L \times M \times N \longrightarrow L \times M \otimes N \longrightarrow L \otimes (M \otimes N)$$
$$(l, m, n) \mapsto (l, m \otimes n) \mapsto l \otimes (m \otimes n)$$

Также рассмотим отображение

$$L \times M \times N \longrightarrow (L \otimes M) \otimes N$$
$$(l, m, n) \mapsto (l \otimes m) \otimes n$$

Так как $(l \otimes \cdot\,) \otimes \cdot$ – A-билинейное отображение, то (по универсальному свойству) существует единственное отображение $L \times M \otimes N \longrightarrow (L \otimes M) \otimes N$, делающее следующую диаграмму коммутативной:

$$\begin{tikzcd}
L \times M \times N \arrow[r] \arrow[d] & L \times M \otimes N \arrow[dl, dashed, "\exists! B\text{-билинейное отображение}"'] \\
(L \otimes M) \otimes N &
\end{tikzcd}$$

Тогда по универсальному свойству для $L \otimes (M \otimes N)$, существует единственный гомоморфизм $L \otimes (M \otimes N) \longrightarrow (L \otimes M) \otimes N$, делающий следующую диаграмму коммутативной (и аналогично существует единственный гомоморфизм $(L \otimes M) \otimes N \longrightarrow L \otimes (M \otimes N)$):

$$\begin{tikzcd}
L \times M \times N \arrow[r] \arrow[d] & L \times M \otimes N \arrow[r] \arrow[dl, dashed, "\exists! B\text{-билинейное отображение}"'] & L \otimes (M \otimes N) \arrow[dl, dashed, "\exists!"'] \\
(L \otimes M) \otimes N \arrow[urr, dashed, "\exists!"'] & &
\end{tikzcd}$$

Таким образом, получаем два взаимно обратных изоморфизма: из $L \otimes (M \otimes N)$ в $(L \otimes M) \otimes N$, и из $(L \otimes M) \otimes N$ в $L \otimes (M \otimes N)$. ■

Лекция 7. Свойства тензорного произведения.

Свойства тензорного произведения (продолжение).

4) Пусть M_i – (A_{i-1}, A_i)-бимодули $(i = 1, \dots, s)$ и P – (A_0, A_s)-бимодуль. Тогда отображение Φ: $M_1 \times \dots \times M_s \longrightarrow P$ назовем $(A_0, \dots, A_s)$-*полилинейным*, если:

- $\Phi(m_1, \dots, m_i + m_i', \dots, m_s) = \Phi(m_1, \dots, m_i, \dots, m_s) + \Phi(m_1, \dots, m_i', \dots, m_s)$
- $\Phi(m_1, \dots, \lambda m_i, \dots, m_s) = \lambda\Phi(m_1, \dots, m_i, \dots, m_s)$
- $\Phi(m_1, \dots, m_i, a_i m_{i+1}, \dots, m_s) = \Phi(m_1, \dots, m_i a_i, m_{i+1}, \dots, m_s)$
- $\Phi(a_0 m_1, m_2, \dots, m_s) = a_0\Phi(m_1, m_2, \dots, m_s)$
- $\Phi(m_1, \dots, m_{s-1}, m_s a_s) = \Phi(m_1, \dots, m_{s-1}, m_s)a_s$

$\forall\, m_i, m_i' \in M_i$ $(i = 1, \dots, s)$, $\forall\, a_j \in A_j$ $(j = 1, \dots, s)$, $\forall\, \lambda \in \mathbb{Z}$ или K.

Универсальное свойство тензорного произведения:

Для любого полилинейного отображения Φ: $M_1 \times \dots \times M_s \longrightarrow P$ существует единственный гомоморфизм φ: $M_1 \underset{A_1}{\otimes} \cdots \underset{A_s}{\otimes} M_s \longrightarrow P$, делающий следующую диаграмму коммутативной:

$$\begin{tikzcd}
(m_1, \dots, m_s) \in M_1 \times \dots \times M_s \arrow[r, "\Phi"] \arrow[d, mapsto] & P \\
m_1 \otimes \dots \otimes m_s \in M_1 \underset{A_1}{\otimes} \cdots \underset{A_s}{\otimes} M_s \arrow[ur, dashed, "\exists!\,\varphi"'] &
\end{tikzcd}$$

Т.е. $\Phi(m_1, \dots, m_s) = \varphi(m_1 \otimes \dots \otimes m_s)$.

Доказательство.
Отображение Φ: $M_1 \times \dots \times M_s \longrightarrow P$ билинейно по M_1, M_2, а значит, существует единственное отображение $M_1 \otimes M_2 \times M_3 \times \dots \times M_s \longrightarrow P$ (которое тоже полилинейно), делающее следующую диаграмму коммутативной:

$$\begin{tikzcd}
(m_1, m_2, m_3, \dots, m_s) \in M_1 \times \dots \times M_s \arrow[r, "\Phi"] \arrow[d, mapsto] & P \\
(m_1 \otimes m_2, m_3, \dots, m_s) \in M_1 \otimes M_2 \times M_3 \times \dots \times M_s \arrow[ur, dashed, "\exists!"'] &
\end{tikzcd}$$

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Далее аналогичными расуждениями получаем, что существует единственный гомоморфизм $(M_1 \otimes M_2) \otimes M_3 \times M_4 \cdots \times M_s \longrightarrow P$, делающий следующую диаграмму коммутативной:

$$\begin{tikzcd}
(m_1, m_2, m_3, \dots, m_s) \in M_1 \times \cdots \times M_s \arrow[r, "\Phi"] \arrow[d, mapsto] \arrow[d] & P \\
(m_1 \otimes m_2, m_3, \dots, m_s) \in M_1 \otimes M_2 \times M_3 \times \cdots \times M_s \arrow[ur, dashed, "\exists!"'] \arrow[d, mapsto] \arrow[d] & \\
((m_1 \otimes m_2) \otimes m_3, m_4, \dots, m_s) \in (M_1 \otimes M_2) \otimes M_3 \times \cdots \times M_s \arrow[uur, dashed, "\exists!"'] &
\end{tikzcd}$$

И так далее – в итоге получим, что существует единственный гомоморфизм φ: $M_1 \otimes M_2 \otimes \cdots \otimes M_s \longrightarrow P$, делающий соответствующую диаграмму коммутативной. ■

5) Тензорное произведение векторных пространств V, W над полем K.

Пусть $e_1, \dots, e_n$ – базис V, $f_1, \dots, f_m$ – базис W. Тогда:

а) $\forall u \in V \otimes W$ существует единственное выражение

$$u = e_1 \otimes w_1 + \cdots + e_n \otimes w_n = v_1 \otimes f_1 + \cdots + v_m \otimes f_m, \text{ где } w_i \in W, v_j \in V$$

б) $\{e_i \otimes f_j \mid i = 1, \dots, n,\ j = 1, \dots, m\}$ – базис $V \otimes W$ и $\dim V \otimes W = \dim V \cdot \dim W$.

Доказательство.
а) Так как $V = Ke_1 \oplus \cdots \oplus Ke_n$, то

$$V \otimes W = \bigoplus_i Ke_i \otimes W \cong W \oplus \cdots \oplus W$$

При этом изоморфизме всякому элементу $u = e_1 \otimes w_1 + \cdots + e_n \otimes w_n$ из $V \otimes W$ взаимно-однозначно соответствует $(w_1, \dots, w_n) \in W \oplus \cdots \oplus W$. Аналогично доказывается существование и единственность второго разложения для u.

б) $\forall i = 1, \dots, n$: w_i однозначно разлагается по базису $f_1, \dots, f_m$, откуда следует, что $u = e_1 \otimes w_1 + \cdots + e_n \otimes w_n$ однозначно разлагается в линейную комбинацию элементов $e_i \otimes f_j$. ■

Пример: расширение скаляров. Пусть $K \subseteq L$ – расширение полей, V – векторное пространство над K. Тогда $V \underset{K}{\otimes} L$ – векторное пространство над L с базисом $e_1 \otimes 1, \dots, e_n \otimes 1$ (так как $e_i \otimes w_i = (e_i \otimes 1) \cdot w_i,\ w_i \in L$).

6) Полилинейные функции на векторных пространствах (конечномерных).

$$\left\{\text{Полилинейные функции } V_1 \times \dots \times V_s \xrightarrow{\Phi} K\right\} \simeq (V_1 \otimes \dots \otimes V_s)^* \simeq V_1^* \otimes \dots \otimes V_s^*$$

Доказательство.
1-ый изоморфизм: из универсального свойства тензорного произведения следует, что существует единственная линейная функция φ такая, что следующая диаграмма коммутативна:

$$\begin{tikzcd}
V_1 \times \dots \times V_s \arrow[r, "\Phi"] \arrow[d, "\otimes"'] & K \\
V_1 \otimes \dots \otimes V_s \arrow[ur, dashed, "\exists!\varphi"'] &
\end{tikzcd}$$

т.е. $\varphi(v_1 \otimes \dots \otimes v_s) = \Phi(v_1, \dots, v_s)$. Таким образом, свойство универсальности дает нам первый изоморфизм $\Phi \leftrightarrow \varphi$.

2-ой изоморфизм: сопоставим набору $\varphi_i \in V_i^*$ $(i = 1, \dots, s)$ полилинейную функцию $\Phi\colon V_1 \times \dots \times V_s \longrightarrow K$ по правилу $\Phi(v_1, \dots, v_s) = \varphi_1(v_1) \cdots \varphi_s(v_s)$. Этой функции (по первому изоморфизму) соответствует функция $\varphi \in (V_1 \otimes \dots \otimes V_s)^*$, $\varphi = \varphi(v_1 \otimes \dots \otimes v_s)$. Получаем полилинейное отображение

$$\begin{aligned} V_1^* \times \dots \times V_s^* &\longrightarrow (V_1 \otimes \dots \otimes V_s)^* \\ (\varphi_1, \dots, \varphi_s) &\mapsto \varphi, \end{aligned}$$

которое (по универсальному свойству тензорного произведения) пропускается через $V_1^* \otimes \dots \otimes V_s^*$:

$$\begin{tikzcd}
V_1^* \times \dots \times V_s^* \arrow[r, "\Phi"] \arrow[d] & (V_1 \otimes \dots \otimes V_s)^* \\
V_1^* \otimes \dots \otimes V_s^* \arrow[ur, dashed, "\exists!\sigma"'] &
\end{tikzcd}$$

Выбор базисов в $V_1, \dots, V_s$ автоматически влечет за собой выбор дуальных базисов в $V_1^*, \dots, V_s^*$, что, в свою очередь, означает выбор базиса в $V_1^* \otimes \dots \otimes V_s^*$.

С другой стороны, выбор базисов в $V_1, \dots, V_s$ задает базис в $V_1 \otimes \dots \otimes V_s$, который задает базис в $(V_1 \otimes \dots \otimes V_s)^*$. Легко видеть, что при этом базис в $(V_1 \otimes \dots \otimes V_s)^*$ переходит в базис в $V_1^* \otimes \dots \otimes V_s^*$, следовательно, σ – изоморфизм. ■

7) Тензорное произведение колец / алгебр.

Пусть A, B, C – ассоциативные кольца / алгебры и $\alpha\colon C \longrightarrow A$ и $\beta\colon C \longrightarrow B$ – гомоморфизмы, такие что $\alpha(C)$ коммутирует с A, а $\beta(C)$ коммутирует с B. Тогда A и B являются (C, C)-бимодулями: $\forall a \in A, b \in B, c \in C$:

$$ca = ac = a\alpha(c)$$
$$cb = bc = b\beta(c)$$

При этом $A \underset{C}{\otimes} B$ – ассоциативное кольцо / алгебра, умножение в котором устроено так:

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$$

Доказательство.
Рассмотрим отображение

$$A \times B \times A \times B \longrightarrow A \otimes B$$
$$(a, b, a', b') \mapsto aa' \otimes bb'$$

Очевидно, что оно (C, C, C, C, C)-полилинейно, следовательно, (по универсальному свойству тензорного произведения) пропускается через $A \otimes B \times A \otimes B$, т.е. существует единственное C-билинейное отображение из $A \otimes B \times A \otimes B$ в $A \otimes B$:

$$A \otimes B \times A \otimes B \longrightarrow A \otimes B$$
$$(a \otimes b, a' \otimes b') \mapsto aa' \otimes bb'$$

- это и есть операция умножения на $A \underset{C}{\otimes} B$ (свойства умножения легко проверяются).

$$\begin{tikzcd}
A \times B \times A \times B \arrow[r] \arrow[d] & A \otimes B \\
A \otimes B \times A \otimes B \arrow[ur, dashed, "\exists!\, C\text{-билинейное отображение}"'] &
\end{tikzcd}$$

■

Пример: A, B-бимодули – это то же самое, что и левые модули над $A \underset{\mathbb{Z}}{\otimes} B^{op}$ или над $A \underset{K}{\otimes} B^{op}$, умножение (для разложимых элементов) определяется так: $(a \otimes b)m = amb$.

Структура колец / модулей.

Теперь перейдем к вопросам структуры колец/модулей. Далее под модулем будем подразумевать левый модуль.

Определение 1. A-модуль M *порожден* семейством элементов $\{m_i\}_{i\in I}$, если $\forall m \in M$ представляется в виде $m = a_1 m_{i_1} + \cdots + a_n m_{i_n}$, где $a_i \in A$.

- Модуль, порожденный конечным набором элементов $m_1, \dots, m_n$, называется *конечно порожденным*: $\forall m \in M \quad \exists a_1, \dots, a_n \in A$: $\quad m = a_1 m_1 + \cdots + a_n m_n$. Обозначение: $M = < m_1, \dots, m_n >_A = Am_1 + \cdots + Am_n$.
- Модуль, порожденный одним элементом, называется *циклическим*: $M = Am$.
- Конечно порожденный модуль = сумма конечного числа циклических подмодулей
- Конечно порожденный модуль $F = Af_1 + \cdots + Af_n$ называется *свободным* модулем с базисом $\{f_1, \dots, f_n\}$, если $\forall f \in F \ \exists!\, a_1, \dots, a_n \in A$: $f = a_1 f_1 + \cdots + a_n f_n$. Эквивалентно: $F = A \oplus \cdots \oplus A = A^{\oplus n}$, где A – левый регулярный A-модуль (т.е. кольцо A рассматриваем как модуль над собой), $f \leftrightarrow (a_1, \dots, a_n)$.

Замечание. Конечно порожденные модули = фактормодули свободных конечно порожденных модулей: отображение

$$A^{\oplus n} \xrightarrow{\pi} M = Am_1 + \cdots + Am_n$$
$$(a_1, \dots, a_n) \mapsto a_1 m_1 + \cdots + a_n m_n$$

- сюръективный гомоморфизм, следовательно, $M \simeq A^{\oplus n}/Ker\,\pi$.

Примеры.

- Конечно порожденные $\mathbb{Z}$-модули = конечно порожденные абелевы группы
- Циклические $\mathbb{Z}$-модули = циклические группы
- Свободные $\mathbb{Z}$-модули = свободные абелевы группы
- Векторные пространства (конечномерные) над K = свободные K-модули

Нётеровы модули.

Предложение 1. Для A-модуля M следующие условия эквивалентны:

(1) Любой подмодуль $N \subseteq M$ конечно порожден
(2) Любая возрастающая цепочка подмодулей $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$ стабилизируется, т.е. $\exists k$: $N_k = N_{k+1} = N_{k+2} = \cdots$ (условие обрыва возрастающих цепей)

Доказательство.
(1) $\Longrightarrow$ (2). Рассмотрим

$$N_\infty = \bigcup_k N_k - \text{подмодуль в } M$$

Следовательно, $N_\infty = Am_1 + \cdots + Am_n$, где $m_i \in N_{k_i}$ для некоторого $k_i \in \mathbb{N}$ $(i = 1, \dots, n)$. Выберем $k = \max\{k_1, \dots, k_n\}$, тогда $m_1, \dots, m_n \in N_k$, откуда следует, что $N_\infty = N_k = N_{k+1} = N_{k+2} = \cdots$.

(2) $\Longrightarrow$ (1). От противного: пусть N не конечно порожден.

- Выберем $m_1 \in N$: так как $N \neq Am_1$, то можно выбрать $m_2 \in N \backslash Am_1$.
- Так как $N \neq Am_1 + Am_2$, то можно выбрать $m_3 \in N \backslash (Am_1 + Am_2)$, и так далее.
- Получаем последовательность $m_k \in N \backslash (Am_1 + \cdots + Am_{k-1})$, $\forall k \in \mathbb{N}$, т.е. существует цепочка подмодулей $N_1 \subset N_2 \subset \cdots \subset N_{k-1} \subset N_k \subset \cdots$ - противоречие.

■

Определение 2. Модуль M, удовлетворяющий условиям (1), (2) называется *нётеровым*.

Нётеровы модули ближе всего по своим свойствам к конечным векторным пространствам (которые являются нётеровыми модулями над полем).

Предложение 2. Пусть M – модуль, $N \subseteq M$ – подмодуль. Тогда: M нётеров $\Longleftrightarrow$ N и M/N нётеровы.

Доказательство.
$\Longrightarrow$:
Нётеровость N очевидна (любой подмодуль в N будет подмодулем и в M). Для доказательства нётеровости M/N рассмотрим каноническую проекцию π: $M \longrightarrow M/N$. Пусть $L \subseteq M/N$ – подмодуль, тогда $\pi^{-1}(L)$ – подмодуль в M, т.е. $\pi^{-1}(L) = Am_1 + \cdots + Am_n$, откуда следует, что $L = A\pi(m_1) + \cdots + A\pi(m_n)$, т.е. L конечно порожден. Следовательно, M/N нётеров.
$\Longleftarrow$:
Пусть $L \subseteq M$ – подмодуль, тогда $\pi(L) \subseteq M/N$ – подмодуль, порожденный конечным числом элементов $\overline{m}_i = \pi(m_i)$ $(i = 1, \dots, n)$.
Пусть $L_0 = Ker\ (\pi|_L) = L \cap N$. L_0 – подмодуль в N, следовательно, порожден конечным числом элементов $n_1, \dots, n_m$. Тогда

$$L = L_0 + Am_1 + \cdots + Am_n = An_1 + \cdots + An_m + Am_1 + \cdots + Am_n$$

Таким образом, L конечно порожден, а значит, M нётеров. ■

Следствие. Пусть $M = M_1 \oplus \cdots \oplus M_s$. Тогда M нётеров $\Leftrightarrow M_1, \dots, M_s$ нётеровы.

Доказательство.

При $s = 2$ имеем: $M/M_1 \simeq M_2$, а значит, можно применить предложение 2. Далее индукция по s. ■

Лекция 8. Нётеровы кольца.

На прошлой лекции мы показали, что необходимым условием является нётеровости модуля является его конечная порожденность. Поймем, когда это условие будет являться также и достаточным. Ограничимся классом коммутативных колец/алгебр.

Определение 1. Коммутативное ассоциативное кольцо/алгебра A с единицей *нётерово*, если регулярный A-модуль A нётеров, т.е. любой идеал $I \lhd A$ конечно порожден (как A-модуль) или, эквивалентно, любая возрастающая цепочка идеалов $I_1 \subseteq I_2 \subseteq \cdots \lhd A$ стабилизируется.

Предложение 1. Любой конечно порожденный модуль над нётеровым кольцом/алгеброй нётеров.

Доказательство.
Пусть M – конечно порожденный модуль, тогда (см. прошлую лекцию) $M \simeq F/N$, где F – свободный конечно порожденный модуль, т.е. $F \simeq A^{\oplus n}$. Так как A нётерово, то и F нётеров, а значит, и M нётеров. ■

Таким образом, для модулей над нётеровыми кольцами конечная порожденность равносильна нётеровости. Возникает естественный вопрос – какие кольца/алгебры являются нётеровыми.

Предложение 2. Если кольцо/алгебра A нётерово, $I \lhd A$, то A/I нётерово.

Доказательство.
Рассмотрим A/I как циклический A-модуль:

- $a(b + I) = ab + I$
- порождающий элемент: $1 + I$

Далее применим предложение 1 – получим, что A/I – нётеров A-модуль, а значит, A/I – нётеров A/I-модуль. ■

Теорема Гильберта о базисе идеала. Если кольцо A нётерово, то кольцо многочленов $A[x]$ нётерово.

Доказательство.
Пусть $I \lhd A[x]$. Рассмотрим $\hat{I} = \{a \in A \mid \exists f = ax^n + \cdots \in I\}$ – множество всех старших коэффициентов многочленов, лежащих в I. Проверим, что $\hat{I} \lhd A$:

- $a, b \in \hat{I} \Longrightarrow \exists f = ax^n + \cdots \in I$, $\exists g = ax^m + \cdots \in I$. Без ограничения общности можем считать, что $n \geq m$, тогда $f + gx^{n-m} = (a+b)x^n + \cdots \in I$, откуда следует, что $a + b \in \hat{I}$
- $c \in A \Longrightarrow cf = cax^n + \cdots \in I$, откуда следует, что $ca \in \hat{I}$

Так как A нётерово, то $\hat{I}$ конечно порожден: $\hat{I} = Aa_1 + \cdots + Aa_s$ и $\exists f_i = a_i x^{n_i} + \cdots \in I$. Положим $n = \max\{n_1, \dots, n_s\}$.

Теперь рассмотрим $A[x]_{<n}$ – свободный A-подмодуль в $A[x]$, состоящий из многочленов степени меньше n. Имеем: $A[x]_{<n} = A \oplus Ax \oplus \cdots \oplus Ax^{n-1}$ – свободный конечно порожденный A-модуль, следовательно, $A[x]_{<n}$ нётеров (по предложению 1). Тогда $I_{<n} = I \cap A[x]_{<n}$ – A-подмодуль, следовательно, $I_{<n}$ порожден конечным числом элементов $g_1, \dots, g_r$.

Получаем $\forall f \in I$: $f = ax^n + \cdots$ $\exists b_1, \dots, b_s \in A$: $a = a_1 b_1 + \cdots + a_s b_s$. Если $m \geq n$, то $f = b_1 x^{m-n_1} f_1 + \cdots + b_s x^{m-n_s} f_s + h$, где $h \in I$, $\deg h < n$. Рассуждая так же для h, и так далее, в итоге получим $f = h_1 f_1 + \cdots + h_s f_s + g$, где $h_i \in A[x]$, $g \in I_{<n}$. Отсюда следует, что $\exists\, c_1, \dots, c_r \in A$: $g = c_1 g_1 + \cdots + c_r g_r$.

Следовательно, I порожден элементами $f_1, \dots, f_s, g_1, \dots, g_r$. ■

Следствие 1. $K[x_1, \dots, x_n]$ (K – поле) и $\mathbb{Z}[x_1, \dots, x_n]$ нётеровы. Аналогично для любого кольца $A[x_1, \dots, x_n]$, где A нётерово.

Доказательство – по индукции. ■

Следствие 2. Любое конечно порожденное коммутативное ассоциативное кольцо /алгебра с единицей нётерово.

Доказательство.
Такие кольца/алгебры являются факторкольцами/факторалгебрами колец/алгебр из следствия 1. Комбинируя это соображение с предложением 2, получаем требуемое. ■

Определение 2. Коммутативное ассоциативное кольцо с единицей без делителей нуля A называется *кольцом главных идеалов*, если любой идеал $I \lhd A$ – *главный*, т.е. порожден одним элементом: $I = Aa$.

Примеры колец главных идеалов:

- $\mathbb{Z}$
- $K[x]$ (K – поле)
- Любое евклидово кольцо

Важное свойство колец главных идеалов – однозначное разложение любого элемента кольца на простые множители.

Определение 3. Элемент $p \in A$ *прост*, если p необратим, и его нельзя разложить в произведение необратимых множителей: $p \notin A^{\times}$ и $\nexists$ разложения $p = ab$, $a, b \notin A^{\times}$.

Теорема. Пусть A – кольцо главных идеалов. Тогда $\forall a \in A$, $a \notin A^{\times}$ существует разложение $a = p_1 \cdots p_n$ (p_i - простые), единственное с точностью до перестановки множителей и их умножения на обратимые элементы кольца.

Доказательство.
Существование: от противного. Пусть a не разложим на простые множители $\Longrightarrow a$ не прост $\Longrightarrow a = a_1 b_1$, где $a_1, b_1 \notin A^{\times}$. Один из множителей (например, a_1) не разложим на простые множители (иначе бы a разлагался на простые множители) $\Longrightarrow a_1$ не прост $\Longrightarrow$ $a_1 = a_2 b_2$, где $a_2, b_2 \notin A^{\times}$. Один из множителей (например, a_2) не разложим на простые множители и т.д.

В итоге получаем последовательность $a_1, a_2, \ldots \in A$, такую что $a_i = a_{i+1} b_{i+1}$, $a_{i+1}, b_{i+1} \notin A^{\times}$. Отсюда, в частности, следует, что a_i не делит a_{i+1}, а это означает, что имеется цепочка вложенных идеалов $Aa_1 \subset Aa_2 \subset \cdots \subset Aa_i \subset Aa_{i+1} \subset \cdots$, которая не стабилизируется, что противоречит нётеровости.

Единственность: введем понятие наибольшего общего делителя элементов: НОДом элементов $a_1, \ldots, a_s \in A$ называется $d \in A$, такой что $d \mid a_1, \ldots, a_s$ и $d \vdots c$, $\forall c \mid a_1, \ldots, a_s$.

Лемма 1. Для любого набора $a_1, \ldots, a_s$ в кольце главных идеалов A существует их НОД.

Доказательство леммы 1.
Рассмотрим $I = Aa_1 + \cdots + Aa_s$. Это главный идеал (т.к. A – кольцо главных идеалов), следовательно, $I = Ad$ для некоторого $d \in A$. Докажем, что $d = \text{НОД}(a_1, \ldots, a_s)$. В самом деле: $a_1, \ldots, a_s \vdots d = a_1 b_1 + \cdots + a_s b_s$ для некоторых $b_1, \ldots, b_s \in A$, поэтому если $c \mid a_1, \ldots, a_s$, то $c \mid d$. ■

Лемма 2. Если p прост и $p \mid ab$, то $p \mid a$ или $p \mid b$.

Доказательство леммы 2.
Либо $p \mid a$ (и лемма 2 доказана), либо $\text{НОД}(p, a)$ обратим (можно считать, что $\text{НОД}(p, a) = 1$). Тогда $\text{НОД}(p, a) = 1 = up + va$ для некоторых $u, v \in A$. Домножив на b, получим, что $b = upb + vab$ делится на p (т.к. $upb \vdots p$ и $vab \vdots p$), т.е. $p \mid b$. ■

Предположим, что существует два разложения a на простые множители: $a = p_1 \cdots p_n$ и $a = q_1 \cdots q_m$. По лемме 2, $p_1 \mid q_i$ для некоторого i – без ограничения общности можно считать, что $p_1 \mid q_1$, тогда $p_1 = q_1 u$, где $u \in A^\times$. Получаем $p_2 \cdots p_n = (uq_2) \cdots q_m$, далее используем индукцию по числу множителей в разложении. ■

Конечно порожденные модули над кольцами главных идеалов.

Конечно порожденные модули над кольцом главных идеалов похожи на конечно порожденные абелевы группы (которые являются их частным случаем), которые мы рассматривали ранее в курсе Алгебра-3. Пусть A – кольцо главных идеалов.

Предложение 3. Пусть F – свободный конечно порожденный A-модуль, $N \subseteq F$ – подмодуль. Тогда N свободен, и существует базис $\{f_1, \dots, f_n\}$ для F, такой что $\{u_1 f_1, \dots, u_m f_m\}$ – базис N для некоторых $u_1, \dots, u_m \in A$, $u_i \mid u_{i+1}$, $\forall i < m$.

Доказательство.
Так как F нётеров, то N конечно порожден: $N = An_1 + \cdots + An_k$. Выберем базис $\{f_1, \dots, f_n\}$ в F произвольно, тогда $n_j = a_{1j} f_1 + \cdots + a_{nj} f_n$ для некоторых $a_{ij} \in A$. Возникает матрица

$$\begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nk} \end{pmatrix},$$

по столбцам которой записаны координаты порождающих элементов подмодуля N в выбранном базисе модуля F.

Введем понятие *квазиэлементарного преобразования* системы $\{m_1, \dots, m_l\}$ элементов A-модуля: это замена $\{m_i, m_j\}$ на $\{m_i', m_j'\}$ так, что $m_i' = am_i + bm_j$ и $m_j' = cm_i + dm_j$, при этом $ad - bc \in A^\times$.

Частным случаем квазиэлементарных преобразований являются привычные элементарные преобразования:

- ЭП 1: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$
- ЭП 2: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- ЭП 3: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $a \in A^\times$

Лемма 3. Любую матрицу с элементами из A можно с помощью квазиэлементарных преобразований (КЭП) строк и столбцов привести к виду

$$\begin{pmatrix} u_1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \dots & \dots & \dots \\ 0 & & u_m & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \ddots & \dots \\ 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix}, \quad u_i \mid u_{i1}$$

Эту лемму мы докажем на следующей лекции.

Квазиэлементарным преобразованиям строк матрицы $\begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nk} \end{pmatrix}$ соответствуют замены базиса в F, а квазиэлементарным преобразованиям столбцов этой матрицы соответствуют замены порождающей системы в N. После замен по лемме 3 можно считать, что $n_i = u_i f_i$ при $i \leq m$ и $n_i = 0$ при $i > m$. Отсюда следует, что $\{u_1 f_1, \dots, u_m f_m\}$ – базис N. ■

Лекция 9. Основная теорема о структуре конечно порожденных модулей над кольцом главных идеалов.

Лемма. Любую матрицу с элементами из A можно с помощью квазиэлементарных преобразований (КЭП) строк и столбцов привести к виду

$$\begin{pmatrix} u_1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \dots & \dots & \dots \\ 0 & & u_m & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \ddots & \dots \\ 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix}, \quad u_i \mid u_{i1}$$

Доказательство.
Будем считать, что $\exists a_{ij} \neq 0$. С помощью ЭП 2 типа добьемся того, чтобы $a_{11} \neq 0$.

- 1) Если $a_{i1}, a_{j1} \vdots a_{11}, \forall i,j > 1$, то с помощью ЭП 1 добьемся, чтобы $a_{i1} = a_{j1} = 0$, $\forall i,j > 1$.
- 2) Если $\exists a_{i1}$ $(i > 1)$, не делящееся на a_{11}, то положим НОД$(a_{11}, a_{i1}) = a'_{11}$, тогда $a'_{11} = ua_{11} + va_{i1}$ и матрица $\begin{pmatrix} u & v \\ -\frac{a_{i1}}{a'_{11}} & \frac{a_{11}}{a'_{11}} \end{pmatrix}$ обратима: $\begin{vmatrix} u & v \\ -\frac{a_{i1}}{a'_{11}} & \frac{a_{11}}{a'_{11}} \end{vmatrix} = 1$.

Применим КЭП $\{m_1, m_i\} \longrightarrow \{m'_1, m'_i\}$ (под m_i понимаем строки матрицы):

$$m'_1 = um_1 + vm_i = (a'_{11}, \dots)$$
$$m'_i = -\frac{a_{i1}}{a'_{11}} m_1 + \frac{a_{11}}{a'_{11}} m_i = (0, \dots)$$

- мы сумели заменить угловой элемент a_{11} на его НОД с другим элементом из первого столбца, при этом a_{11} делится на a'_{11}, но a'_{11} не делится на a_{11}. Это, в частности, означает, что $Aa_{11} \subset Aa'_{11}$.

Если $\exists a_{1j}$ $(j > 1)$, не делящееся на a_{11}, то аналогично действуем со столбцами. В результате получим цепочку $Aa_{11} \subset Aa'_{11} \subset Aa''_{11} \subset \cdots$, которая стабилизируется (так как A нётерово). В итоге придем к случаю 1), т.е. получим матрицу вида:

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & a_{ij} & \\ 0 & & & \end{array}\right)$$

- 3) Если существует a_{ij}, которое не делится на a_{11}, то с помощью ЭП 1 типа столбцов можно добиться, чтобы a_{i1} не делилось на a_{11}, после чего действовать, как в шаге 2). В итоге придем к ситуации, когда $a_{ij} \vdots a_{11}$, $\forall i, j > 1$.

Доказательство завершается индукцией по размеру матрицы. ■

Эта лемма заершает доказательство предложения 3 из предыдущей лекции. Перейдем к доказательству основной теоремы о структуре конечно порожденных модулей над кольцом главных идеалов.

Теорема. Для любого конечно порожденного модуля M над кольцом главных идеалов A существуют изоморфизмы

$$M \simeq A/Au_1 \oplus \cdots \oplus A/Au_m \oplus \underbrace{A \oplus \cdots \oplus A}_{r \text{ слагаемых}}$$
$$M \simeq A/Ap_1^{k_1} \oplus \cdots \oplus A/Ap_s^{k_s} \oplus \underbrace{A \oplus \cdots \oplus A}_{r \text{ слагаемых}}$$

где $u_1, \dots, u_m \in A$, $u_i \mid u_{i+1}$, $\forall i < m$; $p_1, \dots, p_s \in A$ – простые элементы.

При этом $r = rk(M)$ (*ранг* модуля) не зависит от разложения, а $u_1, \dots, u_m$ (*инвариантные множители*) и $p_1^{k_1}, \dots, p_s^{k_s}$ (*элементарные делители*) не зависят от разложения с точностью до допустимых перестановок и умножения на обратимые элементы.

Доказательство.
Существование. Имеет место изоморфизм $M \simeq F/N$, где F свободный модуль, $N \subseteq F$. Выберем базисы в F и в N как в предложении 3, доказанном на прошлой лекции, получим:

- $F = \underbrace{A \oplus \cdots \oplus A}_{m \text{ слагаемых}} \oplus \underbrace{A \oplus \cdots \oplus A}_{n-m \text{ слагаемых}}$,
- $N = Au_1 \oplus \cdots \oplus Au_m$,

тогда

$$F/N \simeq A/Au_1 \oplus \cdots \oplus A/Au_m \oplus \underbrace{A \oplus \cdots \oplus A}_{r = n-m \text{ слагаемых}}$$

Для того, чтобы получить второе разложение, понадобится следующая лемма:

Лемма. Если $a = bc$, НОД$(b, c) = 1$, то $A/Aa \simeq A/Ab \oplus A/Ac$.

Доказательство леммы.
Рассмотрим гомоморфизм A-модулей

$$\varphi\colon A \longrightarrow A/Ab \oplus A/Ac$$
$$a \mapsto (a + Ab, a + Ac)$$

Докажем, что φ сюръективен: так как НОД$(b, c) = 1$, то $1 = ub + vc$ для некоторых $u, v \in A$. Далее $\forall y, z \in A$ положим $a = yvc + zub$, тогда:

- $a + Ab = yvc + Ab = y(1 - ub) + Ab = y + Ab$
- аналогично $a + Ac = z + Ac$

- для любых смежных классов из A/Ab и A/Ac построили их прообраз при гомоморфизме φ, следовательно, φ сюръективен.

При этом $Ker\,\varphi = Ab \cap Ac = Aa$ – остается применить основную теорему о гомоморфизмах модулей. ■

Продолжим доказательство существования. Разложим каждый u_i в произведение $u_i = wp_1^{k_1} \cdots p_t^{k_t}$, где $p_1, \dots, p_t$ – простые элементы, $p_j \nmid p_k$ при $j \neq k$, а $w \in A^\times$ (можно отбросить). По лемме, доказанной выше, получаем:

$$A/Au_i \simeq A/Ap_1^{k_1} \oplus \cdots \oplus A/Ap_t^{k_t}$$

Объединяя такие выражения для каждого слагаемого в разложении F/N, получаем второе разложение M.

<u>Единственность</u>. Обозначим $K = Quot(A)$ (поле частных кольца A). Имеем: $M \underset{A}{\otimes} K$ – векторное пространство над K, при этом

$$M \underset{A}{\otimes} K \simeq \left(A/Au_1 \underset{A}{\otimes} K\right) \oplus \cdots \oplus \left(A/Au_m \underset{A}{\otimes} K\right) \oplus \left(A \underset{A}{\otimes} K\right)^{\oplus r}$$

Но все слагаемые вида $A/Au_i \underset{A}{\otimes} K$ равны нулю, в самом деле:

$$(a + Au_i) \otimes q = (a + Au_i) \otimes u_i \frac{q}{u_i} = (u_i + Au_i) \otimes \frac{q}{u_i} = 0 \otimes \frac{q}{u_i} = 0$$

Так как $A \underset{A}{\otimes} K = K$, получаем $M \underset{A}{\otimes} K \simeq K^{\oplus r}$, т.е. $r = \dim M \underset{A}{\otimes} K$ и не зависит от разложения.

Для того, чтобы доказать, что инвариантные множители не зависят от разложения, введем понятие аннулятора. *Аннулятор* элемента $v \in M$: $Ann(v) = \{a \in A \mid av = 0\}$. Легко видеть, что $Ann(v) \lhd A$.

Например, для $A/Au_i \ni v = 1 + Au_i$ имеем: $Ann(v) = Au_i$. Для произвольного $v \in M$, $v = (a_1 + Au_1, \dots, a_m + Au_m, b_1, \dots, b_r)$ возможны две ситуации:

- $\exists b_i \neq 0$, тогда $Ann(v) = \{0\}$
- $b_1 = \dots = b_r = 0$, тогда $Ann(v) \supseteq Au_m$

Обозначим совокупность элементов из M, имеющих ненулевой аннулятор $Tor(M) = \{v \in M \mid Ann(v) \neq \{0\}\}$ – *подмодуль кручения* (*периодическая часть*). Имеем:

$$Tor(M) = A/Au_1 \oplus \dots \oplus A/Au_m$$

- не зависит от разложения. Далее без ограничения общности можно считать, что $M = Tor(M)$. Отсюда следует, что Au_m – наименьший из аннуляторов элементов M, т.е. Au_m определен однозначно, и u_m определен однозначно с точностью до обратимого множителя.

Имеем цепочку вложенных идеалов: $Au_1 \supseteq Au_2 \supseteq \dots \supseteq Au_k \supset Au_{k+1} = \dots = Au_m$. Обозначим $M \supseteq M_0$ подмодуль, порожденный элементами с наименьшим аннулятором. Имеем:

- $M_0 = A/Au_{k+1} \oplus \dots \oplus A/Au_m$ – не зависит от разложения,
- $M/M_0 \cong A/Au_1 \oplus \dots \oplus A/Au_k$ – не зависит от разложения.

Рассуждая индукцией по числу инвариантных множителей, можно считать, что набор $u_1, \dots, u_k$ определен однозначно (с точностью до допустимых перестановок и умножения на обратимые элементы).

Осталось доказать, что набор $u_1, \dots, u_m$ определено однозначно. Выберем простой $p \mid u_m$.

Лемма. A/Ap – поле.

Доказательство леммы.
Если $a + Ap \neq 0$, то a не делится на p, поэтому НОД$(a, p) = 1 = ua + vp$, откуда следует, что $u + Ap = (a + Ap)^{-1}$. ■

Теперь заметим, что $M_0 \underset{A}{\otimes} A/Ap$ можно рассматривать как тензорное произведение над A/Au_m (так как структура A-модуля сводится к структуре модуля над A/Au_m):

$$M_0 \underset{A}{\otimes} A/Ap = M_0 \underset{A/Au_m}{\otimes} A/Ap \simeq (A/Ap)^{\oplus(m-k)}$$

- векторное пространство над полем A/Ap, размерности $m - k$. Так как размерность пространства является его инвариантом, то $m - k$ определено однозначно.

Следовательно, набор инвариантных множителей $u_1, \dots, u_m$ определен однозначно (с точностью до допустимых перестановок и умножения на обратимые элементы).

Осталось доказать, что элементарные делители не зависят от разложения. Сгруппируем их по одинаковым (с точностью до обратимых множителей) простых множителей:

$$\begin{gathered} p_1^{k_{11}}, p_1^{k_{12}}, \dots, p_1^{k_{1m_1}} \\ p_2^{k_{21}}, p_2^{k_{22}}, \dots, p_2^{k_{2m_2}} \\ \vdots \\ p_t^{k_{t1}}, p_t^{k_{t2}}, \dots, p_t^{k_{tm_t}} \end{gathered}$$

так, что:

- p_i простые
- $p_i \nmid p_j$ при $i \neq j$
- $k_{i1} \geq k_{i2} \geq \dots \geq k_{im_i}$
- $m = m_1 \geq m_2 \geq \dots \geq m_t$

и рассмотрим произведение элементов в каждом столбце: положим

$$u_{m+1-j} = \prod_i p_i^{k_{ij}}$$

Имеем: $u_1 \mid u_2 \mid \dots \mid u_m$.

Теперь рассмотрим $\bigoplus_i A/Ap_i^{k_{ij}}$ – по лемме, доказанной в начале доказательства теоремы, имеем:

$$\bigoplus_i A/Ap_i^{k_{ij}} \simeq A/Au_{m+1-j},$$

откуда следует, что

$$Tor(M) = \bigoplus_{i,j} A/Ap_i^{k_{ij}} \simeq A/Au_1 \oplus \dots \oplus A/Au_m,$$

т.е. $u_1, \dots, u_m$ – инвариантные множители, а они определены однозначно. Поэтому набор $p_i^{k_{ij}}$ тоже определен однозначно. Теорема полностью доказана. ■

Приложения теоремы.

1) $A = \mathbb{Z}$, M – конечно порожденная абелева группа. M есть прямая сумма бесконечных и примарных циклических групп.

2) $A = K[x]$, $M = V$ – векторное пространство над полем K, $\dim V < \infty$. Линейный оператор $\mathcal{A} \in L(V)$ позволяет задать структуру $K[x]$-модуля на V:

$$xv = \mathcal{A}v$$
$$fv = f(\mathcal{A})v$$

На V оператор $\mathcal{A}$ имеет блочно-диагональную матрицу, составленную из блоков A_i – *нормальная форма Фробениуса* (подробнее см. на следующей лекции).

Лекция 10. Теория представлений.

Нормальная форма Фробениуса линейного оператора.

Пусть V – векторное пространство над полем K, $\dim V < \infty$. Линейный оператор $\mathcal{A} \in L(V)$ позволяет задать структуру $K[x]$-модуля на V:

$$xv = \mathcal{A}v$$
$$fv = f(\mathcal{A})v$$

Доказанная на прошлой лекции теорема о структуре конечно порожденных модулей над кольцом главных идеалов утверждает, что

$$V = K[x]/K[x]g_1 \oplus \cdots \oplus K[x]/K[x]g_m,$$

где

- $g_1, \dots, g_m \in K[x]$, $g_i(x) = x^{n_i} + a_{i1}x^{n_i-1} + \cdots + a_{in_i}$
- $g_1 \mid g_2 \mid \dots \mid g_m$

Т.е. $V = V_1 \oplus \cdots \oplus V_m$, где $V_1, \dots, V_m$ – $\mathcal{A}$-инвариантные подпространства, $V_i \simeq K[x]/K[x]g_i$ как $K[x]$-модуль. В базисе V_i, соответствующем смежным классам $1, x, x^2, \dots, x^{n_i-1}$ оператор $\mathcal{A}|_{V_i}$ имеет матрицу

$$A_i = \begin{pmatrix} 0 & \vdots & \vdots & \dots & 0 & -a_{in_i} \\ 1 & 0 & \vdots & \dots & \dots & \vdots \\ 0 & 1 & 0 & \dots & \dots & \vdots \\ \vdots & 0 & 1 & \ddots & \dots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 & -a_{i2} \\ 0 & 0 & 0 & \dots & 1 & -a_{i1} \end{pmatrix}$$

В соответствующем базисе V оператор $\mathcal{A}$ имеет блочно-диагональную матрицу, составленную из блоков A_i – *нормальная форма Фробениуса* (определена однозначно).

Замечание: $g_m = \mu_{\mathcal{A}}$ – минимальный многочлен оператора $\mathcal{A}$.

Упражнение. Показать, что $g_1 \cdots g_m = \chi_{\mathcal{A}}$ – характеристический многочлен оператора $\mathcal{A}$.

В формулировке теоремы о структуре конечно порожденных модулей над кольцом главных идеалов присутствовало два разложения модуля M: первому соответствовало разложение $V = V_1 \oplus \cdots \oplus V_m$, приведенное выше, второму разложению соответствует

$V = U_1 \oplus \cdots \oplus U_s$, где $U_i \simeq K[x]/K[x]p_j^{k_j}$ как $K[x]$-модуль, а p_j – неприводимый многочлен.

Это разложение (в отличие от первого) существенно зависит от поля K. Если поле K алгебраически замкнуто (или хотя бы все собственные значения $\mathcal{A}$ лежат в K), тогда $p_j(x) = x - \lambda_j$ $(j = 1, \dots, s)$. В базисе U_j, соответствующем смежным классам $(x-\lambda_j)^{k_j-1}, (x-\lambda_j)^{k_j-2}, \dots, (x-\lambda_j)^2, x-\lambda_j, 1$ оператор $\mathcal{A}|_{U_j}$ имеет матрицу

$$J_j = \begin{pmatrix} \lambda_j & 1 & \dots & \dots & 0 & 0 \\ 0 & \lambda_j & 1 & \dots & \dots & \vdots \\ 0 & 0 & \lambda_j & \ddots & \dots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \dots & \dots & \dots & \ddots & \lambda_j & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda_j \end{pmatrix}$$

- жорданова клетка, соответствующая собственному значению λ_j. В соответствующем базисе V оператор $\mathcal{A}$ имеет блочно-диагональную матрицу, составленную из блоков J_j – это привычная нам жорданова нормальная форма линейного оператора. Единственность ЖНФ следует из единственности набора элементарных делителей. ■

Теория представлений.

Перейдем к новой теме, которая близка по духу к теории модулей – к теории представлений. В прошлом семестре мы уже изучали линейные представления групп (в основном конечных), но теория представлений носит более общий характер.

Отметим, что понятие линейного представления осмысленно для тех типов математических структур, для которых на множестве линейных операторов есть структура такого же типа. Перечислим некоторые из этих структур. Пусть V – векторное пространство над K, $L(V)$ – множество линейных операторов на V. Имеем:

- $L(V)$ - множество
- $L(V)$ - векторное пространство над K
- $L(V)$ - ассоциативная алгебра (с 1) над K
- $L(V)$ - алгебра Ли
- $L(V)$ - йорданова алгебра

  ...

Также $L(V)$ – полугруппа, которая содержит группу обратимых линейных операторов $GL(V)$. Имеем:

- $GL(V)$ – группа
- $GL(V)$ - группа Ли (при $K = \mathbb{R}$ или $\mathbb{C}$)
- $GL(V)$ - алгебраическая группа

  ...

Определение. *Линейное представление* математической структуры S в векторном пространстве V – это гомоморфизм $\mathcal{R}$: $S \longrightarrow L(V)$.

Например:

- для множеств: $\mathcal{R}$ - произвольное отображение
- для векторных пространств: $\mathcal{R}$ - линейное отображение
- для ассоциативных алгебр: $\mathcal{R}$ - гомоморфизм алгебр
  - - с единицей: $\mathcal{R}(1) = \mathcal{E}$
- для групп: $\mathcal{R}$: $S \longrightarrow GL(V)$ - гомоморфизм групп

  ...

Прежде чем мы перейдем к изучению линейных представлений конкретных структур, обсудим вещи, общие для любых линейных представлений.

Терминология:

- V – *пространство представления*
- $dim\,\mathcal{R} = dim\,V$ – *размерность* представления
- $\mathcal{R}(s)$, $(s \in S)$ – *операторы представления*

Если V конечномерно, то параллельно с линейными можно рассматривать матричные представления.

- *Матричное представление* структуры S над полем K – это гомоморфизм R: $S \longrightarrow Mat_n(K)$.

Между матричными и линейными представлениями существует естественная связь, а именно – выбор базиса $(e_1, \dots, e_n)$ в пространстве V устанавливает взаимно-однозначное соответствие между линейными операторами и матрицами размера $n \times n$:

$$L(V) \simeq Mat_n(K)$$

$$\begin{tikzcd} & L(V) \arrow[d, equal, "\text{выбор базиса}"] \\ S \arrow[ur, "\mathcal{R}"] \arrow[r, "R"'] & Mat_n(K) \end{tikzcd}$$

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Таким образом, возникает взаимно-однозначное соответствие между линейными и матричными представлениями соответствующей размерности: $\mathcal{R} \leftrightarrow R$. Подчеркнем, однако, что это соответствие не каноническое, а зависит от базиса в пространстве V. Замена базиса $(e_1, \dots, e_n) \xrightarrow{C} (e_1', \dots, e_n')$ задает *эквивалентное* матричное представление R', связанное с представлением R формулой:

$$R'(s) = C^{-1}R(s)C, \ \ \forall s \in S$$

Пусть $\mathcal{R}\colon\ S \longrightarrow L(V)$ – линейное представление.

- Подпространство $U \subseteq V$ называется *инвариантным*, если $\forall s \in S, \forall u \in U$: $\mathcal{R}(s)u \in U$
- *Подпредставление*
$$\mathcal{P} = \mathcal{R}|_U\colon\ S \longrightarrow L(U)$$
$$\mathcal{P}(s) = \mathcal{R}(s)|_U$$
- *Факторпредставление*
$$\mathcal{F} = \mathcal{R}/\mathcal{P}\colon\ S \longrightarrow L(V/U)$$
$$\mathcal{F}(s)(v + U) = \mathcal{R}(s)v + U$$

В согласованном базисе $(\underbrace{e_1, \dots, e_m}_{\text{базис } U}, e_{m+1}, \dots, e_n)$ пространства V матрица оператора $R(s)$ выглядит так:

$$R(s) = \left(\begin{array}{c|c} P(s) & * \\ \hline 0 & F(s) \end{array}\right)$$

- *Прямая сумма* линейных представлений: $\mathcal{R} = \mathcal{R}_1 \oplus \dots \oplus \mathcal{R}_m$, если V разлагается в прямую сумму инвариантных подпространств: $V = V_1 \oplus \dots \oplus V_m$ и $\mathcal{R}|_{V_i} = \mathcal{R}_i$ $(i = 1, \dots, m)$

В базисе, согласованном с $V_1, \dots, V_m$, матрица оператора $\mathcal{R}(s)$ будет иметь блочно-диагональный вид (блоки – матрицы операторов $\mathcal{R}_i(s)$):

$$R(s) = \left(\begin{array}{c|c|c} R_1(s) & & 0 \\ \hline & \ddots & \\ \hline 0 & & R_m(s) \end{array}\right)$$

- Линейное представление $\mathcal{R}\colon S \longrightarrow L(V)$ *приводимо*, если существует инвариантное подпространство $U \subset V,\ U \neq \{0\}$

- Линейное представление $\mathcal{R}\colon S \longrightarrow L(V)$ *неприводимо*, если $V \neq \{0\}$ и $\mathcal{R}$ не является приводимым (т.е. в V нет нетривиальных инвариантных подпространств)
- Линейное представление $\mathcal{R}\colon S \longrightarrow L(V)$ *вполне приводимо*, если для любого инвариантного подпространства $U \subseteq V$ существует инвариантное дополнительное подпространство $W \subseteq V$, такое что $V = U \oplus W$

В согласованном базисе $(\underbrace{e_1, \dots, e_m}_{\text{базис } U}, \underbrace{e_{m+1}, \dots, e_n}_{\text{базис } W})$ пространства V матрица оператора $R(s)$ будет блочно-диагональной:

$$R(s) = \left(\begin{array}{c|c} R|_U(s) & 0 \\ \hline 0 & R|_W(s) \end{array}\right)$$

Предложение. Подпредставление вполне приводимого представления вполне приводимо.

Доказательство.
Пусть $\mathcal{R}$ вполне приводимо, $U \subseteq V$ – инвариантное подпространство, $\mathcal{P} = \mathcal{R}|_U$ – подпредставление $\mathcal{R}$. Пусть $U' \subseteq U$ – инвариантное подпространство. Возьмем дополнительное инвариантное подпространство $W \subseteq V$, такое что $V = U' \oplus W$, тогда $W' = U \cap W$ – тоже инвариантное подпространство. Докажем, что $U = U' \oplus W'$. Происходящее иллюстрирует рис. 10.1:

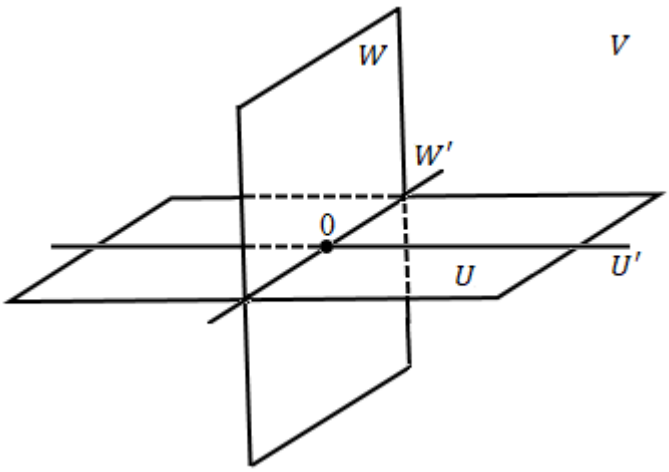


Рис. 10.1. Иллюстрация к предложению

Нужно доказать, что любой вектор $u \in U$ единственным способом разлагается в сумму векторов из U' и W'. В самом деле, так как $V = U' \oplus W$, то $\forall u \in V$ существует единственное разложение

$$u = u' + w, \;\; u' \in U', w \in W$$

Так как $u \in U$ и $u' \in U' \subseteq U$, то и $u - u' = w \in U$. Тогда $u - u' = w \in U \cap W = W'$. Это и означает, что $U = U' \oplus W'$. Следовательно, $\mathcal{P}$ тоже вполне приводимо. ■

Теорема. Конечномерное линейное представление $\mathcal{R}$ вполне приводимо $\Leftrightarrow$ $\mathcal{R} = \mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_m$, где $\mathcal{R}_i$ неприводимы.

Доказательство.
$\Longrightarrow$:
Докажем утверждение индукцией по $dim\, \mathcal{R}$.

База индукции: $V = \{0\}$ или $\mathcal{R}$ неприводимо $\Longrightarrow$ доказывать нечего (если $V = \{0\}$, то $dim\, \mathcal{R} = 0$ – нулевое пространство является прямой суммой нулевого числа слагаемых, а если $\mathcal{R}$ неприводимо, то необходимое разложение уже получено).

Шаг индукции: если $\mathcal{R}$ приводимо, то существует нетривиальное инвариантное подпространство $U \subset V$, $U \neq \{0\}$. Так как $\mathcal{R}$ вполне приводимо, то существует дополнительное инвариантное подпространство $W \subset V$, такое что $V = U \oplus W$. Тогда

$$\mathcal{R} = \mathcal{R}|_U \oplus \mathcal{R}|_W$$

Но $\mathcal{R}|_U$ и $\mathcal{R}|_W$ - вполне приводимые представления (по предложению, доказанному выше) меньшей размерности, и к ним можно применить предположение индукции.

$\Longleftarrow$:
Пусть $V = V_1 \oplus \cdots \oplus V_m$ и $\mathcal{R}|_{V_i} = \mathcal{R}_i$ неприводимы. Пусть $U \subseteq V$ – инвариантное подпространство, рассмотрим инвариантные подпространства $W_{i_1 \cdots i_k} = V_{i_1} \oplus \ldots \oplus V_{i_k}$ ($i_1, \ldots, i_k$ попарно различны, $k \geq 0$) и среди $W_{i_1 \cdots i_k}$ выберем максимальное, такое что $W_{i_1 \cdots i_k} \cap U = \{0\}$. Далее $\forall i \neq i_1, \ldots, i_k$ рассмотрим $W_{i_1 \cdots i_k i}$ – его пересечение с U будет ненулевым: $W_{i_1 \cdots i_k i} \cap U \ni u \neq 0$.

Имеем: $u = v_{i_1} + \cdots + v_{i_k} + v_i$ ($v_j \in V_j$), откуда $v_i = u - v_{i_1} - \cdots - v_{i_k} \in U + W_{i_1 \cdots i_k}$, причем $v_i \neq 0$ (так как иначе $W_{i_1 \cdots i_k} \cap U \neq \{0\}$) и $U \oplus W_{i_1 \cdots i_k}$ – инвариантное подпространство (так как оба подпространства инвариантные и $W_{i_1 \cdots i_k} \cap U = \{0\}$).

Так как $v_i \in V_i$ и $v_i \in U \oplus W_{i_1 \cdots i_k}$, то $v_i \in \left(U \oplus W_{i_1 \cdots i_k}\right) \cap V_i$. Но из того, что $\mathcal{R}_i$ неприводимо, следует, что $V_i \subseteq U \oplus W_{i_1 \cdots i_k}$. Таким образом, мы доказали, что $\forall i = 1, \ldots, m$ выполнено $V_i \subseteq U \oplus W_{i_1 \cdots i_k}$, откуда следует, что $U \oplus W_{i_1 \cdots i_k} = V$, т.е. мы сконструировали инвариантное дополнение к произвольному инвариантному подпространству $U \subseteq V$, что означает, что представление $\mathcal{R}$ вполне приводимо. ■

- *Гомоморфизм* линейного представления $\mathcal{R}\colon\ S \longrightarrow L(V)$ в линейное представление $\mathcal{R}'\colon S \longrightarrow L(V')$ – это линейное отображение $\mathcal{C}\colon V \longrightarrow V'$, такое что $\forall s \in S$ выполнено:

$$\mathcal{C} \cdot \mathcal{R}(s) = \mathcal{R}'(s) \cdot \mathcal{C}$$

Другими словами, перестановка оператора представления через гомоморфизм $\mathcal{C}$ превращает одно представление в другое. Происходящее можно изобразить в виде коммутативной диаграммы:

$$\begin{tikzcd} V \arrow[r, "\mathcal{C}"] \arrow[d, "\mathcal{R}(s)"'] & V' \arrow[d, "\mathcal{R}'(s)"] \\ V \arrow[r, "\mathcal{C}"] & V' \end{tikzcd}$$

- *Эндоморфизм* – это гомоморфизм из $\mathcal{R}$ в $\mathcal{R}$
- *Изоморфизм* – это взаимно однозначный гомоморфизм из $\mathcal{R}$ в $\mathcal{R}'$

Все гомоморфизмы из $\mathcal{R}$ в $\mathcal{R}'$ образуют векторное пространство $Hom(\mathcal{R}, \mathcal{R}')$. Все эндоморфизмы представления $\mathcal{R}$ образуют алгебру с единицей $End(\mathcal{R})$.

Если $\mathcal{C}\colon\ V \longrightarrow V'$ – изоморфизм линейных представлений, то $\mathcal{R}'(s) = \mathcal{C}\mathcal{R}(s)\mathcal{C}^{-1}$, $\forall s \in S$ – эта формула напоминает формулу для эквивалентного матричного представления при замена базиса $(e_1, \dots, e_n) \overset{C}{\to} (e_1', \dots, e_n')$, которую мы приводили выше. Это не случайно: выбор базиса в пространстве представления $\Leftrightarrow$ изоморфизм $V \simeq K^n$, изоморфизм линейного представления $\Leftrightarrow$ эквивалентность матричных представлений.

Лекция 11. Лемма Шура. Тензорное произведение представлений групп.

Лемма Шура. Пусть $\mathcal{R}, \mathcal{R}'$ – неприводимые представления. Тогда:

- (а) Любой гомоморфизм $\mathcal{C} \in Hom\,(\mathcal{R}, \mathcal{R}')$ – либо нулевой, либо изоморфизм,
- (б) $End\,(\mathcal{R})$ – алгебра с делением,
- (в) Если K алгебраически замкнуто, $\dim \mathcal{R} < \infty$, то $End\,(\mathcal{R}) = K$, т.е. любой эндоморфизм этого представления является скалярным оператором (т.е. оператором умножения на некоторую константу $\lambda \in K$): $\mathcal{C} = \lambda\mathcal{E}$.

Доказательство.
(а) Пусть $\mathcal{R}$: $S \longrightarrow L(V)$, $\mathcal{R}'$: $S \longrightarrow L(V')$. Условие $\mathcal{C} \in Hom\,(\mathcal{R}, \mathcal{R}')$ означает, что следующая диаграмма коммутативна:

$$\begin{tikzcd} V \arrow[r, "\mathcal{C}"] \arrow[d, "\mathcal{R}(s)"'] & V' \arrow[d, "\mathcal{R}'(s)"] \\ V \arrow[r, "\mathcal{C}"] & V' \end{tikzcd}$$

Используя эту диаграмму, нетрудно заметить, что $Ker\,\mathcal{C} \subseteq V$ и $Im\,\mathcal{C} \subseteq V'$ - инвариантные подпространства. Так как $\mathcal{R}, \mathcal{R}'$ – неприводимые представления, то возможны следующие варианты:

- $Ker\,\mathcal{C} = V$, тогда $\mathcal{C} = 0$
- $Ker\,\mathcal{C} = \{0\}$, тогда $Im\,\mathcal{C} \neq \{0\}$, откуда следует, что $Im\,\mathcal{C} = V'$ и $\mathcal{C}$ – изоморфизм

(б) Следует из пункта а): любой ненулевой $\mathcal{C} \in Hom\,(\mathcal{R}, \mathcal{R}')$ обратим.

(в) Можно воспользоваться ранее доказанным фактом: над алгебраически замкнутым полем не существует нетривиальных конечномерных алгебр с делением, или доказать непосредственно: пусть $\mathcal{C} \in End\,(\mathcal{R})$, $\lambda \in K$ – собственное значение $\mathcal{C}$, тогда $\mathcal{C} - \lambda\mathcal{E} \in End\,(\mathcal{R})$. С другой стороны, $\mathcal{C} - \lambda\mathcal{E}$ вырожден, тогда из пункта б) следует, что $\mathcal{C} - \lambda\mathcal{E} = 0$, т.е. $\mathcal{C} = \lambda\mathcal{E}$. ■

Лемма Шура хорошо работает при изучении не только неприводимых, но и вполне приводимых представлений. Пусть $\mathcal{R}$: $S \longrightarrow L(V)$ – вполне приводимое конечномерное линейное представление. Тогда (см. теорему из прошлой лекции) $\mathcal{R} = \mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_m$, $V = V_1 \oplus \cdots \oplus V_m$, $\mathcal{R}_i = \mathcal{R}|_{V_i}$ неприводимы.

Определение. Пусть $\mathcal{P}\colon S \longrightarrow L(U)$ – произвольное неприводимое представление. *Кратностью* $\mathcal{P}$ в разложении $\mathcal{R} = \mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_m$ (обозначение: $(\mathcal{R}\colon \mathcal{P})$) назовем количество слагаемых $\mathcal{R}_i \simeq \mathcal{P}$. *Изотипная компонента* типа $\mathcal{P}$:

$$V_{(\mathcal{P})} = \bigoplus_{\mathcal{R}_i \simeq \mathcal{P}} V_i$$

Представления $\mathcal{R}|_{V_{(\mathcal{P})}} \simeq \underbrace{\mathcal{P} \oplus \cdots \oplus \mathcal{P}}_{(\mathcal{R}:\mathcal{P})}$ называются *изотипными*. При этом

$$V = \bigoplus_{(\mathcal{R}:\mathcal{P}) \neq 0} V_{(\mathcal{P})}$$

Оказывается, такое разложение V на изотипные компоненты определено однозначно.

Предложение 1. Кратности $(\mathcal{R}\colon \mathcal{P})$ и изотипные компоненты $V_{(\mathcal{P})}$ не зависят от разложения $\mathcal{R}$ на неприводимые слагаемые.

Доказательство.
Пусть $\mathcal{C} \in Hom\,(\mathcal{P}, \mathcal{R})$, тогда $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_m$, где $\mathcal{C}_i \in Hom\,(\mathcal{P}, \mathcal{R}_i)$. Так как $\mathcal{P}$ и $\mathcal{R}_i$ – неприводимые представления, то

- $Hom\,(\mathcal{P}, \mathcal{R}_i) = \{0\}$, если $\mathcal{R}_i \not\simeq \mathcal{P}$,
- $Hom\,(\mathcal{P}, \mathcal{R}_i) \simeq End\,(\mathcal{P})$, если $\mathcal{R}_i \simeq \mathcal{P}$.

Получаем $Hom\,(\mathcal{P}, \mathcal{R}) \simeq \underbrace{End\,(\mathcal{P}) \oplus \cdots \oplus End\,(\mathcal{P})}_{(\mathcal{R}:\mathcal{P})}$.

Аналогично, если $\mathcal{B} \in Hom\,(\mathcal{R}, \mathcal{P})$, то $\mathcal{B} = \mathcal{B}_1 \times \cdots \times \mathcal{B}_m$, где $\mathcal{B}_i \in Hom\,(\mathcal{R}_i, \mathcal{P})$ и

- $Hom\,(\mathcal{R}_i, \mathcal{P}) = \{0\}$, если $\mathcal{R}_i \not\simeq \mathcal{P}$,
- $Hom\,(\mathcal{R}_i, \mathcal{P}) \simeq End\,(\mathcal{P})$, если $\mathcal{R}_i \simeq \mathcal{P}$.

Тогда $Hom\,(\mathcal{R}, \mathcal{P}) \simeq \underbrace{End\,(\mathcal{P}) \oplus \cdots \oplus End\,(\mathcal{P})}_{(\mathcal{R}:\mathcal{P})}$.

Следовательно,

$$(\mathcal{R}\colon \mathcal{P}) = \frac{dim\,Hom\,(\mathcal{P}, \mathcal{R})}{dim\,End\,(\mathcal{P})} = \frac{dim\,Hom\,(\mathcal{R}, \mathcal{P})}{dim\,End\,(\mathcal{P})}$$

- не зависит от разложения.

В случае алгебраически замкнутого поля $(\mathcal{R}\colon \mathcal{P}) = dim\,Hom\,(\mathcal{P}, \mathcal{R}) = dim\,Hom\,(\mathcal{R}, \mathcal{P})$.

Теперь докажем, что изотипные компоненты $V_{(\mathcal{P})}$ не зависят от разложения $\mathcal{R}$ на неприводимые слагаемые. Заметим, что $Im\,\mathcal{C} \subseteq V_{(\mathcal{P})}$. Если $\mathcal{C} \neq 0$, то по лемме Шура $U \simeq Im\,\mathcal{C}$, следовательно,

$$V_{(\mathcal{P})} = \sum_{\substack{W \subseteq V \text{ инв.подпр.} \\ \mathcal{R}|_W \simeq \mathcal{P}}} W$$

- не зависит от разложения. ■

Замечание. Разложение $V = V_1 \oplus \cdots \oplus V_m$, где $\mathcal{R}|_{V_i} = \mathcal{R}_i$ неприводимы, вообще говоря, не единственно.

Пример. $S = \{1\}$ – тривиальная группа. $\mathcal{R}(1) = \mathcal{E}$, следовательно, любое подпространство $U \subseteq V$ инвариантно, поэтому существует единственное неприводимое представление $\mathcal{P}$, $\dim \mathcal{P} = 1$. Тогда разложение $\mathcal{R} = \underbrace{\mathcal{P} \oplus \cdots \oplus \mathcal{P}}_{n = \dim \mathcal{R}}$, единственно, но разложений $V = V_1 \oplus \cdots \oplus V_n$, где $\dim V_i = 1$, много.

Предложение 2. Пусть $\mathcal{P}\colon S \longrightarrow L(U)$ – неприводимое линейное представление, $\mathcal{R}\colon\ S \longrightarrow L(V)$ – вполне приводимое линейное представление. Существует канонический изоморфизм

$$V_{(\mathcal{P})} \simeq Hom\,(\mathcal{P}, \mathcal{R}) \underset{End\,(\mathcal{P})}{\otimes} U$$

Доказательство.
Структура левого $End\,(\mathcal{P})$-модуля на U задается следующим образом: $\mathcal{A}u = \mathcal{A}(u)$. Структура правого $End\,(\mathcal{P})$-модуля на $Hom\,(\mathcal{P}, \mathcal{R})$ задается следующим образом: $\mathcal{C}\mathcal{A}$ – композиция. Рассмотрим отображение

$$Hom\,(\mathcal{P}, \mathcal{R}) \times U \longrightarrow V$$
$$(\mathcal{C}, u) \mapsto \mathcal{C}(u)$$

Это отображение $End\,(\mathcal{P})$-билинейно, поэтому (по универсальному свойству тензорного произведения), существует линейное отображение

$$\Phi\colon\ Hom\,(\mathcal{P}, \mathcal{R}) \underset{End\,(\mathcal{P})}{\otimes} U \longrightarrow V$$
$$\mathcal{C} \otimes u \mapsto \mathcal{C}(u)$$

Покажем, что Φ изоморфно отображает $Hom\,(\mathcal{P}, \mathcal{R}) \underset{End\,(\mathcal{P})}{\otimes} U$ на $V_{(\mathcal{P})}$. Воспользуемся доказательством предложением 1: $Hom\,(\mathcal{R}, \mathcal{P}) \simeq \underbrace{End\,(\mathcal{P}) \oplus \cdots \oplus End\,(\mathcal{P})}_{(\mathcal{R}:\mathcal{P})}$, тогда

$$Hom\,(\mathcal{P}, \mathcal{R}) \underset{End\,(\mathcal{P})}{\otimes} U = \underbrace{End\,(\mathcal{P}) \oplus \cdots \oplus End\,(\mathcal{P})}_{k = (\mathcal{R}:\mathcal{P})} \underset{End\,(\mathcal{P})}{\otimes} U \simeq \underbrace{U \oplus \cdots \oplus U}_{k = (\mathcal{R}:\mathcal{P})}$$

$Im\,\Phi \subseteq V_{(\mathcal{P})}$, но $V_{(\mathcal{P})} = V_1 \oplus \cdots \oplus V_k$, $\mathcal{R}|_{V_i} \simeq \mathcal{P}$ $(i = 1, \dots, k)$, поэтому при отображении Φ $\underbrace{U \oplus \cdots \oplus U}_{k=(\mathcal{R}:\mathcal{P})}$ отображается в $V_1 \oplus \cdots \oplus V_k$. Поймем, что это за отображение. Имеем:

$$\mathcal{C} \otimes u \mapsto \mathcal{C}_1(u) + \cdots + \mathcal{C}_k(u)$$

также

$$0 \oplus \cdots \oplus \underset{i}{\underset{\smile}{U}} \oplus \cdots \oplus 0 \longrightarrow V_i \simeq U$$
$$\mathcal{E} \otimes u \mapsto u$$

Следовательно, Φ: $Hom\,(\mathcal{P}, \mathcal{R}) \underset{End\,(\mathcal{P})}{\otimes} U \longrightarrow V$ – изоморфизм. ■

Доказанные нами утверждения показывают, что неприводимые представления являются элементарными “кирпичиками”, из которых складываются любые вполне приводимые представления.

Далее от вещей, общих для любых линейных представлений, перейдем к изучению представлений конкретных математических структур. Нас будут интересовать в основном представления ассоциативных алгебр, а также групп и алгебр Ли. Пока же закончим лекцию применением результатов, которые мы получили, к теории групп.

Тензорное произведение представлений групп.

Пусть U, W – два векторных пространства над K, и $\mathcal{A} \in L(U)$, $\mathcal{B} \in L(W)$ – линейные операторы. Отображение

$$U \times W \longrightarrow U \underset{K}{\otimes} W$$
$$(u, w) \mapsto \mathcal{A}u \otimes \mathcal{B}w$$

билинейно, значит (по универсальному свойству тензорного произведения), существует единственное линейное отображение $\mathcal{C}$: $U \otimes W \longrightarrow U \underset{K}{\otimes} W$, делающее следующую диаграмму коммутативной (другими словами, $\mathcal{C}(u \otimes w) = \mathcal{A}u \otimes \mathcal{B}w$):

$$\begin{tikzcd}
U \times W \arrow[r] \arrow[d] & U \underset{K}{\otimes} W \\
U \otimes W \arrow[ur, dashed, "\exists!\ \text{линейный оператор } \mathcal{C} = \mathcal{A} \otimes \mathcal{B}"'] &
\end{tikzcd}$$

Определение. Пусть

$$\mathcal{P}\colon\ G \longrightarrow GL(U)$$
$$\mathcal{Q}\colon\ H \longrightarrow GL(W)$$

- линейные представления групп. Их *тензорное произведение* $\mathcal{R} = \mathcal{P} \otimes \mathcal{Q}$:

$$G \times H \longrightarrow GL(U \otimes W)$$
$$\mathcal{R}(g,h) = \mathcal{P}(g) \otimes \mathcal{Q}(h)$$

Предложение 3. Пусть $\mathcal{P}, \mathcal{Q}$ – неприводимые конечномерные представления групп G, H над алгебраически замкнутым полем K. Тогда $\mathcal{R} = \mathcal{P} \otimes \mathcal{Q}$ будет неприводимо, и любое неприводимое конечномерное представление группы $G \times H$ устроено таким образом.

Доказательство.
1) $U \otimes W = u_1 \otimes W \oplus \cdots \oplus u_n \otimes W \simeq \underbrace{W \oplus \cdots \oplus W}_{n}$, где $u_1, \dots, u_n$ – базис U. Этот изоморфизм с точки зрения теории представлений дает разложение $\mathcal{R}|_H$ в прямую сумму:

$$\mathcal{R}|_H \simeq \underbrace{\mathcal{Q} \oplus \cdots \oplus \mathcal{Q}}_{n}$$

Отсюда следует, что $\mathcal{R}|_H$ вполне приводимо и изотипно. Следовательно, все неприводимые подпредставления в $\mathcal{R}|_H$ изоморфны $\mathcal{Q}$ $\Longrightarrow$ любое минимальное ненулевое инвариантное подпространство относительно $\mathcal{R}|_H$ имеет вид $Im\,\mathcal{C}$, где $\mathcal{C} \in Hom\,(\mathcal{Q}, \mathcal{R}|_H)$.

Но $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_n$, где $\mathcal{C}_i \in End\,(\mathcal{Q})$, и $\mathcal{C}(w) = \mathcal{C}_1(w) + \cdots + \mathcal{C}_n(w)$, $\mathcal{C}_i(w) \in u_i \otimes W$, т.е. $\mathcal{C}_i(w) = u_i \otimes \lambda_i w$ $(\lambda_i \in K)$ – так как эндоморфизмы неприводимого представления скалярны (мы отождествили $u_i \otimes W$ с W). Получаем

$$\mathcal{C}(w) = \sum_i u_i \otimes \lambda_i w = \left(\sum_i \lambda_i u_i\right) \otimes w$$

Следовательно, $Im\,\mathcal{C} = u \otimes W$, где $u = \sum_i \lambda_i u_i$. Итак, любое минимальное ненулевое инвариантное подпространство относительно $\mathcal{R}|_H$ имеет вид $u \otimes W$, где $u = \sum_i \lambda_i u_i$. Тогда любое инвариантное подпространство относительно $\mathcal{R}|_H$ в $U \otimes W$ имеет вид $U' \otimes W$, где $U' \subseteq U$.

Если $U' \otimes W$ инвариантно относительно $\mathcal{R}$, то $U' \subseteq U$ – инвариантно относительно $\mathcal{P}$, поэтому $U' = \{0\}$ или U. Тогда $U' \otimes W = \{0\}$ или $U \otimes W$, следовательно, $\mathcal{R}$ неприводимо.

2) Обратно, пусть $\mathcal{R}$: $G \times H \longrightarrow GL(V)$ неприводимо. $\forall g \in G,\ h \in H$ выполнено: $\mathcal{R}(g)\mathcal{R}(h) = \mathcal{R}(h)\mathcal{R}(g)$, откуда следует, что $\mathcal{R}(g) \in End\,(\mathcal{R}|_H)$.

Выберем в V минимальное ненулевое инвариантное подпространство $W \subseteq V$ относительно $\mathcal{R}|_H$, тогда $\mathcal{Q} = \mathcal{R}|_{H,W}$ неприводимо. Рассмотрим

$$V \supseteq \sum_{g \in G} \mathcal{R}(g)W$$

- инвариантно относительно $\mathcal{R} \Longrightarrow$

$$V = \sum_{g \in G} \mathcal{R}(g)W$$

Эта сумма, вообще говоря, не прямая, но ее можно записать в виде прямой суммы нескольких слагаемых:

$$V = \mathcal{R}(g_1)W \oplus \cdots \oplus \mathcal{R}(g_m)W$$

Отсюда, в частности, следует, что $\mathcal{R}|_H \simeq \underbrace{\mathcal{Q} \oplus \cdots \oplus \mathcal{Q}}_{n}$ изотипно. Тогда (по предложению 2):

$$V \simeq \underbrace{Hom\,(\mathcal{Q}, \mathcal{R}|_H)}_{U} \otimes W$$

$$u(w) \leftarrow\!\shortmid u \otimes w$$

Определим $\mathcal{P}$: $G \longrightarrow GL(U)$:

$$(\mathcal{P}(g)u)(w) = \mathcal{R}(g)(u(w))$$

$\Longrightarrow$

$$\mathcal{R} = \mathcal{P} \otimes \mathcal{Q}$$

Осталось показать, что $\mathcal{P}$ неприводимо. В самом деле: если $U' \subseteq U$ – инвариантное подпространство относительно $\mathcal{P}$, тогда $U' \otimes W$– инвариантное подпространство относительно $\mathcal{R}$, т.е. $U' \otimes W = \{0\}$ или V. Следовательно, $U' = \{0\}$ или V, а значит, $\mathcal{P}$ неприводимо. ■

Лекция 12. Конечномерные ассоциативные алгебры и их представления.

Перейдем к изучению конечномерных ассоциативных алгебр, их структуры и линейных представлений. Пусть A – ассоциативная алгебра над полем K. Если задано линейное представление $\mathcal{R}$: $A \longrightarrow L(V)$, тогда на V возникает естественная структура левого A-модуля (из того, что $\mathcal{R}$ – гомоморфизм, вытекает выполнение аксиом модуля): $\forall a \in A, \forall v \in V$:

$$av = \mathcal{R}(a)v$$

Верно и обратное. Таким образом:

- линейные представления алгебры $A \Leftrightarrow$ левые A-модули

Соответственно, понятия, которые мы вводили для теории представлений, переносятся на язык модулей, и наоборот:

- подпредставления $\Leftrightarrow$ подмодули
- факторпредставления $\Leftrightarrow$ фактормодули
- прямая сумма линейных представлений $\Leftrightarrow$ прямая сумма модулей
- гомоморфизмы линейных представлений $\Leftrightarrow$ гомоморфизмы модулей
- неприводимое представление $\Leftrightarrow$ *простой* модуль (т.е. ненулевой модуль без ненулевых собственных подмодулей)
- вполне приводимое представление $\Leftrightarrow$ *полупростой* модуль (т.е. у любого подмодуля существует дополнительный подмодуль)

Если $\dim A < \infty$, то любой элемент $v \in V$ содержится в конечномерном подмодуле $Kv + Av$, т.е. для конечномерных алгебр пространство представлений есть объединение пространств конечномерных представлений. В частности, все неприводимые представления конечномерны. Далее будем рассматривать конечномерные ассоциативные алгебры и их конечномерные линейные представления / модули.

Нильпотентные алгебры.

Определение 1. Алгебра A нильпотентна, если все ее элементы нильпотентны: $\forall a \in A$ $\exists n \in \mathbb{N}$: $a^n = 0$.

Пример. Алгебра всех верхних нильтреугольных матриц нильпотентна. Оказывается, этот пример является универсальным.

Задача 1. Доказать, что любая конечномерная нильпотентная алгебра вкладывается в качестве подалгебры в алгебру верхних нильтреугольных матриц.

Лемма 1. Алгебра A нильпотентна $\Longrightarrow \exists n \in \mathbb{N}$: $\forall a_1, \dots, a_n \in A$ выполнено $a_1 \cdots a_n = 0$.

Обозначения: A – алгебра, M – левый A-модуль. Если $B_1, \dots, B_m \subseteq A$ – подпространства, $N \subseteq M$ – подпространство, то $B_1 \cdots B_m N = < b_1 \cdots b_m n \mid b_i \in B_i, n \in N >_K \subseteq M$.

Доказательство.
Без ограничения общности можно считать, что $A \neq \{0\}$. Тогда существуют подпространства $B \subseteq A$, $B \neq \{0\}$, такие что $B^n = \underbrace{B \cdots B}_{n} = \{0\}$ для некоторого $n \in \mathbb{N}$ (например, $B = Ka$, $a \in A$, $a \neq 0$). Пусть B – максимальное (по включению) подпространство с этим свойством. Докажем, что $B = A$ от противного.

1) Пусть $a \in A$, $a \notin B$. Рассмотрим подпространства Ka, aB, aB^2, $aB^3, \dots, aB^n = \{0\}$ $\Longrightarrow \exists k \geq 0$: $aB^k \nsubseteq B$, $aB^{k+1} \subseteq B$ (считаем, что $aB^0 = Ka$). Возьмем $c \in aB^k$, но $c \notin B$ $\Longrightarrow cB \subseteq B$. $\exists m \in \mathbb{N}$: $c^m = 0$. Положим $C = B \oplus Kc$.

2) Покажем, что $C^{mn} = \{0\}$. Пусть $c_1, \dots, c_{mn} \in C$ – покажем, что $c_1 \cdots c_{mn} = 0$. Без ограничения общности можно считать, что либо $c_i \in B$, либо $c_i = c$ (следует из того, что $C = B \oplus Kc$ – представим c_i в виде суммы слагаемых из B и Kc, и раскроем скобки в произведении $c_1 \cdots c_{mn}$).

Возможны два случая:

- среди c_i встречается подряд m элементов c, и тогда $c_1 \cdots c_{mn} = 0$,
- $c_1 \cdots c_{mn} = c^{k_1} b_1 c^{k_2} b_2 \cdots c^{k_s} b_s c^{k_{s+1}}$, где $0 \leq k_i < m$, $b_i \in B$. Тогда в каждой группе вида $c^{k_i} b_i$ не более m множителей, откуда следует, что $s \geq n$. Так как $cB \subseteq B$, то $c^{k_i} b_i \in B$, т.е. $c^{k_1} b_1 c^{k_2} b_2 \cdots c^{k_s} b_s c^{k_{s+1}} \in B^s c^{k_{s+1}}$. Но $B^s = \{0\}$ (так как $s \geq n$), поэтому $c_1 \cdots c_{mn} = c^{k_1} b_1 c^{k_2} b_2 \cdots c^{k_s} b_s c^{k_{s+1}} = 0$.

3) $C \supset B$ – противоречие с максимальностью B. Следовательно, $B = A \Longrightarrow A^n = \{0\}$. ■

Задача 2. Доказать, что у нильпотентной алгебры существует единственное неприводимое представление; оно одномерно.

Задача 3. Пусть $\mathcal{R}$: $A \longrightarrow L(V)$ – линейное представление нильпотентной алгебры. Доказать, что при некотором выборе базиса в V соответствующее матричное представление $R(A)$ будет задаваться нильтреугольными матрицами.

Лемма 2. Пусть A – конечномерная ассоциативная алгебра, $I, J \lhd A$ – нильпотентные идеалы. Тогда $I + J \lhd A$ – нильпотентный идеал.

Доказательство.

Рассмотрим алгебру $(I+J)/I$. Имеем: $(I+J)/I \simeq J/(I \cap J)$, но $J/(I \cap J)$ нильпотентна (так как J нильпотентный идеал), поэтому $\forall a \in I+J \ \exists n \in \mathbb{N}$: $a^n \in I$. Но I также нильпотентен, т.е. $\exists m \in \mathbb{N}$: $(a^n)^m = a^{nm} = 0$, следовательно, $I+J \lhd A$ – нильпотентный идеал. ■

Радикал.

Определение 2. Пусть A – конечномерная ассоциативная алгебра. *Радикал* $Rad(A)$ – наибольший нильпотентный двусторонний идеал в A.

Замечание. Существование радикала вытекает из леммы 2: пусть $J \lhd A$ – максимальный нильпотентный идеал. Если J не наибольший, то существует нильпотентный идеал $I \lhd A$, $I \nsubseteq J$, тогда $I+J$ – нильпотентный идеал и $I+J \supset J$, что противоречит максимальности J.

Пример. Пусть A – алгебра верхнетреугольных матриц. $Rad(A)$ – это алгебра всех верхних нильтреугольных матриц.

Стандартное скалярное умножение.

Если мы рассматриваем алгебру A над полем нулевой характеристики, можно охарактеризовать радикал с помощью скалярного умножения. Рассмотрим левое регулярное представление

$$\mathcal{L}\colon A \longrightarrow L(A)$$
$$\mathcal{L}(a)\colon x \mapsto ax$$

Определение 3. *Стандартное скалярное умножение* на A: $(a \mid b) = tr(\mathcal{L}(a)\mathcal{L}(b))$ - симметрическая билинейная функция $A \times A \longrightarrow K$.

Основное свойство скалярного умножения (A-билинейность): $(ab \mid c) = (a \mid bc)$, $\forall a, b, c \in A$.

Доказательство.

$$\mathcal{L}(ab)\mathcal{L}(c) = \mathcal{L}(a)\mathcal{L}(b)\mathcal{L}(c) = \mathcal{L}(a)\mathcal{L}(bc)$$

Остается взять tr. ■

Лемма 3. Пусть $I \lhd A$. Тогда:
а) $I^{\perp} \lhd A$ (ортогональное дополнение в смысле стандартного скалярного умножения),
б) $(\cdot \mid \cdot)|_I$ – стандартное скалярное умножение на I.

Доказательство.

а) $\forall b \in I^{\perp}, a \in A, c \in I$:

$$(ba \mid c) = (b \mid ac) = 0 \text{ (т.к. } b \in I^{\perp}, ac \in I) \Longrightarrow ba \in I^{\perp}$$
$$(c \mid ab) = (ca \mid b) = 0 \text{ (т.к. } b \in I^{\perp}, ac \in I) \Longrightarrow ab \in I^{\perp}$$

Следовательно, $I^{\perp} \lhd A$.

б) В базисе A, согласованном с I:
$\forall a \in L(I)$:

$$L(a) = \left(\begin{array}{c|c} L_I(a) & * \\ \hline 0 & 0 \end{array}\right)$$

где L_I – матричное представление, соответствующее $\mathcal{L}|_I$. Имеем: $(a \mid b) = tr\big(\mathcal{L}(a)\mathcal{L}(b)\big) = tr\mathcal{L}(ab)$, поэтому если $a, b \in I$, то

$$(a \mid b) = tr\mathcal{L}(ab) = tr\mathcal{L}(ab)|_I = tr\mathcal{L}(a)|_I \cdot tr\mathcal{L}(b)|_I$$

- стандартное скалярное умножение на I. ■

Теорема. Если $char\, K = 0$, то $Rad(A) = A^{\perp}$ - ядро стандартного скалярного умножения.

Доказательство.
1) Докажем, что $Rad(A) \subseteq A^{\perp}$: $\forall a \in A, b \in Rad(A)$: $ab \in Rad(A) \Longrightarrow \exists n \in \mathbb{N}$: $(ab)^n = 0$, тогда и $\mathcal{L}(ab)^n = 0$, т.е. $\mathcal{L}(ab)$ – нильпотентный линейный оператор, следовательно, $tr\mathcal{L}(ab) = 0$, поэтому $tr\mathcal{L}(ab) = tr\big(\mathcal{L}(a)\mathcal{L}(b)\big) = (a \mid b) = 0$.

2) Докажем, что $Rad(A) \supseteq A^{\perp}$: по п.а) леммы 3, $A^{\perp} \lhd A$; $\forall a \in A^{\perp}$ и $\forall k, l \in \mathbb{N}$ имеем:

$$(a^k \mid a^l) = tr\Big(\mathcal{L}(a^k)\mathcal{L}(a^l)\Big) = tr\mathcal{L}(a)^{k+l} = 0,$$

т.е. $\forall m \geq 2$: $tr\mathcal{L}(a)^m = 0$.

Лемма 4. Пусть $\mathcal{B} \in L(V)$, такой что $tr(\mathcal{B}^m) = 0$, $\forall m \geq m_0$. Тогда $\mathcal{B}$ нильпотентен.

Доказательство леммы 4.
Пусть $\lambda_1, \dots, \lambda_s$ – все различные ненулевые корни $\chi_{\mathcal{B}}$ в его поле разложения, $k_1, \dots, k_s$ – их кратности. Тогда

$$tr(\mathcal{B}^m) = k_1\lambda_1^m + k_2\lambda_2^m + \dots + k_s\lambda_s^m = 0$$

при $m = m_0, m_0 + 1, \dots, m_0 + s - 1$. Посмотрим на это равенство как на однородную систему линейных уравнений на $k_1, \dots, k_s$. Матрица системы:

$$M = \begin{pmatrix} \lambda_1^{m_0} & \lambda_2^{m_0} & \cdots & \lambda_s^{m_0} \\ \lambda_1^{m_0+1} & \lambda_2^{m_0+1} & \cdots & \lambda_s^{m_0+1} \\ \vdots & \vdots & \cdots & \vdots \\ \lambda_1^{m_0+s-1} & \lambda_2^{m_0+s-1} & \cdots & \lambda_s^{m_0+s-1} \end{pmatrix}$$

Если мы вынесем общие множители из каждого столбца, то определитель этой матрицы превратится в определитель Вандермонда, поэтому

$$\det M = \lambda_1^{m_0} \cdots \lambda_s^{m_0} \prod_{i>j} (\lambda_i - \lambda_j) \neq 0,$$

откуда следует, что $k_1 = \cdots = k_s = 0$ (здесь используется условие $char\, K = 0$). Противоречие показывает, что все корни $\chi_{\mathcal{B}}$ равны нулю $\Longrightarrow$ оператор $\mathcal{B}$ нильпотентен. ■

По лемме 4 $\mathcal{L}(a)$ нильпотентен $\Longrightarrow$ $\exists n \in \mathbb{N}$: $\mathcal{L}(a)^n = 0$, тогда $\mathcal{L}(a)^n a = a^{n+1} = 0$. Следовательно, $A^{\perp}$ - нильпотентный идеал. Теорема доказана. ■

Замечание. Условие $char\, K = 0$ использовалось только во второй части доказательства. В частности, в любой характеристике верно:

- A нильпотентна $\Longrightarrow (\cdot \mid \cdot) = 0$
- $(\cdot \mid \cdot)$ невырождено $\Longrightarrow Rad(A) = \{0\}$

Алгебры с нулевым радикалом называются полупростыми, их изучению мы посвятим следующую лекцию.

Лекция 13. Структура полупростых алгебр. Теорема Бернсайда.

Продолжим изучение конечномерных ассоциативных алгебр. На прошлой лекции мы ввели понятие радикала $Rad(A)$ конечномерной ассоциативной алгебры. Нам понадобится характеризация радикалов в терминах теории представлений. Докажем следующее предложение.

Предложение 1. $Rad(A)$ = пересечение ядер всех неприводимых линейных представлений алгебры A.

Доказательство.
Пусть I = пересечение ядер всех неприводимых линейных представлений алгебры A, $J = Rad(A)$.

1) Докажем, что $J \subseteq I$. Пусть M – простой A-модуль, тогда $JM \subseteq M$ – подмодуль и возможны два варианта:

- $JM = M \Longrightarrow J^n M = M, \forall n \in \mathbb{N}$. Но $\exists n$: $J^n = \{0\}$ – противоречие
- $JM = \{0\}$. Следовательно, $J \subseteq I$

2) Докажем, что $I \subseteq J$. Рассмотрим цепочку вложенных идеалов: $I \supseteq I^2 \supseteq \cdots \supseteq I^n \supseteq \cdots$ Если $I^n \neq \{0\}$, то выберем максимальный левый идеал $N \subset I^n$, тогда $M = I^n/N$ – простой A-модуль, откуда следует, что $IM = \{0\} \Longrightarrow I^{n+1} \subseteq N \subset I^n$.

Таким образом, последовательность $\{I^n\}_{n\in\mathbb{N}}$ не может бесконечно убывать по соображениям размерности $\Longrightarrow \exists n$: $I^n = \{0\}$. Следовательно, $I \subseteq J$. ■

Теперь перейдем к изучению важного класса конечномерных ассоциативных алгебр, на которых нет ненулевых нильпотентных идеалов (т.е. радикал которых равен нулю). Такие алгебры называются полупростыми.

Полупростые алгебры.

Определение. Ненулевая конечномерная ассоциативная алгебра A *полупроста*, если $Rad(A) = \{0\}$.

Пример 1. Простая алгебра A с ненулевым умножением полупроста: иначе бы $Rad(A) = A$ была бы нильпотентна $\Longrightarrow A^n = \{0\} \Longrightarrow A^2 \subset A$, $A^2 \lhd A \Longrightarrow A^2 = \{0\}$.

Пример 2. $A = Mat_n(K)$ или, более общо, $A = Mat_n(D)$, где D – конечномерная алгебра с делением над K. Такая алгебра проста, с ненулевым умножением.

Простота: пусть $I \lhd Mat_n(D)$, $I \neq \{0\}$. Рассмотрим $a \in I$, $a = (a_{ij})_{i,j=1}^n$, $\exists i,j$: $a_{ij} \neq 0$. Умножим матрицу a слева и справа на подходящие матричные единицы: $\forall k,l \in \{1,\dots,n\}$ $e_{ki} \cdot a \cdot e_{jl} = a_{ij} \cdot e_{kl} \in I$.

Так как $a_{ij} \neq 0$, то $\exists a_{ij}^{-1}$, тогда $\forall \delta \in D$: $a_{ij} \cdot e_{kl} \cdot \delta a_{ij}^{-1} \cdot e_{ll} = \delta e_{kl} \in I$, откуда следует, что $I = Mat_n(D)$.

Замечание. В случае $char\, K = 0$ алгебра A полупроста $\Leftrightarrow$ стандартное скалярное умножение на A невырождено.

Структура полупростых алгебр.

Лемма 1. Полупростая алгебра A имеет точное вполне приводимое конечномерное линейное представление.

Доказательство.
Так как A полупроста, то (по предложению 1):

$$\bigcap_{\substack{\mathcal{R}:\ A \longrightarrow L(V) \\ \text{неприводимо}}} Ker\, \mathcal{R} = Ker\, \mathcal{R}_1 \cap \dots \cap Ker\, \mathcal{R}_m = \{0\},$$

где $\mathcal{R}_i$: $A \longrightarrow L(V_i)$ неприводимо.

С другой стороны, представление $\mathcal{R} = \mathcal{R}_1 \oplus \dots \oplus \mathcal{R}_m$: $A \longrightarrow L(V_1 \oplus \dots \oplus V_m)$ вполне приводимо (так как является прямой суммой неприводимых представлений), $Ker\, \mathcal{R} = \{0\}$. ■

Лемма 2. Левое регулярное представление полупростой алгебры A вполне приводимо.

Доказательство.
Рассмотрим точное вполне приводимое представление $\mathcal{R}$: $A \longrightarrow L(V)$. Во-первых, это вложение: $\mathcal{R}$: $A \hookrightarrow L(V)$, а во-вторых, это изоморфизм левых A-модулей:

$$L(V) \simeq \underbrace{V \oplus \dots \oplus V}_{\dim V = n \text{ слагаемых}}$$
$$\mathcal{A} \longleftrightarrow (\mathcal{A}e_1, \dots, \mathcal{A}e_n)$$

где $(e_1, \dots, e_n)$ – фиксированный базис V. Но $V \oplus \dots \oplus V$ – полупростой A-модуль, следовательно, левый регулярный A-модуль A тоже полупрост, что означает, что левое регулярное представление полупростой алгебры A вполне приводимо. ■

Чуть позже мы докажем, что любое линейное представление полупростой алгебры будет вполне приводимо. Более того, это свойство характеризует полупростые алгебры.

Предложение 2. Если A – полупростая алгебра, то $A = A_1 \oplus \dots \oplus A_s$, где A_i – простые алгебры с ненулевым умножением.

Доказательство.
Рассмотрим изотипное разложение левого регулярного A-модуля: $A = A_1 \oplus \dots \oplus A_s$ (A_i = сумма всех ненулевых минимальных левых идеалов (= простых подмодулей) в A, изоморфных друг другу (какA-модули)). Докажем, что A_i являются двусторонними идеалами.

$\forall a \in A$ рассмотрим отображение $\varphi\colon A \longrightarrow A$, $\varphi(x) = xa$ – эндоморфизм левого регулярного A-модуля $\Longrightarrow$ для любого минимального левого идеала $J \subseteq A$ выполнено: $\varphi(J) \simeq J$ или $\varphi(J) = \{0\}$ (по лемме Шура), откуда следует, что $\varphi(A_i) \subseteq A_i \Longrightarrow A_i \lhd A$.

Простота: пусть $I \lhd A_i$, тогда $I \lhd A$. Из полной приводимости вытекает, что $A_i = I \oplus J$, где J – дополнительный левый идеал. Рассмотрим IJ: так как $I \lhd A$, то $IJ \subseteq I$, а так как J левый идеал, то $IJ \subseteq J$, следовательно, $IJ \subseteq I \cap J = \{0\}$. Тогда для любого минимального левого идеала $N \subseteq J$ выполнено: $IN = \{0\}$.

Из изотипности вытекает, что:

- либо $IA_i = \{0\}$, тогда $I^2 = \{0\} \Longrightarrow I = \{0\}$ (следует из полупростоты A)
- либо $J = \{0\}$, тогда $A_i = I$

Итак, мы доказали, что любой идеал в A_i или нулевой, или совпадает с A_i, следовательно, алгебра A_i проста.

Ненулевое умножение: рассмотрим идеал $A_i^2 \lhd A_i$. Так как A_i проста, то либо $A_i^2 = A_i \neq \{0\}$ и умножение ненулевое, либо $A_i^2 = \{0\}$, $A_i \lhd A$, тогда $A_i \neq \{0\}$ – нильпотентый идеал, что противоречит полупростоте A. ■

Прежде чем перейти к изучению устройства простых конечномерных ассоциативных алгебр, сделаем небольшое отступление. Пусть A – произвольная конечномерная ассоциативная алгебра, $\mathcal{R}\colon A \longrightarrow L(V)$ – ее неприводимое конечномерное линейное представление. Из леммы Шура следует, что $End\ \mathcal{R}$ – алгебра с делением.

Рассмотрим противоположную алгебру $D = (End\ \mathcal{R})^{op}$ – это тоже конечномерная алгебра с делением. $\forall v \in V, \forall \delta \in D$ определим умножение как $v\delta = \delta(v)$. Проверим, что V – (A, D)-бимодуль: $\forall a \in A,\ v \in V,\ \delta, \delta' \in D$:

- $(v\delta)\delta' = \delta'(\delta(v)) = (\delta\delta')(v) = v(\delta\delta')$
- $(av)\delta = \delta(av) = a\delta(v) = a(v\delta)$

В частности, V является правым векторным пространством над D, и $\mathcal{R}$: $A \longrightarrow L_D(V) \subseteq L(V)$, где $L_D(V)$ – алгебра D-линейных операторов. Таким образом, можно рассматривать неприводимые представления произвольной конечномерной ассоциативной алгебры как гомоморфизмы в алгебру линейных операторов на векторном пространстве над соответствующим телом.

Линейная алгебра над телами – такая же, как над полями (в основах). В частности: выбор базиса $(e_1, \dots, e_n)$ в V над D позволяет отождествить V с пространством столбцов D^n: $V \simeq D^n$, а всякий линейный оператор на V над D задается матрицей размера $n \times n$ над D, т.е. $L_D(V) \simeq Mat_n(D)$.

Ключевым результатом, который нам понадобится для описания структуры простых (а значит, и полупростых) алгебр, является теорема Бернсайда.

Теорема Бернсайда. Пусть $\mathcal{R}$: $A \longrightarrow L(V)$ – ненулевое неприводимое представление конечномерной ассоциативной алгебры. Тогда $\mathcal{R}(A) = L_D(V)$, где $D = (End\ \mathcal{R})^{op}$.

Доказательство.
Достаточно доказать, что $\forall e_1, \dots, e_m \in V$ линейно независимых над D и $\forall v_1, \dots, v_m \in V$ $\exists a \in A$, такой что $\forall i = 1, \dots, m$: $ae_i = v_i$ (так как любой линейный оператор задается своим действием на базисные векторы). Другими словами, достаточно доказать, что $V^{\oplus m} = A \cdot (e_1, \dots, e_m)$. Докажем индукцией по m.

<u>База индукции</u>: $m = 1$. Тогда $Ae_1 \subseteq V$ – A-подмодуль, ненулевой (иначе $Ke_1 \subseteq V$ – подмодуль, тогда $Ke_1 = V$ и $\mathcal{R} = 0$ – противоречие). Следовательно, $Ae_1 = V$.

<u>Шаг индукции</u>: $V^{\oplus m} = V^{\oplus(m-1)} \oplus V_m$ (понятно, что $V_m = V$). Рассмотрим $W = A \cdot (e_1, \dots, e_m) \subseteq V^{\oplus m}$ и две проекции: π: $W \longrightarrow V^{\oplus m}$ и τ: $W \longrightarrow V_m$. Имеем:

- $Im\ \pi = A \cdot (e_1, \dots, e_m) = V^{\oplus(m-1)}$ (по предположению индукции)
- $Ker\ \pi = W \cap V_m$ – подмодуль в V. Так как V – простой A-модуль, то $W \cap V_m = \{0\}$, либо $W \cap V_m = V$.

Если $W \cap V_m = \{0\}$, то π – изоморфизм, и $\varphi = \tau\pi^{-1}$ – гомоморфизм из $V^{\oplus m}$ в V, откуда следует, что $\varphi = \tau\pi^{-1} = \varphi_1 \oplus \cdots \oplus \varphi_{m-1}$, где φ_i: $V \nrightarrow V \Longrightarrow \varphi_i(v) = v\delta_i$ для некотрого фиксированного $\delta_i \in D$:

$$\begin{tikzcd} W \arrow[r, "\pi", "\sim"'] \arrow[d, "\tau"'] & V^{\oplus(m-1)} \arrow[dl, "\varphi = \tau\pi^{-1} = \varphi_1 \oplus \cdots \oplus \varphi_{m-1}"] \\ V & \end{tikzcd}$$

Заметим, что $W \ni (e_1, \dots, e_m)$: иначе бы $\widetilde{W} = W \oplus K(e_1, \dots, e_m) \subseteq V^{\oplus m}$ – полупростой подмодуль, т.е. $\widetilde{W} = W \oplus U$, где U – одномерный A-подмодуль. Отсюда следует, что $U \simeq V$ и $\mathcal{R} = 0$ – противоречие.

Следовательно, $e_m = \tau(e_1, \dots, e_m)$, также $e_m = \varphi(e_1, \dots, e_{m-1}) = e_1\delta_1 + \cdots + e_{m-1}\delta_{m-1}$, т.е. e_m является линейной комбинацией $e_1, \dots, e_{m-1}$ – противоречие с линейной независимостью.

Итак, вариант $W \cap V_m = \{0\}$ невозможен, следовательно, $W \cap V_m = V$. Тогда $W \supseteq V_m$ и $\pi(W) = V^{\oplus(m-1)}$, откуда следует, что $W = V^{\oplus m}$. ■

Лекция 14. Структура простых и полупростых алгебр.

На прошлой лекции мы получили два ключевых результата, которые помогут нам разобраться с устройством простых и полупростых алгебр:

- (Предложение 2): если A – полупростая алгебра, то $A = A_1 \oplus \cdots \oplus A_s$, где A_i – простые алгебры с ненулевым умножением
- (Теорема Бернсайда): пусть $\mathcal{R}\colon A \longrightarrow L(V)$ – ненулевое неприводимое представление конечномерной ассоциативной алгебры. Тогда $\mathcal{R}(A) = L_D(V)$, где $D = (End\ \mathcal{R})^{op}$ – конечномерная алгебра с делением.

Структуру простых алгебр описывает следующая теорема:

Теорема Веддербёрна. Всякая простая конечномерная ассоциативная алгебра A над полем K с ненулевым умножением изоморфна $Mat_n(D)$, где D – конечномерная алгебра с делением над K.

Доказательство.
Рассмотрим произвольное ненулевое неприводимое представление $\mathcal{R}\colon A \longrightarrow L(V)$. Например: $N \subset A$ – максимальный собственный левый идеал, $V = A/N$ – имеем: $A \cdot A = A^2 \Longrightarrow A \cdot V = V \Longrightarrow \mathcal{R} \neq 0$.

A проста $\Longrightarrow$ $Ker\ \mathcal{R} = \{0\} \Longrightarrow A \simeq \mathcal{R}(A)$. Воспользуемся теоремой Бернсайда: $A \simeq \mathcal{R}(A) = L_D(V)$, где $D = (End\ \mathcal{R})^{op}$. Но $L_D(V)$ путем выбора базиса отождествляется с алгеброй квадратных матриц над D: $L_D(V) \simeq Mat_n(D)$, поэтому $A \simeq Mat_n(D)$. ■

Структуру полупростых алгебр описывает следующая теорема:

Теорема Веддербёрна - Артина. Ассоциативная алгебра A над полем K полупроста $\Leftrightarrow$ $A \simeq Mat_{n_1}(D_1) \oplus \cdots \oplus Mat_{n_s}(D_s)$, где D_j – конечномерные алгебры с делением над K. В частности, все полупростые алгебры содержат единицу.

Доказательство.
$\Longrightarrow$: следует из сформулированных в начале лекции предложения 2 и теоремы Веддербёрна.

$\Longleftarrow$: обозначим $A_j = Mat_{n_j}(D_j)$ $(j = 1, \dots, s)$. Докажем, что $A = A_1 \oplus \cdots \oplus A_s$ является полупростой алгеброй, т.е. в ней нет нильпотентных идеалов. Пусть $I \lhd A$, $I \neq \{0\}$. Обозначим I_j проекцию I на A_j – несложно видеть, что $I_j \lhd A_j$. Так как A_j – простая алгебра, то либо $I_j = A_j$, либо $I_j = \{0\}$.

С одной стороны, $I \subseteq I_1 \oplus \cdots \oplus I_s$. С другой стороны, $I \supseteq IA_j = I_jA_j = I_j$. Следовательно, $I = I_1 \oplus \cdots \oplus I_s$, а так как $I_j = A_j$, либо $I_j = \{0\}$, то $I = A_{j_1} \oplus \cdots \oplus A_{j_k}$ $(1 \leq j_1 \leq \cdots \leq j_k \leq s)$, откуда следует, что I не нильпотентен и $Rad(A) = \{0\}$. ■

Полупростые алгебры интересны с точки зрения теории представлений алгебр – их можно охарактеризовать в терминах теории представлений.

Предложение 1. Конечномерная ассоциативная алгебра A полупроста $\Leftrightarrow$ все ее конечномерные линейные представления вполне приводимы. В обозначениях теоремы Веддербёрна – Артина, все простые A-модули (кроме одномерного модуля с нулевым действием A) имеют вид $D_j^{n_j}$ $(j = 1, \dots, s)$, где $Mat_{n_j}(D_j)$ действует умножениями слева, а остальные $Mat_{n_i}(D_i)$ действуют нулевым образом.

Доказательство.
$\Longrightarrow$:
Из теоремы Веддербёрна – Артина следует, что $A \simeq Mat_{n_1}(D_1) \oplus \cdots \oplus Mat_{n_s}(D_s)$, при этом $Mat_{n_j}(D_j)$ может быть разложена в прямую сумму n_j своих левых идеалов, состоящих из матриц, у которых все столбцы, кроме k-го, нулевые $(k = 1, \dots, n_j)$, откуда следует, что

$$Mat_{n_j}(D_j) \simeq \underbrace{D_j^{n_j} \oplus \cdots \oplus D_j^{n_j}}_{n_j}$$

Проделав такое разложение для каждого слагаемого из $Mat_{n_1}(D_1) \oplus \cdots \oplus Mat_{n_s}(D_s)$, получим, что

$$A = J_1 \oplus \cdots \oplus J_{n_1+\cdots+n_s},$$

где каждый $J_k \simeq D_j^{n_j}$ для некоторого j. Заметим, что $\forall k$: J_k – простой A-модуль, поскольку $\forall v, w \in D_j^{n_j}, v \neq 0, \ \exists a \in Mat_{n_j}(D_j)$: $av = w$.

Пусть $\mathcal{R}$: $A \longrightarrow L(V)$ – произвольное линейное представление, тогда $1 \mapsto \mathcal{R}(1) = \mathcal{R}(1)^2$. Как известно из линейной алгебры, если оператор равен своему квадрату, то это оператор проектирования, поэтому $V = V_0 \oplus V_1$, где $V_0 = Ker\, \mathcal{R}(1)$, $V_1 = Im\, \mathcal{R}(1)$. При этом V_0 и V_1 – подмодули, так как $\mathcal{R}(1) \in End\, \mathcal{R}$. Имеем:

- $A \cdot V_0 = A \cdot 1 \cdot V_0 = \{0\} \Longrightarrow V_0$ полупрост
- $A \cdot V_1 = V_1$. Докажем, что V_1 полупрост:

Пусть $(e_1, \dots, e_n)$ – базис V_1, тогда

$$A \cdot V_1 = V_1 = Ae_1 + \cdots + Ae_n = \sum_{k,l} J_k e_l$$

Отображение

$$J_k \longrightarrow J_k e_l$$
$$a \longrightarrow a e_l$$

является сюръективным гомоморфизмом A-модулей. Так как J_k неприводим, то по лемме Шура, $J_k e_l \simeq J_k$ или $\{0\}$. Следовательно, $V_1 = U_1 + \cdots + U_m$, где $U_1, \dots, U_m$ – простые модули, каждый из который изоморфен некоторому $D_j^{n_j}$.

$\forall i$ имеем: $U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_m) = U_i$ или $\{0\}$. Если $U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_m) = U_i$, то U_i можно выкинуть из суммы – выкидывая лишние слагаемые, добьемся того, что $V_1 = U_1 \oplus \cdots \oplus U_m$. Это означает, что V_1 полупрост (как прямая сумма простых модулей).

Итак, V_0 полупрост, V_1 полупрост, значит, и $V = V_0 \oplus V_1$ полупрост, т.е. $\mathcal{R}\colon A \longrightarrow L(V)$ вполне приводимо.

$\Longleftarrow$:
$Rad(A)$ лежит в ядре любого неприводимого представления, следовательно, $Rad(A)$ лежит в ядре любого представления. Существует точное линейное представление $\mathcal{R}\colon A \hookrightarrow L(V)$, например, $V = A \oplus K$: $\mathcal{R}(a)(x, \lambda) = (ax + \lambda a, 0)$. Несложно видеть, что это представление является точным, так как $\mathcal{R}(a)(0,1) = (a, 0)$ – каждый ненулевой элемент A действует в $L(V)$ ненулевым образом, т.е. $Ker\,\mathcal{R} = \{0\}$. Следовательно, $Rad(A) = \{0\}$ и A полупроста. ■

Стоит отметить, что теория представлений ассоциативных алгебр играет центральную роль в теории представлений, так как к ним зачастую сводятся представления других алгебраических структур (причина в богатстве структуры ассоциативной алгебры – она содержит другие структуры в себе). Например, посмотрим на теорию представлений групп с точки зрения теории представлений ассоциативных алгебр.

Представления групп с точки зрения ассоциативных алгебр.

В прошлом семестре мы изучали теорию представлений групп, и отмечали, что с каждой группой G можно связать ассоциативную алгебру, а именно – ее *групповую алгебру* над полем K:

$$A = KG = \left\{ a = \sum_i \lambda_i g_i \mid g_i \in G, \lambda_i \in K \right\}$$

Можно воспринимать групповую алгебру как множество формальных линейных комбинаций элементов группы G с коэффициентами из поля K, которые складываются и

перемножаются по формальным правилам.

Всякое линейное представление группы G задает на пространстве представлений структуру модуля над групповой алгеброй, т.е. существует взаимно-однозначное соответствие:

$$\mathcal{R}\colon G \longrightarrow GL(V) \quad \leftrightarrow \quad \mathcal{R}\colon A \longrightarrow L(V) \quad \leftrightarrow \quad A\text{-модули } V$$

$$a = \sum_i \lambda_i\, g_i \Longrightarrow \mathcal{R}(a) = \sum_i \lambda_i\, \mathcal{R}(g_i), \;\; av = \sum_i \lambda_i\, \mathcal{R}(g_i)v$$

Таким образом, если мы хотим применять к представлениям групп теорию представлений ассоциативных алгебр, то представления групп удобно рассматривать как модули над групповой алгеброй этой группы.

Пусть $G = \{g_1, \dots, g_N\}$ – конечная группа (обозначим $g_1 = 1$ нейтральный элемент группы). Тогда $A = KG$ – конечномерная ассоциативная алгебра с базисом $(g_1, \dots, g_N)$.

Предложение 2. Если $char\ K = 0$, или $char\ K$ не делит $|G|$, то KG полупроста.

Доказательство.
Будем использовать следующий критерий полупростоты (см. лекцию 12): алгебра полупроста $\Leftrightarrow$ стандартное скалярное умножение на A невырождено.

Поймем, как устроено стандартное скалярное умножение на A. Пусть $\mathcal{L}\colon A \longrightarrow L(A)$ – левое регулярное представление. По определению, $\mathcal{L}(g_i)g_j = g_i g_j$, другими словами, операторы регулярного представления, соответствующие базисным элементам алгебры, переставляют базисные элементы. Матрица $\mathcal{L}(g_i)$ в базисе $(g_1, \dots, g_N)$ выглядит так:

- $\begin{pmatrix} 0 & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & 0 \end{pmatrix}$ при $g_i \neq 1$ (т.е. на диагонали стоят нули, все остальные элементы – нули или единицы, в каждой строке и каждом столбце стоит ровно одна единица)
- $\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$ при $g_i = 1$ (единичная матрица)

Теперь вычислим скалярное произведение двух базисных векторов:

$$(g_i \mid g_j) = tr\left(\mathcal{L}(g_i)\mathcal{L}(g_j)\right) = tr\mathcal{L}(g_i g_j) = \begin{cases} N \text{ при } g_i^{-1} = g_j \\ 0 \text{ иначе} \end{cases}$$

Отсюда следует, что стандартное скалярное умножение в базисе $(g_1, \dots, g_N)$ имеет следующую матрицу:

$$\begin{pmatrix} N & & & & & \\ & \ddots & & & & \\ & & N & & & \\ & & & \begin{boxed}\begin{matrix} 0 & N \\ N & 0 \end{matrix}\end{boxed} & & \\ & & & & \ddots & \\ & & & & & \begin{boxed}\begin{matrix} 0 & N \\ N & 0 \end{matrix}\end{boxed} \end{pmatrix}$$

т.е $(\cdot \mid \cdot)$ невырождено, поэтому A полупроста. ■

Как следствие из предложения 1 и предложения 2, получается теорема Машке:

Теорема Машке. Если $char\ K = 0$, или $char\ K$ не делит $|G|$, то все конечномерные линейные представления группы G вполне приводимы.

Далее считаем, что K алгебраически замкнуто и либо $char\ K = 0$, либо $char\ K$ не делит $|G|$. Над K существует единственная конечномерная алгебра с делением $D = K$ (действительно, в алгебре с делением минимальный многочлен любого элемента неприводим, а над алгебраически замкнутым полем минимальными многочленами являются только многочлены первой степени, т.е. любой элемент D является элементом поля K). Тогда из теоремы Веддербёрна – Артина вытекает, что

$$A = KG \simeq Mat_{n_1}(K) \oplus \cdots \oplus Mat_{n_s}(K),$$

а из предложения 1 следует, что все неприводимые представления G имеют вид $\mathcal{R}_i\colon\ G \longrightarrow GL(V_i),\ \ V_i \simeq K^{n_i}$, где $Mat_{n_i}(K)$ действует умножениями слева, а остальные $Mat_{n_j}(K)$ действуют нулевым образом.

Следствие 1. $n_1^2 + \cdots + n_s^2 = dim\ A = |G|$.

Теперь найдем количество неприводимых конечномерных линейных представлений G. Центр $Z(A) = \{z \in A \mid \forall a \in A\colon\ za = az\}$ – подалгебра в A. Как известно из курса лекций предыдущего семестра, $Z\big(Mat_n(K)\big) = K$, откуда следует, что

$$Z(KG) = Z\left(Mat_{n_1}(K)\right) \oplus \cdots \oplus Z\left(Mat_{n_s}(K)\right) = K^s$$

С другой стороны,

$$z = \sum_i \lambda_i\, g_i \in Z(KG) \Leftrightarrow zg = gz \Leftrightarrow gzg^{-1} = z,\ \ \forall g \in G$$

Но

$$gzg^{-1} = \sum_i \lambda_i \, g g_i g^{-1},$$

поэтому

$$z = \sum_i \lambda_i \, g_i \in Z(KG) \Leftrightarrow z = \sum_k \mu_k \, z_k,$$

где

$$z_k = \sum_{g_i \in C_k} g_i,$$

C_k – один из классов сопряженности в G.

Элементы z_k образуют базис $Z(KG)$.

Следствие 2. Количество неприводимых представлений $s = \dim Z(KG) =$ количество классов сопряженности в G.

Лекция 15. Группы Ли и алгебры Ли.

Перейдем от абстрактной алгебры к той части нашего курса, которая ближе к геометрии и анализу – группам Ли и алгебрам Ли. Зафиксируем основное поле $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$.

Определение 1. Вещественная/комплексная *линейная группа Ли* – это подгруппа $G \subseteq GL_n(\mathbb{K})$, являющаяся вещественным/комплексным дифференцируемым подмногообразием в $Mat_n(\mathbb{K}) \simeq \mathbb{K}^{n^2}$.

Напоминание. Подмножество $M \subseteq \mathbb{K}^N$ называется дифференцируемым многообразием, если $\forall x_0 \in M$ существует окрестность $U \ni x_0$ в $\mathbb{K}^N$, в которой M задается системой уравнений:

$$\begin{cases} f_1(x_1, \dots, x_N) = 0 \\ \vdots \\ f_m(x_1, \dots, x_N) = 0 \end{cases},$$

где $m \leq N$, f_i – дифференцируемые функции от координат $x_1, \dots, x_N$ на U и матрица Якоби

$$J = J(f_1, \dots, f_m) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_N} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \dots & \frac{\partial f_m}{\partial x_N} \end{pmatrix}$$

имеет ранг m на U.

Отсюда следует, что существует ненулевой минор порядка m, например:

$$\begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_m} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \dots & \frac{\partial f_m}{\partial x_m} \end{vmatrix} \neq 0$$

Тогда, по теореме о неявной функции, координаты $x_{m+1}, \dots, x_N$ принимают на $M \cap U$ любой набор значений из некоторой окрестности в $\mathbb{K}^{N-m}$, а $\begin{cases} x_i = \varphi_i(x_{m+1}, \dots, x_N) \\ i = 1, \dots, m \end{cases}$ на $M \cap U$, где φ_i – дифференцируемые функции. Таким образом, $x_{m+1}, \dots, x_N$ – локальные координаты на $M \cap U$ (см. рис. 15.1). Размерность многообразия M: $\dim M = N - m$.

Замечание. Если $rk\, J(x_0) = m$, то $rk\, J = m$ и в некоторой окрестности $U \ni x_0$.

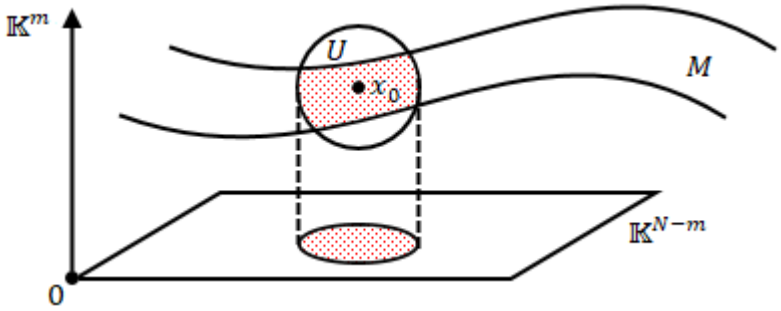


Рис. 15.1. $M \subseteq \mathbb{K}^N$ – дифференцируемое многообразие, $x_{m+1}, \dots, x_N$ – локальные координаты на $M \cap U$

В нашем курсе: группы Ли = линейные группы Ли.

Примеры групп Ли.

1) $G = GL_n(\mathbb{K})$, $\dim G = n^2$

2) $G = \mathbb{K}^n$ с операцией сложения (покомпонентно). Ее реализация как группы Ли:

$$G = \mathbb{K}^n \simeq \left\{ \begin{pmatrix} 1 & x_1 & \cdots & x_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \mid x_i \in \mathbb{K} \right\} \subset GL_{n+1}(\mathbb{K})$$

$\dim G = n$

3) $G = (\mathbb{K}^\times)^n$ с операцией умножения (покомпонентно). Ее реализация как группы Ли:

$$G = (\mathbb{K}^\times)^n \simeq \left\{ \begin{pmatrix} x_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & x_n \end{pmatrix} \mid x_i \in \mathbb{K}^\times \right\} \subseteq GL_n(\mathbb{K})$$

$\dim G = n$

4) Пусть $G \subseteq GL_n(\mathbb{K})$, $H \subseteq GL_m(\mathbb{K})$ – группы Ли. Тогда и $G \times H$ – группа Ли:

$$G \times H \simeq \left\{ \left(\begin{array}{c|c} g & 0 \\ \hline 0 & h \end{array} \right) \mid g \in G, h \in H \right\} \subseteq GL_{n+m}(\mathbb{K})$$

$\dim(G \times H) = \dim(G) + \dim(H)$

Предложение 1. Пусть $G \subseteq GL_n(\mathbb{K})$ – подгруппа. Если G – многообразие в окрестности $g_0 \in G$, то G – группа Ли.

Доказательство.
Пусть $g_1 \in G$ – другая точка. Положим $g = g_1 g_0^{-1} \in G$ и рассмотрим отображение левого сдвига:

$$l_g\colon\ Mat_n(\mathbb{K}) \longrightarrow Mat_n(\mathbb{K})$$
$$x \mapsto gx$$

- невырожденное линейное преобразование $\Longrightarrow$ диффеоморфизм, $l_g(G) = G$.

Пусть в окрестности $U \ni g_0$ $G \cap U$ задается системой уравнений $\begin{cases} f_i(x) = 0 \\ i = 1, \dots, m \end{cases}$, $rk\, J(f_1, \dots, f_m) = m$. Тогда в окрестности $gU \ni g_1$: $l_g(G \cap U) = G \cap gU$ задается системой уравнений $\begin{cases} \widetilde{f_i}(x) = 0 \\ i = 1, \dots, m \end{cases}$, где $\widetilde{f_i}(x) = f_i(g^{-1}x)$ – тоже дифференцируемые функции и $J(\widetilde{f_1}, \dots, \widetilde{f_m}) = J(f_1, \dots, f_m) \cdot l_{g^{-1}}$, откуда $rk\, J(\widetilde{f_1}, \dots, \widetilde{f_m}) = rk\, J(f_1, \dots, f_m) = m$. Следовательно, G является многообразием в окрестности g_1. ■

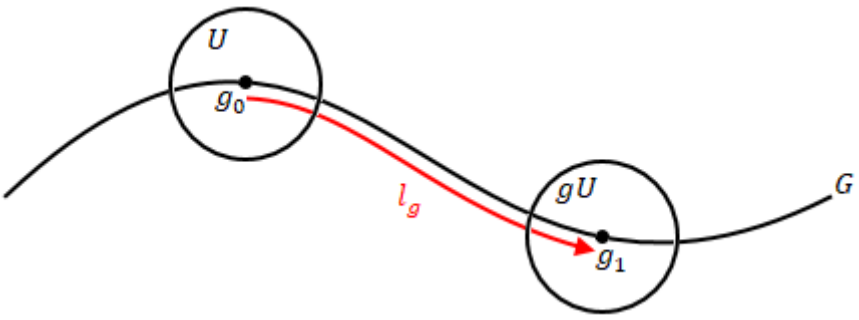


Рис. 15.2. К доказательству предложения 1

Замечания:

1) Для того, чтобы G оказалась группой Ли, достаточно проверить условие $rk\, J(g_0) = m$ (где J – матрица Якоби системы из m уравнений, задающих G в окрестности точки g_0).

2) Чаще всего удобно брать $g_0 = E = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$

Отметим, что $rk\, J(g_0)$ часто неудобно вычислять в явном виде, удобнее рассматривать пространство решений соответствующей однородной системы линейных уравнений. Как известно из курса линейной алгебры, размерность этого пространства будет равна $N - rk\, J(g_0)$. Геометрический смысл пространства решений соответствующей однородной системы линейных уравнений, как известно из курса дифференциальной геометрии, - это касательное пространство к многообразию G в точке g_0.

Напоминание. Касательный вектор к параметризованной кривой $x(t) \in \mathbb{K}^n$ в точке $x_0 = x(t_0)$:

$$X = \dot{x}(t_0) = \left.\frac{dx(t)}{dt}\right|_{t=t_0} = \left(\left.\frac{dx_1(t)}{dt}\right|_{t=t_0}, \dots, \left.\frac{dx_N(t)}{dt}\right|_{t=t_0}\right)$$

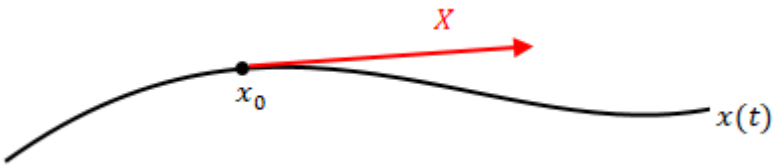


Рис. 15.3. Касательный вектор

Если $x(t) \in M$, где M – многообразие, заданное системой уравнений $\begin{cases} f_i(x_{m+1}, \dots, x_N) = 0 \\ i = 1, \dots, m \end{cases}$ $rk\, J(x_0) = m$, то касательный вектор X удовлетворяет однородной системе линейных уравнений:

$$\begin{cases} \dfrac{\partial f_i(x_0)}{\partial x_1} \cdot X_1 + \dots + \dfrac{\partial f_i(x_0)}{\partial x_N} \cdot X_N = 0 \\ \forall i = 1, \dots, m \end{cases}$$

Выражение $\frac{df_i(x_0)}{dx_1} \cdot X_1 + \dots + \frac{df_i(x_0)}{dx_N} \cdot X_N$ можно записать как $d_{x_0} f_i(X)$ – дифференциал функции f_i в точке x_0 на векторе X. Вообще, $d_{x_0} f$ (дифференциал функции f в точке x_0) определяется так:

$$d_{x_0} f = \frac{\partial f(x_0)}{\partial x_1} \cdot dx_1 + \dots + \frac{\partial f(x_0)}{\partial x_N} \cdot dx_N,$$

где $dx_1, \dots, dx_N$ – координатные функции на векторах пространства $\mathbb{K}^n$.

Верно и обратное: если X удовлетворяет однородной системе линейных уравнений, приведенной выше, то существует кривая $x(t) \in M$, проходящая через точку x_0, такая что $\dot{x}(t_0) = X$.

Таким образом, множество решений однородной системы линейных уравнений с матрицей коэффициентов $J(x_0)$ – это в точности $T_{x_0}M$ (касательное пространство к многообразию M в точке x_0), т.е. множество касательных векторов ко всевозможным кривым на M, проходящих через точку x_0.

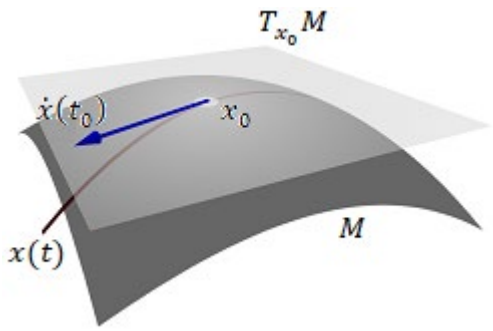


Рис. 15.4. Касательное пространство

Вооружившись приведенными выше фактами, рассмотрим новые примеры групп Ли:

Примеры групп Ли.

1) $G = SL_n(\mathbb{K}) = \{g \mid \det g = 1\}$

$$\det g = \sum_{(i_1,\dots,i_n)} \left(g_{1i_1} \cdot \dots \cdot g_{ki_k} \cdot \dots \cdot g_{ni_n}\right) \cdot sgn(i_1, \dots, i_n)$$

Продифференцируем в точке $g = E$:

$$d_{g=E}(\det g - 1) = \left(\sum_{\substack{(i_1,\dots,i_n) \\ k=1,\dots,n}} \left(g_{1i_1} \cdot \dots \cdot dg_{ki_k} \cdot \dots \cdot g_{ni_n}\right) \cdot sgn(i_1, \dots, i_n) \right)\Bigg|_{g=E} =$$

$$= dg_{11} + \dots + dg_{kk} + \dots + dg_{nn} = tr(dg)$$

Однородная система линейных уравнений, соответствующая матрице Якоби, выглядит следующим образом: $trX = 0$. Размерность пространства решений этой системы равна $n^2 - 1$. Следовательно, $rk\, J(E) = n^2 - (n^2 - 1) = 1$, откуда следует, что $SL_n(\mathbb{K})$ – группа Ли.

2) $G = O_n(\mathbb{K}) = \{g \mid gg^T = E\}$

Условие $gg^T = E$ дает $\frac{n(n+1)}{2}$ уравнений на элементы матрицы g (а не n^2, так как матрица gg^T симметрична, и элементы ниже главной диагонали однозначно определяются элементами выше главной диагонали).

$$d_{g=E}(gg^T - E) = (dg \cdot g^T + g \cdot (dg)^T)|_{g=E} = dg + (dg)^T$$

Соответствующая однородная система линейных уравнений: $X + X^T = 0 \Leftrightarrow X^T = -X$, т.е. матрицы X, удовлетворяющие этой системе, являются кососимметричными, и пространство решений этой системы является пространством кососимметрических матриц. Размерность этого пространства равна $\frac{n(n-1)}{2}$, следовательно, $rk\, J(E) = n^2 - \frac{n(n-1)}{2} = \frac{n(n+1)}{2}$, откуда следует, что $O_n(\mathbb{K})$ – группа Ли.

3) $G = U_n(\mathbb{C}) = \{g \in Mat_n(\mathbb{C}) \mid gg^* = E\}$ ($g^* = \bar{g}^T$ – эрмитово сопряженная матрица)

Заметим, что условие $gg^* = E$ задает систему из $n + 2 \cdot \frac{n(n-1)}{2} = n^2$ вещественно дифференцируемых уравнений (а не $2n^2$, так как матрица gg^* эрмитова, и элементы ниже главной диагонали однозначно определяются элементами выше главной диагонали).

$$d_{g=E}(gg^* - E) = (dg \cdot g^* + g \cdot (dg)^*)|_{g=E} = dg + (dg)^*$$

Соответствующая однородная система линейных уравнений: $X + X^* = 0 \Leftrightarrow X^* = -X$, т.е. матрицы X, удовлетворяющие этой системе, являются косоэрмитовыми, и пространство решений этой системы является пространством косоэрмитовых матриц. Размерность этого пространства равна n^2, следовательно, $rk\, J(E) = 2n^2 - n^2 = n^2$, откуда следует, что $U_n(\mathbb{C})$ – вещественная группа Ли.

Лекция 16. Свойства групп Ли.

Предложение 1. Всякая группа Ли $G \subseteq GL_n(\mathbb{K})$ замкнута в $GL_n(\mathbb{K})$.

Доказательство.
Рассмотрим замыкание $\bar{G} \subseteq GL_n(\mathbb{K})$ и докажем, что это подгруппа Ли. Пусть $g, h \in \bar{G}$, т.е. $g = \lim\limits_{n\to\infty} g_n$ и $h = \lim\limits_{n\to\infty} h_n$, где $g_n, h_n \in G$. Тогда:

- $gh = \lim\limits_{n\to\infty} \underbrace{g_n h_n}_{\in G} \in \bar{G}$
- $g^{-1} = \lim\limits_{n\to\infty} \underbrace{g_n^{-1}}_{\in G} \in \bar{G}$

Значит, $\bar{G}$ – подгруппа.

G – многообразие в $Mat_n(\mathbb{K})$, следовательно, $\forall g \in G$: G замкнуто в некоторой окрестности g. Отсюда следует, что G открыто в $\bar{G}$.

$\forall g \in \bar{G}$ рассмотрим смежный класс gG – на него можно посмотреть как на результат действия на G преобразования левого сдвига: $gG = l_g(G)$. Но l_g – диффеоморфизм, а значит, сохраняет все топологические свойства множеств. Поэтому, если G открыто в $\bar{G}$, то и $l_g(G)$ открыто в $\bar{G}$, откуда следует, что $gG \cap G \neq \emptyset$. Но если пересечение двух смежных классов непусто, то они совпадают, т.е. $gG = G$, тогда $g \in G$. Следовательно, $\bar{G} = G$. ■

Обратное утверждение верно лишь отчасти. Например, на прошлой лекции мы видели, что группа унитарных матриц $U_n(\mathbb{C})$ является подгруппой Ли в группе $GL_n(\mathbb{C})$, но подгруппой вещественной, а не комплексной. Однако, верно следующее утверждение, которое мы приведем без доказательства:

Теорема Картана. Любая замкнутая подгруппа в $GL_n(\mathbb{R})$ есть вещественная группа Ли.

Будем дальше анализировать связь между топологической и групповой структурой групп Ли. Для этого напомним еще одно понятие из дифференциальной геометрии.

Напоминание. Пусть $M \subseteq \mathbb{K}^N$ – многообразие, тогда $M = \bigsqcup\limits_{i\in I} M_i$, где M_i – открыты, замкнуты, связны ($\forall x, y \in M_i$ существует соединяющая их непрерывная (гладкая) кривая). M_i называются комонентами связности многообразия M, они определены однозначно, множество индексов I не более чем счетно.

Теорема 1. Пусть G – группа Ли, $G^0 \subseteq G$ – связная компонента, содержащая E. Тогда:

1) G^0 – подгруппа Ли.
2) $G^0 \lhd G$.
3) Остальные компоненты связности в G – это в точности смежные классы gG^0 ($g \in G$).

Доказательство.
3) $\forall g \in G$ отображение левого сдвига l_g: $G \longrightarrow G$, $x \mapsto gx$ является диффеоморфизмом, поэтому l_g переставляет компоненты связности между собой. Отсюда следует, что gG^0 – тоже компонента связности. Такие компоненты связности покрывают всю G, а значит, других компонент связности нет.

1) Сначала докажем, что G^0 – подгруппа. Пусть $g \in G^0$, тогда $gG^0 \cap G^0 \neq \emptyset$ (так как это пересечение содержит, например, элемент g), откуда следует, что $gG^0 = G^0$, т.е. G^0 замкнуто относительно умножения: $G^0 \cdot G^0 = G^0$.

Докажем, что G^0 замкнуто относительно взятия обратного элемента. Рассмотрим отображение инверсии ι:

$$\iota\colon G \longrightarrow G$$
$$x \mapsto x^{-1}$$

ι также является диффеоморфизмом, поэтому переставляет компоненты связности между собой. При этом $\iota(G^0) \cap G^0 \neq \emptyset$ (так как это пересечение содержит, например, элемент e), откуда следует, что $\iota(G^0) = G^0$, т.е. G^0 замкнуто относительно взятия обратного элемента. Следовательно, G^0 – подгруппа.

Очевидно, что G^0 – подмногообразие (потому что это связная компонента G). Следовательно, G^0 – подгруппа Ли.

2) $\forall g \in G$ сопряжение i_g: $G \longrightarrow G$, $x \mapsto gxg^{-1}$ является диффеоморфизмом, поэтому i_g переставляет компоненты связности между собой. При этом $gG^0g^{-1} \cap G^0 \neq \emptyset$ (так как это пересечение содержит, например, элемент e), откуда следует, что $gG^0g^{-1} = G^0$, т.е. $G^0 \lhd G$. ■

Пример. Расмотрим группу $G = O_n(\mathbb{R}) = \{g \mid gg^T = E\}$. Тогда $O_n(\mathbb{R})^0 = SO_n(\mathbb{R})$. В самом деле:

- $SO_n(\mathbb{R})$ открыто в $O_n(\mathbb{R})$: следует из того ,что $SO_n(\mathbb{R})$ задается условие $\det > 0$
- $SO_n(\mathbb{R})$ замкнуто в $O_n(\mathbb{R})$: следует из того ,что $SO_n(\mathbb{R})$ задается условие $\det = 0$
- $SO_n(\mathbb{R})$ связно: матрицы из $SO_n(\mathbb{R})$ являются матрицами собственных ортогональных линейных операторов, значит (по теореме о каноническом виде матрицы ортогонального оператора), существует ортонормированный базис, в котором матрица оператора имеет канонический вид:

$$h = \begin{pmatrix} \begin{pmatrix} \cos\varphi_1 & -\sin\varphi_1 \\ \sin\varphi_1 & \cos\varphi_1 \end{pmatrix} & & & & & \mathbf{0} \\ & \ddots & & & & \\ & & \begin{pmatrix} \cos\varphi_k & -\sin\varphi_k \\ \sin\varphi_k & \cos\varphi_k \end{pmatrix} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ \mathbf{0} & & & & & 1 \end{pmatrix}$$

Т.е. $\forall g \in SO_n(\mathbb{R})$: $g = chc^{-1}$. Но матрицу h можно соединить непрерывной кривой с единичной матрицей:

$$h(t) = \begin{pmatrix} \begin{pmatrix} \cos t\varphi_1 & -\sin t\varphi_1 \\ \sin t\varphi_1 & \cos t\varphi_1 \end{pmatrix} & & & & & \mathbf{0} \\ & \ddots & & & & \\ & & \begin{pmatrix} \cos t\varphi_k & -\sin t\varphi_k \\ \sin t\varphi_k & \cos t\varphi_k \end{pmatrix} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ \mathbf{0} & & & & & 1 \end{pmatrix}$$

$h(t)$ – гладкая кривая в $SO_n(\mathbb{R})$, соединяющая $h = h(1)$ с $E = h(0)$. Отсюда следует, что $g(t) = ch(t)c^{-1}$ – гладкая кривая в $SO_n(\mathbb{R})$, соединяющая $g = g(1)$ с $E = g(0)$. Это означает, что $SO_n(\mathbb{R})$ связно.

Другая компонента связности – это $O_n(\mathbb{R})\backslash SO_n(\mathbb{R})$ (объяснить это можно, например, тем, что $O_n(\mathbb{R})\backslash SO_n(\mathbb{R}) = rSO_n(\mathbb{R})$, т.е. это смежный класс матрицы r, где r – несобственная ортогональная матрица, например, матрица отражения вдоль какой-то координатной прямой).

Теорема 1 показывает, что любая группа Ли составлена как бы из двух “этажей”:

- связного: $G^0 \lhd G$ – связная группа Ли
- дискретного: G/G^0 – не более чем счетная дискретная группа

Устройством G/G^0 занимается абстрактная теория групп, здесь нет топлогической специфики. Вся суть теории Ли относится к связным группам – именно им уделяется особое внимание в теории групп Ли. Связные группы Ли обладают весьма специфическими свойствами, например: устройство такой группы полностью определяется сколь угодно малой окрестностью E.

Предложение 2. Связная группа Ли G порождается (как абстрактная группа) сколь угодно малой окрестностью E.

Доказательство.

Пусть $U \subseteq G$ – окрестность E. Пусть $H \subseteq G$ – подгруппа, порожденная множеством U. $\forall h \in H$: hU – окрестность точки h, $hU \subseteq H$, следовательно, H открыта в G, а значит, H – подгруппа Ли в G. Тогда (по предложению 1) H замкнута в G. Так как G связна, то $H = G$. ■

Алгебра Ли.

Доказанное утверждение наводит на мысль, что на касательном пространстве к E в группе Ли G должна существовать какая-то естественная структура, которая полностью определяет структуру самой группы Ли (по крайней мере, если эта группа связна). Займемся обоснованием этой догадки. Пусть $G \subseteq GL_n(\mathbb{K})$ – группа Ли.

Лемма 1. Пусть $g(t), h(t)$ – гладкие кривые, $g(0) = h(0) = E$, которые имеют в E касательные векторы $\frac{d}{dt}\Big|_{t=0} g(t) = X$, $\frac{d}{dt}\Big|_{t=0} h(t) = Y$. Тогда касательный вектор к E кривой $g(t)h(t)$ равен $\frac{d}{dt}\Big|_{t=0} g(t)h(t) = X + Y$.

Доказательство.

$$\left(\frac{d(g(t)h(t))}{dt}\right)\Bigg|_{t=0} = \left(\frac{dg(t)}{dt}h(t) + \frac{dh(t)}{dt}g(t)\right)\Bigg|_{t=0} = Xh(0) + Yg(0) = X + Y$$

■

Лемма 2. В обозначениях леммы 1:

$$\frac{d}{dt}\Big|_{t=0} g(t)^{-1} = -X$$

Доказательство.
Воспользуемся леммой 1: возьмем $h(t) = g(t)^{-1}$, тогда $g(t)h(t) = E$. По лемме 1, $\frac{d}{dt}\Big|_{t=0} g(t)h(t) = X + Y$. С другой стороны (так как $E = const$), $\frac{d}{dt}\Big|_{t=0} g(t)h(t) = 0$. Получаем $Y = -X$, что и требовалось. ■

Лемма 3. В обозначениях леммы 1: $c(t,s) = [g(t), h(s)]_{gr} = g(t)h(s)g(t)^{-1}h(s)^{-1}$ (групповой коммутатор $g(t)$ и $h(s)$). Тогда

$$\frac{\partial^2 c(t,s)}{\partial t \partial s}\Bigg|_{s=t=0} = [X, Y] = XY - YX$$

Доказательство.

- Дифференцируем по s:

$$\left.\frac{\partial}{\partial s}\right|_{s=0} c(t,s) = g(t)\cdot\left.\frac{d}{ds}\right|_{s=0} h(s)\cdot g(t)^{-1}\cdot h(0)^{-1} + g(t)\cdot h(0)\cdot g(t)^{-1}\cdot\left.\frac{d}{ds}\right|_{s=0} h(s)^{-1}$$
$$= g(t)Yg(t)^{-1} - Y$$

- Дифференцируем по t:

$$\left.\frac{\partial^2}{\partial t\partial s}\right|_{s=t=0} c(t,s) = \left.\frac{d}{dt}\right|_{t=0} (g(t)Yg(t)^{-1} - Y) =$$

$$= \left.\frac{d}{dt}\right|_{t=0} g(t)\cdot Y\cdot g(0)^{-1} + g(0)\cdot Y\cdot\left.\frac{d}{dt}\right|_{t=0} g(t)^{-1} = XY + Y(-X) = XY - YX$$

■

Обратим внимание на операцию взятия коммутатора. *Коммутатор* $[X,Y] = XY - YX$ – новая бинарная операция на $Mat_n(\mathbb{K})$, которая обладает следующими свойствами:

- 1) Билинейность
- 2) Кососимметричность (антикоммутативность): $[X,Y] = -[Y,X]$
- 3) Тождество Якоби: $\big[[X,Y],Z\big] + \big[[Y,Z],X\big] + \big[[Z,X],Y\big] = 0$

Упражнение. Проверить тождество Якоби.

Как мы знаем, если на векторном пространстве $Mat_n(\mathbb{K})$ задана билинейная бинарная операция, то на нем возникает структура алгебры (эту операцию можно рассматривать в качестве умножения). Алгебра, в которой операция умножения удовлетворяет свойствам 1) – 3), называется *алгеброй Ли*. В частности, $Mat_n(\mathbb{K})$ – алгебра Ли.

Леммы 1) – 3), доказанные выше, позволяют получить следующую теорему:

Теорема 2. Пусть $G \subseteq GL_n(\mathbb{K})$ – линейная группа Ли. Тогда касательное пространство $T_E G \subseteq Mat_n(\mathbb{K})$ – подалгебра Ли (такие алгебры Ли называются линейными, обозначение: $T_E G = Lie(G) = \mathfrak{g}$ – (*касательная*) *алгебра Ли* группы Ли G).

Доказательство.
Пусть $X, Y \in \mathfrak{g}$, т.е. $X = \dot{g}(0), Y = \dot{h}(0)$, где $g(t), h(s) \in G$, $g(0) = h(0) = E$. Рассмотрим $c(t,s) = [g(t), h(s)]_{gr} \in G$ и для любого значения параметра t рассмотрим $c(t,s)$ как кривую, зависящую от s. Имеем: $c(t,0) = E$, поэтому (см. лемму 3)

$$\left.\frac{\partial}{\partial s}\right|_{s=0} c(t,s) = g(t)Yg(t)^{-1} - Y \in \mathfrak{g}$$

Отсюда следует, что и

$$\left.\frac{\partial^2 c(t,s)}{\partial t \partial s}\right|_{s=t=0} = \left.\frac{d}{dt}\right|_{t=0} (g(t)Yg(t)^{-1} - Y) = [X,Y] \in \mathfrak{g}$$

Таким образом, $\mathfrak{g}$ замкнуто относительно операции взятия коммутатора, следовательно, является подалгеброй Ли. ■

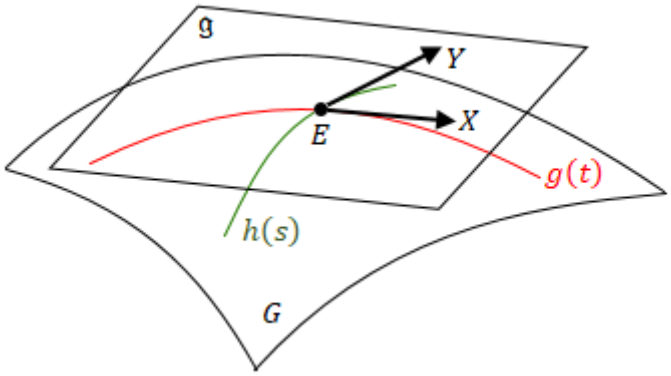


Рис. 16.1. Иллюстрация к теореме 2

Примеры касательных алгебр Ли.

1) $\mathfrak{gl}_n(\mathbb{K}) = Mat_n(\mathbb{K})$. Договоримся далее, что обозначение множества квадратных матриц $Mat_n(\mathbb{K})$ означает ассоциативную алгебру, а $\mathfrak{gl}_n(\mathbb{K})$ – алгебру Ли (т.е. вместо ассоциативного умножения мы рассматриваем операцию коммутирования).

Приведем примеры касательных алгебр Ли групп Ли, которые мы рассматривали в качестве примера на прошлой лекции ($SL_n(\mathbb{K})$, $O_n(\mathbb{K})$, $U_n(\mathbb{C})$ соответственно).

2) $\mathfrak{sl}_n(\mathbb{K}) = \{X \in \mathfrak{gl}_n(\mathbb{K}) \mid trX = 0\}$

3) $\mathfrak{o}_n(\mathbb{K}) = \{X \in \mathfrak{gl}_n(\mathbb{K}) \mid X^T = -X\}$

4) $\mathfrak{u}_n(\mathbb{C}) = \{X \in \mathfrak{gl}_n(\mathbb{C}) \mid X^* = -X\}$

Итак, алгебра Ли группы Ли – это структура на касательном пространстве к E в группе Ли, которая полностью определяет структуру самой группы Ли (если эта группа связна). Группа Ли по алгебре Ли восстанавливается с помощью экспоненциального отображения – мы увидим это на следующей лекции.

Лекция 17. Экспоненциальное отображение.

Экспоненциальное отображение.

Для матриц экспоненциальное отображение можно задать с помощью абсолютно сходящегося степенного ряда:

$$exp\colon\ Mat_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K})$$
$$\exp(X) = X + \frac{X^2}{2!} + \cdots + \frac{X^k}{k!} + \cdots$$

Отметим важное свойство экспоненциального отображения, которое пригодится нам в дальнейшем: если $[X, Y] = 0$, т.е. матрицы X и Y коммутируют, то

$$\exp(X + Y) = \exp(X)\exp(Y)$$

Из того, что ряд для $\exp(X)$ абсолютно сходится, следует, что отображение exp дифференцируемо по своему аргументу, т.е. у этого отображения существует дифференциал.

Напоминание. Пусть $\varphi\colon \mathbb{K}^n \supseteq N \longrightarrow M \subseteq \mathbb{K}^m$ – дифференцирумое отображение многообразий. Его дифференциал в точке $x_0 \in N$ - это отображение $d_{x_0}\varphi\colon\ T_{x_0}N \longrightarrow T_{y_0}M$, где $y_0 = \varphi(x_0)$. Дифференциал переводит касательные векторы к прямым в N в касательные векторы к образам этих кривых в M: если $X = \left.\frac{d}{dt}\right|_{t=t_0} x(t)$, $x(t) \in N$, $x(t_0) = x_0$ и $y(t) = \varphi(x(t)) \in M$, то

$$d_{x_0}\varphi(X) = Y = \left.\frac{d}{dt}\right|_{t=t_0} y(t)$$

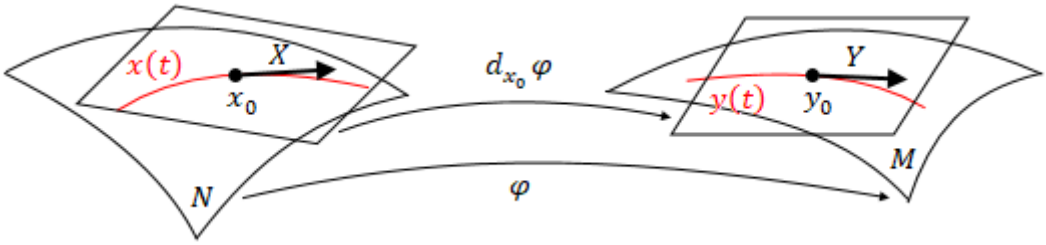


Рис. 17.1. Дифференциал отображения

В координатах: $\varphi(x_1, \dots, x_n) = (f_1(x), \dots, f_m(x))$, откуда следует, что $d_{x_0}\varphi$ – линейное отображение, задаваемое матрицей

$$J(x_0) = \begin{pmatrix} \frac{\partial f_1(x_0)}{\partial x_1} & \cdots & \frac{\partial f_1(x_0)}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m(x_0)}{\partial x_1} & \cdots & \frac{\partial f_m(x_0)}{\partial x_n} \end{pmatrix}$$

Если $m = n$, и $\det J(x_0) \neq 0$, то φ – диффеоморфизм окрестности x_0 в N на окрестность y_0 в M. В частности, exp – диффеоморфизм окрестности 0 в $Mat_n(\mathbb{K})$ на окрестность E в $GL_n(\mathbb{K})$.

Лемма 1. Дифференциал экспоненциального отображения в нуле – это тождественное отображение:

$$d_0 exp = id$$

Доказательство.
Пусть $X \in Mat_n(\mathbb{K})$, рассмотрим прямую $x(t) = tX$ (т.е. кривую самого простого вида, удовлетворяющую условию $x(0) = 0$, $\dot{x}(0) = X$). Рассмотрим ее экспоненциальный образ:

$$\exp x(t) = E + tX + O(t^2)$$

Имеем:

$$\left.\frac{d}{dt}\right|_{t=t_0} \exp x(t) = X$$

■

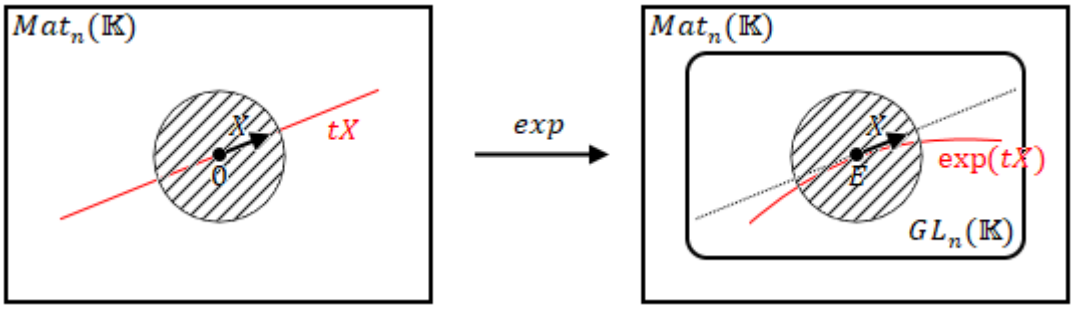


Рис. 17.2. $d_0 exp = id$

Лемма 2. Пусть $X = \dot{g}(0)$, $g(t) \in GL_n(\mathbb{K})$, $g(0) = E$. Тогда

$$\exp X = \lim_{n\to\infty} g\left(\frac{1}{n}\right)^n$$

Доказательство.
Из леммы 1 следует, что $g(t) = \exp x(t)$ при малых t, где $x(t) \in Mat_n(\mathbb{K})$, $x(0) = 0$ и $\left.\frac{d}{dt}\right|_{t=t_0} x(t) = X$. Следовательно, $x(t) = tX + O(t^2)$ при малых t. Тогда

$$g\left(\frac{1}{n}\right) = \exp x\left(\frac{1}{n}\right) = \exp\left(\frac{1}{n}X + O\left(\frac{1}{n^2}\right)\right)$$

и

$$g\left(\frac{1}{n}\right)^n = \exp n\left(\frac{1}{n}X + O\left(\frac{1}{n^2}\right)\right) = \exp\left(X + O\left(\frac{1}{n}\right)\right) \xrightarrow[\text{при } n\to\infty]{} \exp X$$

■

Теорема. Пусть $G \in GL_n(\mathbb{K})$ – группа Ли. Тогда $\exp(\mathfrak{g}) \subseteq G$, причем exp диффеоморфно отображает окрестность 0 в $\mathfrak{g}$ на окрестность E в G.

Доказательство.
1) Докажем, что $\exp(\mathfrak{g}) \subseteq G$: если $X \in \mathfrak{g}$, тогда по определению $X = \dot{g}(0)$, $g(t) \in G$, $g(0) = E$. Воспользуемся леммой 2:

$$\exp X = \lim_{n\to\infty} \underbrace{g\left(\frac{1}{n}\right)^n}_{\in G} \in G,$$

так как G замкнута в $GL_n(\mathbb{K})$.

2) Существует окрестность $U \ni 0$ в $Mat_n(\mathbb{K})$, такая что $V = \exp(U)$ – окрестность E в $GL_n(\mathbb{K})$, и exp: $U \longrightarrow V$ – диффеоморфизм (см. рис. 17.2). Далее, $\mathfrak{g} \cap U$ – замкнутое подмногообразие в U, откуда следует (так как exp: $U \longrightarrow V$ – диффеоморфизм), что $\exp(\mathfrak{g} \cap U)$ – замкнутое подмногообразие в V, и $\exp(\mathfrak{g} \cap U) \subseteq G \cap V$. Уменьшив V и U при необходимости, можно добиться, чтобы $G \cap V$ было связным подмногообразием в V. Тогда $\dim(G \cap V) = \dim G = \dim \mathfrak{g} = \dim(\mathfrak{g} \cap U) = \dim \exp(\mathfrak{g} \cap U)$. Отсюда следует, что $\exp(\mathfrak{g} \cap U)$ открыто и замкнуто в $G \cap V$, а так как $G \cap V$ связно, то $\exp(\mathfrak{g} \cap U) = G \cap V$. ■

Замечание. С помощью отображения exp можно перенести локальные координаты из окрестности 0 в $Mat_n(\mathbb{K})$ на окрестность E в $GL_n(\mathbb{K})$. При такой замене координат линейная группа Ли G превращается в свою алгебру Ли $\mathfrak{g}$.

Доказанная выше теорема является очень важной, так как она позволяет восстанавливать группы Ли по их касательным алгебрам Ли, которые устроены проще.

Предложение 1. Связная линейная группа Ли $G \subseteq GL_n(\mathbb{K})$ однозначно определяется своей касательной алгеброй Ли $\mathfrak{g} \subseteq \mathfrak{gl}_n(\mathbb{K})$.

Доказательство.
По теореме, доказанной выше, $\exp(\mathfrak{g})$ содержит окрестность E в G, следовательно, порождает G как абстрактную группу (см. предложение 2 из прошлой лекции). ■

Предложение 2. Пусть $G, H \subseteq GL_n(\mathbb{K})$ – группы Ли, тогда $G \cap H$ – группа Ли, $Lie(G \cap H) = \mathfrak{g} \cap \mathfrak{h}$.

Доказательство.
Существует окрестности $U \ni 0$ в $Mat_n(\mathbb{K})$ и $V \ni E$ в $GL_n(\mathbb{K})$, такие что exp: $U \longrightarrow V$ – диффеоморфизм, $\mathfrak{g} \cap U \nrightarrow G \cap V$, $\mathfrak{h} \cap U \nrightarrow H \cap V$. Отсюда следует, что exp: $(\mathfrak{g} \cap \mathfrak{h} \cap U) \nrightarrow G \cap H \cap V$ – диффеоморфизм многообразий. Поэтому $G \cap H$ –

подмногообразие в V, а так как $G \cap H$ – подгруппа в $GL_n(\mathbb{K})$ (следует из условия), то $G \cap H$ – группа Ли,.

Осталось заметить, что $d_0 exp = id$: $\mathfrak{g} \cap \mathfrak{h} \rightarrowtail T_E(G \cap H)$, поэтому $T_E(G \cap H) = \mathfrak{g} \cap \mathfrak{h}$. ■

Примеры.

1) $SO_n(\mathbb{K}) = O_n(\mathbb{K}) \cap SL_n(\mathbb{K})$ – группа Ли,
$\mathfrak{so}_n(\mathbb{K}) = \mathfrak{o}_n(\mathbb{K}) \cap \mathfrak{sl}_n(\mathbb{K}) = \{X \in \mathfrak{gl}_n(\mathbb{K}) \mid X^T = -X,\ \ trX = 0\}$

Как легко заметить, условие $trX = 0$ следует из условия $X^T = -X$, т.е. $\mathfrak{so}_n(\mathbb{K}) = \mathfrak{o}_n(\mathbb{K})$. Это неудивительно, ведь $SO_n(\mathbb{K}) = \{g \in O_n(\mathbb{K}) \mid \det g \neq -1\}$ – открытая подгруппа Ли в $O_n(\mathbb{K})$.

2) $SU_n(\mathbb{C}) = U_n(\mathbb{C}) \cap SL_n(\mathbb{C})$ - группа Ли,
$\mathfrak{su}_n(\mathbb{C}) = \mathfrak{u}_n(\mathbb{C}) \cap \mathfrak{sl}_n(\mathbb{C}) = \{X \in \mathfrak{gl}_n(\mathbb{C}) \mid X^* = -X,\ \ trX = 0\}$, $\dim \mathfrak{su}_n(\mathbb{C}) = x^2 - 1$.

Предложение 3. Если группа Ли G коммутативна, то ее алгебра Ли $\mathfrak{g}$ коммутативна (т.е. $[X, Y] = [Y, X] = 0$, $\forall X, Y \in \mathfrak{g}$). Если G связна, то верно и обратное.

Доказательство.
$\Longrightarrow$:
Пусть $X, Y \in \mathfrak{g}$, $X = \dot{g}(0), Y = \dot{h}(0)$, $g(t), h(s) \in G$, $g(0) = h(0) = E$. Тогда (см. лемму 3 прошлой лекции)

$$[X, Y] = \frac{\partial^2}{\partial t \partial s}\bigg|_{s=t=0} [g(t), h(s)]_{gr}$$

Так как G коммутативна, то $[g(t), h(s)]_{gr} = E$, поэтому $[X, Y] = 0$.

$\Longleftarrow$:
Если $\forall X, Y \in \mathfrak{g}$: $[X, Y] = 0$, то $\exp(X)\exp(Y) = \exp(X + Y) = \exp(Y)\exp(X)$, т.е. $\exp(\mathfrak{g})$ состоит из коммутирующих друг с другом элементов. G порождается множеством $\exp(\mathfrak{g})$ (т.к. связна), следовательно, G коммутативна. ■

Замечание. Вместо $GL_n(\mathbb{K})$ и подгрупп Ли в ней можно рассматривать $GL(V)$, где V – векторное пространство над $\mathbb{K}$, $\dim V = n$ – бескоординатная точка зрения на линейные группы Ли.

Линейные представления групп Ли.

Определение. *Линейное представление* группы Ли G в векторном пространстве W – это дифференцируемый гомоморфизм $\mathcal{R}\colon\ G \longrightarrow GL(W)$.

Замечание. Вместо линейных представлений можно рассматривать произвольные дифференцируемые гомоморфизмы групп Ли $\varphi\colon G \longrightarrow H$. Но так как $G \subseteq GL(V)$ и $H \subseteq GL(W)$, то для линейных групп Ли это сводится к линейным представлениям.

Предложение 4. Пусть $\mathcal{R}\colon\ G \longrightarrow GL(W)$ – линейное представление группы Ли. Тогда $d_E\mathcal{R} = d\mathcal{R}\colon\ \mathfrak{g} \longrightarrow \mathfrak{gl}(W)$ – гомоморфизм алгебр Ли.

Доказательство.
Пусть $X, Y \in \mathfrak{g},\ X = \dot{g}(0), Y = \dot{h}(0),\ g(t), h(s) \in G,\ g(0) = h(0) = E$. Имеем:

$$d\mathcal{R}(X) = \frac{d}{dt}\bigg|_{t=0} d\mathcal{R}(g(t)),\ \ d\mathcal{R}(Y) = \frac{d}{ds}\bigg|_{s=0} d\mathcal{R}(h(s))$$

и

$$[X, Y] = \frac{\partial^2}{\partial t \partial s}\bigg|_{s=t=0} [g(t), h(s)]_{gr}$$

Так как $\mathcal{R}$ – гомоморфизм, то $\mathcal{R}\big([g(t), h(s)]_{gr}\big) = [\mathcal{R}(g(t)), \mathcal{R}(h(s))]_{gr}$. Применим к обеим частям этого равенства оператор $\frac{\partial}{\partial s}\Big|_{s=0}$:

$$d\mathcal{R}\left(\frac{\partial}{\partial s}\bigg|_{s=0} [g(t), h(s)]_{gr}\right) = \frac{\partial}{\partial s}\bigg|_{s=0} [\mathcal{R}(g(t)), \mathcal{R}(h(s))]_{gr}$$

Теперь применим оператор $\frac{\partial}{\partial t}\Big|_{t=0}$:

$$d\mathcal{R}\left(\frac{\partial^2}{\partial t \partial s}\bigg|_{s=t=0} [g(t), h(s)]_{gr}\right) = \frac{\partial^2}{\partial t \partial s}\bigg|_{s=t=0} [\mathcal{R}(g(t)), \mathcal{R}(h(s))]_{gr}$$

Получившееся равенство можно переписать в таком виде:

$$d\mathcal{R}([X, Y]) = [d\mathcal{R}(X), d\mathcal{R}(Y)],$$

что и требовалось. ■

Лекция 18. Линейные представления алгебр Ли.

Линейные представления алгебр Ли.

Определение 1. Линейное представление алгебры Ли $\mathfrak{g}$ в векторном пространстве W – это гомоморфизм алгебр Ли $\rho\colon\ \mathfrak{g} \longrightarrow \mathfrak{gl}(W)$.

Это определяет билинейную операцию

$$\mathfrak{g} \times W \longrightarrow \mathfrak{g}$$
$$(X, w) \mapsto Xw \coloneqq \rho(X)w$$

со свойством:

$$[X, Y]w = \rho([X, Y])w = [\rho(X), \rho(Y)]w = \rho(X)\rho(Y)w - \rho(Y)\rho(X)w = X(Yw) - Y(Xw)$$

Определение 2. Векторное пространство W с билинейной операцией $\mathfrak{g} \times W \longrightarrow \mathfrak{g}$, $(X, w) \mapsto Xw$, удовлетворяющей свойству $[X, Y]w = X(Yw) - Y(Xw)$, $\forall X, Y \in \mathfrak{g}$, $\forall w \in W$, называется *модулем над алгеброй Ли* $\mathfrak{g}$ ($\mathfrak{g}$-модулем).

Линейные представления алгебры Ли $\mathfrak{g} \Longleftrightarrow \mathfrak{g}$-модули.

На прошлой лекции мы доказали (см. предложение 4), что если $\mathcal{R}\colon\ G \longrightarrow GL(W)$ – линейное представление группы Ли, тогда $d_E\mathcal{R} = d\mathcal{R}\colon\ \mathfrak{g} \longrightarrow \mathfrak{gl}(W)$ – линейное представление алгебры Ли.

Присоединенное представление.

Важным примером линейного представления группы Ли является т.н. присоединенное представление. Пусть $G \subseteq GL_n(\mathbb{K})$ – линейная группа Ли. $\forall g \in G$ определен внутренний автоморфизм

$$i_g\colon\ G \nrightarrow G$$
$$x \mapsto gxg^{-1}$$

Его дифференциал в E – *присоединенный оператор*:

$$Ad(g) = d_E i_g\colon\ \mathfrak{g} \nrightarrow \mathfrak{g}$$
$$X \mapsto gXg^{-1}$$

Таким образом, возникает отображение $g \mapsto Ad(g)$ из группы G в группу невырожденных линейных операторов на касательной алгебре Ли, при этом произведению элементов группы соответствует произведение операторов, т.е. возникает линейное представление

$$Ad_G = Ad\colon\ G \longrightarrow GL(\mathfrak{g})$$
$$g \mapsto Ad(g)$$

- дифференцируемый гомоморфизм групп Ли. Ad_G – *присоединенное представление* группы Ли G.

Таким образом, с каждой группой Ли можно канонически связать линейное представление – ее представление на своей алгебре Ли. Это можно сделать и для алгебр Ли (представление уже не обязано быть на касательной алгебре).

Присоединенное представление алгебры Ли $\mathfrak{g}$:

$$ad_{\mathfrak{g}} = ad\colon\ \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$$
$$X \mapsto ad(X),$$

где

$$ad(X)\colon\ \mathfrak{g} \longrightarrow \mathfrak{g}$$
$$Y \mapsto [X, Y]$$

– *присоединенный оператор*.

Убедимся в том, что ad – гомоморфизм алгебр Ли:

$$[ad(X), ad(Y)]Z = \big[X, [Y, Z]\big] - \big[Y, [X, Z]\big] = \big[X, [Y, Z]\big] + \big[Y, [Z, X]\big] = -\big[Z, [X, Y]\big] =$$

$$= \big[[X, Y], Z\big] = ad([X, Y])Z$$

Следовательно, $ad([X, Y]) = [ad(X), ad(Y)]$. Отметим, что это рассуждение показывает, что свойство ad быть гомоморфизмом алгебр Ли равносильно тождеству Якоби (также нужно потребовать кососимметричность коммутатора).

Теперь поймем, как связаны представления Ad и ad.

Теорема 1. $d(Ad) = ad$.

Доказательство.
$\forall X \in \mathfrak{g}$: $X = \dot{g}(0)$, $g(t) \in G$, $g(0) = E$. Тогда $d(Ad)X = \frac{d}{dt}\Big|_{t=0} Ad(g(t))$. Имеем: $\forall Y \in \mathfrak{g}$:

$$d(Ad)(X)Y = \frac{d}{dt}\Big|_{t=0} \underbrace{Ad(g(t))Y}_{g(t)Yg(t)^{-1}} = XY + Y(-X) = [X, Y]$$

Следовательно, $d(Ad)(X) = ad(X)$. ■

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

Пример. Присоединенное представление группы Ли $SU_2(\mathbb{C})$ на

$$\mathfrak{su}_2(\mathbb{C}) = \left\{X = \begin{pmatrix} ix & y+iz \\ -y+iz & -ix \end{pmatrix} \mid x, y, z \in \mathbb{R}\right\}.$$

Имеем: $\forall g \in SU_2(\mathbb{C})$:

$$\begin{gathered} Ad(g)\colon \mathfrak{su}_2(\mathbb{C}) \longrightarrow \mathfrak{su}_2(\mathbb{C}) \\ X \mapsto gXg^{-1} \end{gathered}$$

сохраняет $\det X = x^2 + y^2 + z^2$ – положительно определенную вещественную квадратичную форму. Другими словами, операторы $Ad(g)$ группы Ли $SU_2(\mathbb{C})$ являются ортогональными операторами по отношению к квадратичной форме $\det X$. Таким образом:

$$Ad\colon SU_2(\mathbb{C}) \longrightarrow O(\mathfrak{su}_2(\mathbb{C}), \det) \simeq O_3(\mathbb{R})$$

Тогда

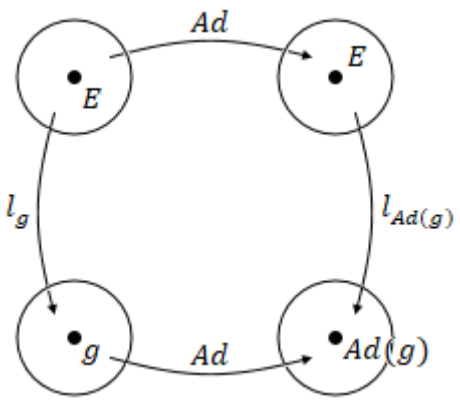
$$ad\colon \mathfrak{su}_2(\mathbb{C}) \longrightarrow \mathfrak{o}(\mathfrak{su}_2(\mathbb{C}), \det) \simeq \underbrace{\mathfrak{o}_3(\mathbb{R})}_{\text{кососим. матрицы}}$$

Так как $\dim(\mathfrak{su}_2(\mathbb{C})) = 3$, $\dim(\mathfrak{o}_3(\mathbb{R})) = 3$, возникает предположение, что данное отображение является изоморфизмом. Проверим:

$$Ker(ad) \ni X \Leftrightarrow [X, Y] = 0, \ \ \forall Y \in \mathfrak{su}_2(\mathbb{C}) \Leftrightarrow$$

$$\Leftrightarrow [X, Z] = 0, \ \ \forall Z \in \mathfrak{gl}_2(\mathbb{C}) = \underbrace{\mathfrak{su}_2(\mathbb{C})}_{\text{кососэрм. матрицы}} \oplus i\, \underbrace{\mathfrak{su}_2(\mathbb{C})}_{\text{эрмитовы матрицы}} \oplus \mathbb{C}E \Leftrightarrow X = \lambda E \in \mathfrak{su}_2(\mathbb{C}) \Leftrightarrow X = 0$$

Итак, $Ker(ad) = \{0\}$, следовательно, $ad\colon \mathfrak{su}_2(\mathbb{C}) \longrightarrow \mathfrak{o}_3(\mathbb{R})$ – изоморфизм. Тогда $Ad\colon SU_2(\mathbb{C}) \longrightarrow O_3(\mathbb{R})$ – локальный диффеоморфизм в окрестности E, а значит, и в окрестности любой точки (следует из того, что l_g – диффеоморфизм, и диаграмма, приведенная ниже, коммутативна):



Осталось заметить, что

$$SU_2(\mathbb{C}) = \left\{ g = \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \mid |a|^2 + |b|^2 = 1 \right\} \approx S^3$$

Но сфера S^3 связна, поэтому:

- $Im(Ad) \subseteq O_3(\mathbb{R})^0 = SO_3(\mathbb{R})$,
- $Ker(Ad) \ni g \Leftrightarrow gYg^{-1} = Y,\ \ \forall Y \in \mathfrak{su}_2(\mathbb{C}) \Leftrightarrow gZg^{-1} = Y,\ \ \forall Z \in \mathfrak{gl}_2(\mathbb{C}) \Leftrightarrow g = \lambda E \in SU_2(\mathbb{C}) \Leftrightarrow g = \pm E$

Окончательно получаем, что $Ad\colon SU_2(\mathbb{C}) \longrightarrow O_3(\mathbb{R}) \simeq SU_2(\mathbb{C})/\{\pm E\}$ – двулистное накрытие.

Аналогично, $Ad\colon SL_2(\mathbb{C}) \longrightarrow SO_3(\mathbb{C}) \simeq SL_2(\mathbb{C})/\{\pm E\}$ – двулистное накрытие.

Теорема 2. Пусть $\mathcal{R}\colon G \longrightarrow GL(W)$ – линейное представление группы Ли, а $d\mathcal{R}\colon \mathfrak{g} \longrightarrow \mathfrak{gl}(W)$ – линейное представление ее касательной алгебры Ли. Тогда $\forall X \in \mathfrak{g}$:

$$\mathcal{R}(\exp X) = \exp\big(d\mathcal{R}(X)\big)$$

Доказательство.
$\forall X \in \mathfrak{g}$: $X = \dot{g}(0)$, $g(t) \in G$, $g(0) = E$. Воспользуемся леммой 2 прошлой лекции: $\exp X = \lim\limits_{n\to\infty} g\left(\frac{1}{n}\right)^n$, следовательно,

$$\mathcal{R}(\exp X) = \lim_{n\to\infty} \mathcal{R}\left(g\left(\frac{1}{n}\right)\right)^n$$

Обозначим $h(t) = \mathcal{R}\big(g(t)\big) \in GL(W)$, тогда $h(0) = \mathcal{R}\big(g(0)\big) = \mathcal{R}(E) = E$, $Y = \dot{h}(0) = d\mathcal{R}(x)$ и

$$\mathcal{R}(\exp X) = \lim_{n\to\infty} \mathcal{R}\left(g\left(\frac{1}{n}\right)\right)^n = \lim_{n\to\infty} h\left(\frac{1}{n}\right)^n = \exp Y$$

■

Пример. Для $\mathcal{R} = Ad$ получаем $Ad(\exp X) = \exp\big(ad(X)\big)$. Преобразуем:

$$(\exp X)Y(\exp(-X)) = Y + [X,Y] + \frac{1}{2}\big[X,[X,Y]\big] + \cdots + \frac{1}{k!}\underbrace{\big[X,[\ldots,[X,Y]\ldots]\big]}_{k\text{ раз}} + \cdots$$

Теорема 2 обнаруживает очень важную связь между представлениями групп Ли и их касательными алгебрами. Из нее вытекает также важное следствие (оно следует из теоремы 2 и того факта, что $\exp(\mathfrak{g})$ порождает связную группу Ли G как абстрактную группу):

Следствие. Если G связно, то $\mathcal{R}$ однозначно определяется по $d\mathcal{R}$.

Предложение. Пусть $\mathcal{R}\colon G \longrightarrow GL(W)$ – линейное представление группы Ли, а $d\mathcal{R}\colon \mathfrak{g} \longrightarrow \mathfrak{gl}(W)$ – линейное представление ее касательной алгебры Ли. Тогда если подпространство $U \subseteq W$ инвариантно относительно $\mathcal{R}$, то оно инвариантно относительно $d\mathcal{R}$, а если G связно, то верно и обратное.

Доказательство.
$\Longrightarrow$:
$\forall u \in U, \forall X \in \mathfrak{g}$: $\quad X = \dot{g}(0), \quad g(t) \in G, \quad g(0) = E, \ d\mathcal{R}(X) = \frac{d}{dt}\Big|_{t=0} \mathcal{R}\big(g(t)\big)$. Тогда $d\mathcal{R}(X)u = \frac{d}{dt}\Big|_{t=0} \underbrace{\mathcal{R}\big(g(t)\big)u}_{\in U} \in U$ (если кривая целиком лежит в подпространстве, то и вектор скорости к любой точке этой кривой лежит в этом подпространстве).

$\Longleftarrow$:
Воспользуемся теоремой 2: $\forall u \in U, \forall X \in \mathfrak{g}$:

$$\mathcal{R}(\exp X)u = \exp\big(d\mathcal{R}(X)\big)\, u = \sum_{k=0}^{\infty} \frac{1}{k!} \underbrace{[d\mathcal{R}(X)]^k u}_{\in U} \in U,$$

откуда следует, что U инвариантно относительно $\mathcal{R}(\exp \mathfrak{g})$, а значит, U инвариантно относительно $\mathcal{R}(G)$ тоже, так как $\exp \mathfrak{g}$ порождает G. ■

Следствие. Линейное представление $\mathcal{R}$ связной группы Ли G приводимо / неприводимо / вполне приводимо $\Longleftrightarrow$ $d\mathcal{R}$ приводимо / неприводимо / вполне приводимо.

Доказательство.
Все эти свойства формулируются в терминах инвариантных подпространств, а они у $\mathcal{R}$ и $d\mathcal{R}$ одни и те же. ■

Лекция 19. Линейные представления компактных групп Ли.

Линейные представления компактных групп Ли.

Определение. Группа Ли $G \subseteq GL_n(\mathbb{K})$ *компактна*, если она компактна как топологическое пространство, т.е. замкнута и ограничена в $Mat_n(\mathbb{K})$.

Примеры компактных групп:

1) $O_n(\mathbb{R})$, $U_n(\mathbb{C})$:

- замкнуты в $Mat_n(\mathbb{K})$, так как задаются алгебраическими уравнениями
- ограничены в $Mat_n(\mathbb{K})$, так как удовлетворяют неравенствам $|g_{ij}| \leq 1$

2) Любая конечная группа

Теорема Машке утверждает, что если $char\ K = 0$, то любое конечномерное линейное представление группы G вполне приводимо. Наша цель – обобщить эту теорему на случай компактных групп.

Теорема 1. Любое линейное представление компактной группы Ли над $\mathbb{R}$ и $\mathbb{C}$ вполне приводимо.

Для доказательства нам понадобится некоторая предварительная подготовка, касающаяся свойств выпуклых множеств в евклидовом пространстве.

Выпуклые множества.

Пусть $M \subseteq \mathbb{R}^N$ – *выпуклое* множество (т.е. вместе с любыми двумя своими точками содержит и отрезок, их соединяющий; более общо: если $p_1, \dots, p_n \in M$, то и $\lambda_1 p_1 + \dots + \lambda_n p_n \in M$, где $\lambda_i \geq 0$, $\lambda_1 + \dots + \lambda_n = 1$ – такие линейные комбинации называются *выпуклыми*). Без ограничения общности можно считать, что $aff(M) = \mathbb{R}^N$ (иначе заменим $\mathbb{R}^N$ на $aff(M)$). Такие выпуклые множества называют еще *выпуклыми телами*.

Свойства выпуклых тел:

1) $int(M) \neq \emptyset$

Доказательство.
Можно найти набор аффинно независимых точек $p_0, \dots, p_n \in M$, тогда подмножество $\{\lambda_0 p_0 + \dots + \lambda_n p_n \in M \mid \lambda_i \geq 0, \lambda_0 + \dots + \lambda_n = 1\} \subseteq M$ будет открытым. ■

2) $M \subseteq \overline{int(M)}$.

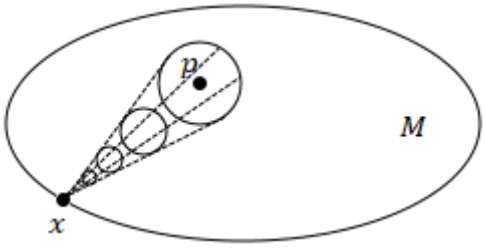


Рис. 19.1. $M \subseteq \overline{int(M)}$

Доказательство.

Пояснить это свойство легче всего с помощью рис. 19.1: если $p \in int(M)$, значит, M содержит и некоторую окрестность p. Рассмотрим произвольную граничную точку x множества M и соединим ее отрезками со всеми точками окрестности точки p. Все эти отрезки целиком будут лежать в M (поскольку M выпукло), а значит, существует последовательность окрестностей (получаемых из окрестности точки p с помощью гомотетии), лежащих все ближе к точке x, т.е. любая граничная точка сколь угодно хорошо приближается внутренними точками. Поэтому $M \subseteq \overline{int(M)}$. ■

3) M ограничено $\Longrightarrow M$ квадрируемо.

Доказательство этого свойства можно найти в курсе математического анализа, мы не будем его приводить.

Теперь мы можем определить понятие центра масс. *Центр масс* ограниченного выпуклого множества:

$$c(M) = \frac{1}{Vol(M)} \int\limits_M x\,dx = \lim_{\dim\{\Delta\}\to 0} \underbrace{\sum_i p_i \frac{Vol(\Delta_i)}{\sum_i Vol(\Delta_i)}}_{\in M} \in \overline{M}$$

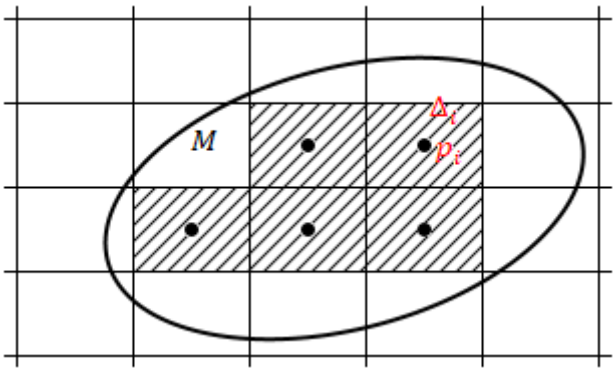


Рис. 19.2. К определению центра масс

4) Если $\varphi\colon\ \mathbb{R}^N \longrightarrow \mathbb{R}^N$ – линейное преобразование, то $\varphi\big(c(M)\big) = c\big(\varphi(M)\big)$.

Доказательство.
Так как $Vol\ \varphi(\Delta_i) = Vol(\Delta_i) \cdot \det\varphi$, то

$$\varphi\big(c(M)\big) = \lim_{\dim\{\Delta\}\to 0} \sum_i \varphi(p_i) \frac{Vol(\Delta_i)}{\sum_i Vol(\Delta_i)} = \lim_{\dim\{\Delta\}\to 0} \sum_i \varphi(p_i) \frac{Vol\ \varphi(\Delta_i)}{\sum_i Vol\ \varphi(\Delta_i)} = c\big(\varphi(M)\big)$$

■

Определим понятие выпуклой оболочки. $\forall S \subseteq \mathbb{R}^N$ *выпуклая оболочка* $conv(S)$ – это наименьшее выпуклое множество, содержащее S:

$$conv(S) = \{p = \lambda_1 p_1 + \dots + \lambda_m p_m \in S \mid p_i \in S,\ \ \lambda_i \geq 0,\ \ \lambda_1 + \dots + \lambda_n = 1\}$$

5) Если S компактно, то $conv(S)$ также компактно.

Доказательство.

- Ограниченность $conv(S)$ вытекает из ограниченности S.
- Замкнутость:

По определению, $\forall p \in conv(S)\quad \exists\, p_1, \dots, p_m \in S$: $\quad p = \lambda_1 p_1 + \dots + \lambda_m p_m, \quad \lambda_i \geq 0$, $\lambda_1 + \dots + \lambda_n = 1$. Без ограничения общности можно считать, что $m \leq N + 1$, иначе существует линейная зависимость

$$\sum_{i<m} \mu_i \overrightarrow{p_i p_m} = 0,$$

Прибавим эту линейную комбинацию, умноженную на малый параметр t к равенству $\lambda_1 p_1 + \dots + \lambda_m p_m = p$, получим

$$(\lambda_1 - t\mu_1)p_1 + \dots + (\lambda_{m-1} - t\mu_{m-1})p_{m-1} + \left(\lambda_m + t\sum_{i<m} \mu_i\right) p_m = p$$

Увеличивая t от 0 добьемся, чтобы один из коэффициентов обратился в нуль, а остальные остались неотрицательными – таким образом мы в равенстве $p = \lambda_1 p_1 + \dots + \lambda_m p_m$ уменьшим количество слагаемых. Действуя так, добьемся того, что $m \leq N + 1$.

Пусть $p \in \overline{conv(S)}$, тогда $p = \lim\limits_{k\to\infty} p(k)$, где $p(k) \in conv(S)$. Можно считать, что

$$p(k) = \sum_{i=0}^{N} \lambda_i(k) p_i(k)\,, \ \text{ где } \ p_i(k) \in S,\ \ \lambda_i(k) \geq 0,\ \ \sum_i \lambda_i(k) = 1$$

Переходя к подпоследовательностям, можно добиться, чтобы $p_i(k) \longrightarrow p_i \in S$ и

$$\lambda_i(k) \longrightarrow \lambda_i \geq 0, \quad \sum_i \lambda_i = 1$$

Тогда

$$p(k) \xrightarrow[\text{при } k\to\infty]{} \sum_{i=0}^{N} \lambda_i p_i \in conv(S),$$

т.е. $conv(S)$ замкнуто.

Итак, $conv(S)$ ограниченно, замкнуто, а значит, компактно. ■

После короткого отступления снова вернемся к группам Ли. Пусть G – компактная группа Ли, $\mathcal{R}$: $G \longrightarrow GL(W)$ – ее линейное представление над $\mathbb{R}$ или $\mathbb{C}$.

Предложение 1. На W существует *инвариантное* евклидово/эрмитово скалярное умножение, т.е. $(v \mid w) = (\mathcal{R}(g)v \mid \mathcal{R}(g)w)$, $\forall v, w \in W$, $\forall g \in G$. Другими словами, $Im\mathcal{R} \subseteq O(W)$ или $U(W)$.

Доказательство.
Обозначим S пространство билинейных / эрмитовых полуторалинейных форм на W, а $P \subset S$ – множество положительно определенных форм. Легко видеть, что S – векторное пространство над $\mathbb{R}$, а P – выпуклое подмножество S. Возникает линейное представление $G \curvearrowright S$:

$$\sigma \xrightarrow{g} (g\sigma)(v, w) = \sigma(\mathcal{R}(g^{-1})v\,, \mathcal{R}(g^{-1})w)$$

P – инвариантное подмножество. Возьмем $\sigma \in P$ и рассмотрим орбиту $G\sigma \subseteq P$. $G\sigma$ компактна (как образ компактного множества при непрерывном отображении: $G\sigma = Im(G \longrightarrow P, g \mapsto \sigma g)$), поэтому $conv(G\sigma) \subseteq P$ компактна, G-инвариантна. Тогда $\sigma_0 = c\big(conv(G\sigma)\big)$ – искомое инвариантное скалярное умножение. ■

Теперь все готово для доказательства теоремы 1. Напомним ее формулировку:

Теорема 1. Любое линейное представление компактной группы Ли над $\mathbb{R}$ и $\mathbb{C}$ вполне приводимо.

Доказательство.
Пусть $U \subseteq W$ – инвариантное подпространство, тогда $U^{\perp}$ – инвариантное дополнительное подпространство. ■

Пример. Найдем линейные представления группы Ли $G = U_1(\mathbb{C}) \simeq SO_2(\mathbb{R})$.

Эта группа состоит из элементов вида $g = e^{it}$ или матриц $g = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$. Касательная алгебра Ли: $\mathfrak{g} = i\mathbb{R}$, соответственно $\mathfrak{g} = \begin{pmatrix} 0 & -t \\ t & 0 \end{pmatrix}$.

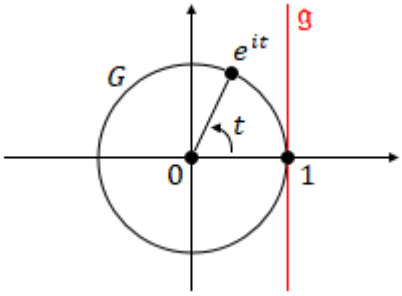


Рис. 19.3. $\mathfrak{g} = i\mathbb{R}$

Пусть $\mathcal{R}\colon G \longrightarrow GL(W)$ – комплексное линейное представление, $d\mathcal{R}\colon \mathfrak{g} \longrightarrow \mathfrak{gl}(W)$ – его дифференциал. На прошлой лекции (см. теорему 2) мы доказали формулу $\mathcal{R} \circ exp = exp \circ d\mathcal{R}$. Воспользуемся ей:

$$\mathcal{R}(g) = \mathcal{R}\left(e^{it}\right) = \exp\left(d\mathcal{R}(it)\right) = \exp(tA),$$

где $A = d\mathcal{R}(i)$.

Выберем в W инвариантное скалярное умножение, тогда $\mathcal{R}\colon G \longrightarrow U(W)$, $d\mathcal{R}\colon \mathfrak{g} \longrightarrow \mathfrak{u}(W)$, откуда следует, что A косоэрмитов, т.е. в походящем базисе его матрица имеет вид:

$$A = \begin{pmatrix} ik_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & ik_m \end{pmatrix}, \quad k_j \in \mathbb{R}$$

Имеем:

$$\mathcal{R}\left(e^{it}\right) = \exp(tA) = \begin{pmatrix} e^{ik_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e^{ik_m} \end{pmatrix} = E \text{ при } t = 2\pi, \text{ откуда } k_j \in \mathbb{Z}$$

Обратно, любой диагонализуемый линейный оператор A с собственными значениями из множества $i\mathbb{Z}$ задает линейное представление группы $U_1(\mathbb{C}) \simeq SO_2(\mathbb{R})$. В частности, неприводимые представления имеют вид:

$$\mathcal{R}_k\colon U_1(\mathbb{C}) \longrightarrow GL_1(\mathbb{C})$$
$$g = e^{it} \mapsto e^{ikt} = g^k, \quad k \in \mathbb{Z}$$

Замечание. Аналогично, линейные представления группы $G = \mathbb{R} \simeq \left\{\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{R}\right\}$ задаются произвольным линейным оператором A по формуле $\mathcal{R}(t) = \exp(tA)$.

Проиллюстрируем полученнное описание линейных представлений группы $U_1(\mathbb{C}) \simeq SO_2(\mathbb{R})$ в терминах математического анализа. Рассмотрим действие $SO_2(\mathbb{R}) \curvearrowright \mathbb{R}^2$ вращениями, тогда возникает линейное представление $SO_2(\mathbb{R})$ в алгебре многочленов $A = \mathbb{C}[x, y]$:

$$(gf)(x, y) = f\left(g^{-1}(x, y)\right)$$

Нам будет удобно представить $\mathbb{C}[x, y]$ в виде $A = \mathbb{C}[z, \bar{z}]$, $z = x + iy$. Эта бесконечномерная алгебра распадается в прямую сумму конечномерных инвариантных подпространств (однородных многочленов степени n):

$$A = \bigoplus_{n=0}^{\infty} \mathbb{C}[z, \bar{z}]_n$$

Введем на каждом из этих подпространств инвариантное эрмитово скалярное умножение:

$$(f_1 \mid f_2) = \frac{1}{2\pi} \int_{S^1} \overline{f_1(e^{it})}\, f_2\left(e^{it}\right) dt$$

Ортонормированный базис пространства $\mathbb{C}[z, \bar{z}]_n$: $\{z^k \bar{z}^l\}_{k+l=n}$. Заметим, что $\mathbb{C}z^k\bar{z}^l$ – инвариантное подпространство с представлением $\mathcal{R}_{l-k}$.

Рассмотрим алгебру многочленов на единичной окружности (т.е. ограничение $\mathbb{C}[z, \bar{z}]$ на единичную окружность): $\mathbb{C}[S^1] = A|_{S^1}$. При таком ограничении $|z| = 1$, поэтому $\bar{z} = z^{-1}$, и алгебра многочленов превращается в алгебру лорановских многочленов:

$$A|_{S^1} = \mathbb{C}[z, z^{-1}] = \mathbb{C}\left[e^{it}, e^{-it}\right] = \bigoplus_{k \in \mathbb{Z}} \mathbb{C}e^{ikt},$$

На каждом из подпространств $\mathbb{C}e^{ikt}$ реализуется представление $\mathcal{R}_{-k}$, поэтому $\forall f \in A|_{S^1}$:

$$f = \sum_{k \in \mathbb{Z}} c_k e^{ikt}$$

- многочлен Фурье.

Таким образом, с точки зрения теории представлений, на разложение Фурье (по крайней мере для многочленов) можно смотреть как на разложение линейного представления группы вращений плоскости на единичной окружности в прямую сумму одномерных представлений.

Вещественная форма.

Отметим, что теория компактных групп Ли является содержательной только для вещественных групп Ли. Комплексные группы Ли, как правило, не компактны, тем не

менее, можно связать линейное представление некоторых комплексных групп Ли с представлениями вещественных групп Ли (в том числе компактных). Это делается через представление их алгебр Ли.

Определение. Пусть G – комплексная группа Ли. Вещественная подгруппа Ли $H \subset G$ называется *вещественной формой* группы G, если:

- $\mathfrak{g} = \mathfrak{h} \underset{\mathbb{R}}{\otimes} \mathbb{C} = \mathfrak{h} \oplus i\mathfrak{h}$
- H пересекает все компоненты связности в G

Примеры вещественных форм.

1) $GL_n(\mathbb{R})$ – вещественная форма группы $GL_n(\mathbb{C})$

2) $O_n(\mathbb{R})$ – вещественная форма группы $O_n(\mathbb{C})$

Предложение 2. Пусть $\mathcal{R}\colon G \longrightarrow GL(W)$ – комплексное линейное представление комплексной группы Ли G, и $H \subset G$ – вещественная форма. Тогда у $\mathcal{R}$ и $\mathcal{R}|_H$ одни и те же инвариантные подпространства.

Доказательство.
Пусть h_i $(i \in I)$ – представители всех связных компонент H. Тогда $H = \underset{i \in I}{\sqcup} h_i H^0$, $G = \underset{i \in I}{\cup} h_i G^0$.

- Подпространство $U \subseteq W$ инвариантно относительно $\mathcal{R}(G) \Leftrightarrow$
- U инвариантно относительно $\mathcal{R}(G^0)$ и относительно всех $\mathcal{R}(h_i) \Leftrightarrow$
- U инвариантно относительно $d\mathcal{R}(\mathfrak{g})$ и относительно всех $\mathcal{R}(h_i) \Leftrightarrow$
- U инвариантно относительно $d\mathcal{R}(\mathfrak{h})$ и относительно всех $\mathcal{R}(h_i) \Leftrightarrow$
- U инвариантно относительно $\mathcal{R}(H^0)$ и относительно всех $\mathcal{R}(h_i) \Leftrightarrow$
- U инвариантно относительно $\mathcal{R}(H)$.

■

Лекция 20. Представления $SL_2(\mathbb{C})$ и $\mathfrak{sl}_2(\mathbb{C})$.

Пусть $\mathcal{R}\colon G \longrightarrow GL(W)$ – комплексное линейное представление комплексной группы Ли G, и $H \subset G$ – ее вещественная форма. На прошлой лекции (см. предложение 2) мы доказали, что у $\mathcal{R}$ и $\mathcal{R}|_H$ одни и те же инвариантные подпространства. Отсюда, например, следует, что $\mathcal{R}$ и $\mathcal{R}|_H$ приводимы / неприводимы / вполне приводимы одновременно. Это позволяет (до некоторой степени) сводить изучение теории представлений комплексной группы к ее вещественной форме, и наоборот. Особенно это полезно, если у группы G имеется компактная вещественная форма.

Унитарный трюк Г. Вейля. Если комплексная группа Ли G имеет компактную вещественную форму (такие группы называют *редуктивными*), то все комплексные линейные представления у G вполне приводимы.

Примеры редуктивных групп:

- $GL_n(\mathbb{C})$, компактная вещественная форма – $U_n(\mathbb{C})$,
- $SL_n(\mathbb{C})$, компактная вещественная форма – $SU_n(\mathbb{C})$,
- $O_n(\mathbb{C})$, компактная вещественная форма – $O_n(\mathbb{R})$.

Представления $SL_2(\mathbb{C})$ и $\mathfrak{sl}_2(\mathbb{C})$ (над $\mathbb{C}$).

Разберем подробно важный пример группы Ли $SL_2(\mathbb{C})$ и ее алгебры Ли $\mathfrak{sl}_2(\mathbb{C})$. Можно сказать, что это простейший интересный пример алгебры Ли, также представления $SL_2(\mathbb{C})$ являются отправной точкой для изучения более сложных групп и алгебр Ли и их линейных представлений.

Пусть $\mathcal{R}\colon SL_2(\mathbb{C}) \longrightarrow GL(V)$ – линейное представление над $\mathbb{C}$. Рассмотрим его дифференциал $\rho = d\mathcal{R}\colon \mathfrak{sl}_2(\mathbb{C}) \longrightarrow \mathfrak{gl}(V)$. Как было отмечено выше, $\mathcal{R}$ и ρ вполне приводимы (так как группа $SL_2(\mathbb{C})$ редуктивна), а значит, разлагаются в прямую сумму неприводимых представлений, поэтому достаточно изучить неприводимые представления. Будем делать это на языке алгебр Ли.

Стандартный базис в $\mathfrak{sl}_2(\mathbb{C})$:

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Коммутационные соотношения:

$$[X,Y] = Z, \quad [Z,X] = 2X, \quad [Z,Y] = -2Y \qquad (*)$$

Пусть $\rho\colon \mathfrak{sl}_2(\mathbb{C}) \longrightarrow \mathfrak{gl}(V)$ – линейное представление над $\mathbb{C}$. Рассмотрим линейные операторы $\mathcal{X} = \rho(X)$, $\mathcal{Y} = \rho(Y)$, $\mathcal{Z} = \rho(Z)$ в пространстве V – они удовлетворяют тем же коммутационным соотношениям $(*)$; и наоборот – если задан набор линейных операторов, удовлетворяющих условиям $(*)$, то этот набор задает линейное представление алгебры Ли $\mathfrak{sl}_2(\mathbb{C})$. Таким образом, задать линейное представление $\mathfrak{sl}_2(\mathbb{C})$ на пространстве V – это то же самое, что задать линейные операторы $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ на V, удовлетворяющие условиям $(*)$.

Лемма 1. Если $v \in V$ – собственный вектор для $\mathcal{Z}$ с собственным значением λ, тогда $\mathcal{X}v$ – собственный вектор для $\mathcal{Z}$ с собственным значением $\lambda + 2$ или $\mathcal{X}v = 0$, а $\mathcal{Y}v$ – собственный вектор для $\mathcal{Z}$ с собственным значением $\lambda - 2$ или $\mathcal{Y}v = 0$.

Доказательство.

$$\mathcal{Z}(\mathcal{X}v) = \mathcal{X}\underbrace{\mathcal{Z}v}_{\lambda v} + \underbrace{[\mathcal{Z}, \mathcal{X}]}_{2\mathcal{X}} v = (\lambda + 2)\mathcal{X}v$$

Аналогично для $\mathcal{Y}v$. ■

Следствие. $\exists v_0 \in V$, $v_0 \neq 0$, такой что $\mathcal{Z}v_0 = \lambda v_0$, $\mathcal{X}v_0 = 0$ – *старший вектор*.

Рассмотрим последовательность векторов $v_0, v_1 = \mathcal{Y}v_0, \dots, v_k = \mathcal{Y}^k v_0, \dots$

Лемма 2.

- $\mathcal{Z}v_k = (\lambda - 2k)v_k$,
- $\mathcal{Y}v_k = v_{k+1}$,
- $\mathcal{X}v_k = c_k v_{k-1}$, где $c_k = (\lambda - k + 1)k$

Доказательство.

- Равенство $\mathcal{Z}v_k = (\lambda - 2k)v_k$ следует из леммы 1.
- Равенство $\mathcal{Y}v_k = v_{k+1}$ очевидно.
- Равенство $\mathcal{X}v_k = c_k v_{k-1}$, где $c_k = (\lambda - k + 1)k$, докажем по индукции.

База индукции: $k = 1$:

$$\mathcal{X}v_1 = \mathcal{X}\mathcal{Y}v_0 = \mathcal{Y}\underbrace{\mathcal{X}v_0}_{=0} + \underbrace{[\mathcal{X}, \mathcal{Y}]}_{=\mathcal{Z}} v_0 = \lambda v_0 \Longrightarrow c_1 = \lambda$$

Шаг индукции:

$$\mathcal{X}v_k = \mathcal{X}\mathcal{Y}v_{k-1} = \mathcal{Y}\underbrace{\mathcal{X}v_{k-1}}_{=c_{k-1}v_{k-2}} + \underbrace{[\mathcal{X}, \mathcal{Y}]}_{=\mathcal{Z}} v_{k-1} = c_{k-1}v_{k-1} + (\lambda - 2k + 2)v_{k-1} =$$

$$= (c_{k-1} + \lambda - 2k + 2)v_{k-1} \Longrightarrow c_k = c_{k-1} + (\lambda - 2k + 2)$$

- получили рекуррентное соотношение на c_k. Так как $c_1 = \lambda$, получаем:

$$c_k = \sum_{j=1}^{k} \lambda - 2j + 2 = \frac{\lambda + (\lambda - 2k + 2)}{2} k = (\lambda - k + 1)k$$

■

Следствие. Ненулевые векторы v_k линейно независимы (как собственные векторы для $\mathcal{Z}$ с различными собственными значениями). Следовательно, $\exists k$: $v_k = 0$.

Лемма 3. Пусть $v_0, v_1, \dots, v_n \neq 0$, $v_{n+1} = 0$. Тогда $v_k = 0, \forall k > n$, и $\lambda = n$.

Доказательство.
Утверждение $v_k = 0, \forall k > n$ очевидно (так как $\mathcal{Y}v_k = v_{k+1}$). Докажем, что $\lambda = n$ – для этого воспользуемся формулой из леммы 2: $\mathcal{X}v_k = c_k v_{k-1}$, где $c_k = (\lambda - k + 1)k$:

$$\mathcal{X}\underbrace{v_{n+1}}_{=0} = (\lambda - n)(n+1)\underbrace{v_n}_{\neq 0} = 0$$

Из этого равенства следует, что $(\lambda - n)(n+1) = 0 \Leftrightarrow \lambda = n$. ■

Теперь мы готовы доказать основную теорему о том, как устроены неприводимые представления алгебры Ли $\mathfrak{sl}_2(\mathbb{C})$.

Теорема 1. $\forall n \geq 0$ существует единственное представление $\rho = \rho_n$ алгебры Ли $\mathfrak{sl}_2(\mathbb{C})$ размерности $n+1$. Оно реализуется в пространстве $V(n) = < v_0, v_1, \dots, v_n >$, где $\mathfrak{sl}_2(\mathbb{C})$ действует по правилам:

- $\mathcal{X}v_k = (n - k + 1)kv_{k-1}$ (при $k > 0$) или 0 (при $k = 0$)
- $\mathcal{Y}v_k = v_{k-1}$ (при $k < n$) или 0 (при $k = n$) (**)
- $\mathcal{Z}v_k = (n - 2k)v_k$

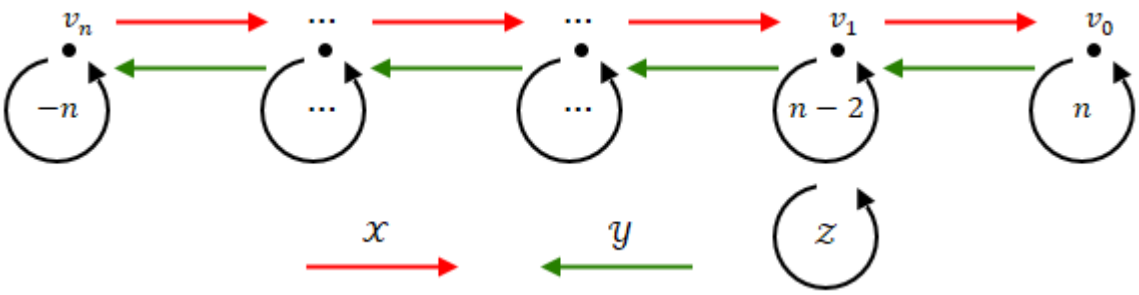


Рис. 20.1. Действие операторов $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$

Числа $n,\ n-2,\ n-4, \dots,\ -n$ называются *весами* представления ρ_n. Число n называется *старшим весом*.

Доказательство.
Пусть $\rho\colon \mathfrak{sl}_2(\mathbb{C}) \longrightarrow \mathfrak{gl}(V)$ – неприводимое представление. Из лемм 1 и 2 следует, что $< v_0, v_1, \dots, v_n >$ – инвариантное подпространство, а так как ρ неприводимо, то $< v_0, v_1, \dots, v_n > = V$, т.е. $V = V(n)$. Формулы $(**)$ выполнены по леммам 2 и 3.

Обратно, задав действия $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ в $(n+1)$-мерном пространстве $V(n)$ с базисом $v_0, v_1, \dots, v_n$ по формулам $(**)$, получим неприводимое линейное представление $\mathfrak{sl}_2(\mathbb{C})$. Коммутационные соотношения $(*)$ легко проверить прямым вычислением, а неприводимость вытекает из следующего соображения: если $U \subseteq V(n)$, $U \neq 0$ – инвариантное подпространство (в частности, для оператора $\mathcal{Z}$), то $\exists k\colon v_k \in U$, тогда $U \ni \mathcal{X}^i v_k \sim v_{k-i}$ и $U \ni \mathcal{Y}^j v_k = v_{k+j}$, следовательно, $U = V(n)$. ■

Итак, мы описали, как устроены все неприводимые представления алгебры Ли $\mathfrak{sl}_2(\mathbb{C})$. Теперь докажем, что все они являются дифференциалами некоторых неприводимых линейных представлений группы Ли $SL_2(\mathbb{C})$, которые мы сейчас предъявим.

Рассмотрим линейное представление $\mathcal{R} = \mathcal{R}_n$ группы Ли $SL_2(\mathbb{C})$ в пространстве $\mathbb{C}[x,y]_n$ однородных многочленов степени n от x, y по правилу:

$$(gf)(x,y) = f\big(g^{-1}(x,y)\big)$$

Вычислим $d\mathcal{R}$ – для этого достаточно понять, как с помощью $d\mathcal{R}$ действуют на $\mathbb{C}[x,y]_n$ базисные элементы X, Y, Z:

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Имеем:

$$\exp(tX) = \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix},\ \exp(tY) = \begin{pmatrix} 0 & 0 \\ t & 1 \end{pmatrix},\ \exp(tZ) = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix},$$

тогда

- $d\mathcal{R}(X)f = \frac{d}{dt}\Big|_{t=0} \exp(tX)\, f = \frac{d}{dt}\Big|_{t=0} f(x - ty, y) = -y\frac{\partial f}{\partial x}$

Аналогично

- $d\mathcal{R}(Y)f = \frac{d}{dt}\Big|_{t=0} f(x, y - tx) = -x\frac{\partial f}{\partial y}$
- $d\mathcal{R}(Z)f = \frac{d}{dt}\Big|_{t=0} f(e^{-t}x, e^t y) = -x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y}$

Базис:

$$v_k = (-1)^k \frac{n!}{(n-k)!} x^k y^{n-k} \quad (k = 0, \dots, n)$$

Действие X, Y, Z на $v_0, \dots, v_n$ – по формулам $(**) \Longrightarrow d\mathcal{R}_n = \rho_n$.

Следствие 1. $\forall n \geq 0$ существует единственное неприводимое комплексное линейное представление группы Ли $SL_2(\mathbb{C})$ размерности $n+1$. Оно реализуется в пространстве $\mathbb{C}[x,y]_n$ линейными заменами переменных.

Помимо представлений группы $SL_2(\mathbb{C})$, можно с помощью полученных результатов описать и линейные представления некоторых близких к ней групп.

Следствие 2. Аналогично следствию 1 для группы $SU_2(\mathbb{C})$.

В самом деле, $SU_2(\mathbb{C})$ является компактной вещественной формой группы $SL_2(\mathbb{C})$, а представления комплексной группы Ли и ее компактной вещественной формы приводимы / неприводимы / вполне приводимы одновременно. Осталось понять, что всякое линейное представление группы $SU_2(\mathbb{C})$ продолжается до линейного представления группы $SL_2(\mathbb{C})$.

Это уже совсем просто: всякое линейное представление $SU_2(\mathbb{C})$ путем перехода к дифференциалу задает линейное представление ее алгебры Ли $\mathfrak{su}_2(\mathbb{C})$, а всякое линейное представление алгебры Ли $\mathfrak{su}_2(\mathbb{C})$ по линейности продолжается до линейного представления ее комплексификации, т.е. до $\mathfrak{sl}_2(\mathbb{C})$ (так как $\mathfrak{sl}_2(\mathbb{C}) = \mathfrak{su}_2(\mathbb{C}) \oplus \mathfrak{su}_2(\mathbb{C})$), которое, в свою очередь, интегрируется до линейного представления группы $SL_2(\mathbb{C})$.

Также с группами $SL_2(\mathbb{C})$ и $SU_2(\mathbb{C})$ связана группа $SO_3(\mathbb{C})$ – рассмотрим эпиморфизмы φ:

$$\begin{array}{ccc} SL_2(\mathbb{C}) & \longrightarrow & SO_3(\mathbb{C}) \\ \cup & & \cup \\ SU_2(\mathbb{C}) & \longrightarrow & SO_3(\mathbb{R}) \end{array}$$

φ – сюръективные гомоморфизмы с ядром $Ker\ \varphi = \{\pm E\}$, поэтому всякое представление группы $SU_2(\mathbb{C})$ или $SL_2(\mathbb{C})$, которое тривиально на $Ker\ \varphi$ (т.е. на $-E$), можно спустить до представления группы $SO_3(\mathbb{C})$. И наоборот – всякое линейное представление $SO_3(\mathbb{C})$ можно поднять до представления $SL_2(\mathbb{C})$ или $SU_2(\mathbb{C})$.

Следствие 3. Неприводимые комплексные представления групп Ли $SO_3(\mathbb{C})$ и $SO_3(\mathbb{R})$ имеют вид $\bar{\mathcal{R}}_{2m}$, где $\bar{\mathcal{R}}_{2m}(\varphi(g)) = \mathcal{R}_{2m}(g)$, $\forall g \in SL_2(\mathbb{C})$, при этом $\dim \bar{\mathcal{R}}_{2m} = 2m+1$.

$\dim \bar{\mathcal{R}}_{2m}$ нечетна, так как неприводимые представления $SO_3(\mathbb{C})$ получаются из нериводимых представлений $SL_2(\mathbb{C})$, которые тривиальны на $-E$, а если $f \in \mathbb{C}[x,y]_n$, то $(-E)f = f(-x,-y) = (-1)^n f(x,y)$ – это действие тривиально тогда и только тогда, когда n четно.

Гармонический анализ на сфере.

В качестве примера применения изложенной теории, разберем задачу гармонического анализа на двумерной сфере. Рассмотрим группу $SO_3(\mathbb{R})$ – она действует в $\mathbb{R}^3$ вращениями вокруг начала координат, т.е. собственными ортогональными преобразованиями: $SO_3(\mathbb{R}) \curvearrowright \mathbb{R}^3$. При этом сфера $\mathbb{R}^3 \supset S^2 = \{x_1^2 + x_2^2 + x_3^2 = 1\}$ переходит в себя, т.е. возникает действие $SO_3(\mathbb{R})$ на двумерной сфере.

Следовательно, возникает линейное представление группы $SO_3(\mathbb{R})$ в алгебре многочленов $\mathbb{C}[x_1,x_2,x_3] = A$. Отметим, что

$$A = \bigoplus_{n=0}^{\infty} A_n$$

где A_n – инвариантное подпространство однородных многочленов степени n. Его размерность: $\dim A_n = C_{n+2}^2 = \frac{(n+2)(n+1)}{2}$. Ограничим многочлены из A на S^2 – получим линейное представление

$$SO_3(\mathbb{R}) \curvearrowright \mathbb{C}[S^2] = A|_{S^2}$$

Разложим это представление на неприводимые слагаемые. Как было показано ранее, представление группы $SO_3(\mathbb{R})$ сводится к представлению группы $SU_2(\mathbb{C})$ путем накрытия. Рассмотрим двулистное накрытие

$$Ad = \varphi\colon\ SU_2(\mathbb{C}) \longrightarrow SO_3(\mathbb{R}) \curvearrowright \mathbb{R}^3 \simeq \mathfrak{su}_2(\mathbb{C}) = \left\{ \begin{pmatrix} ix_1 & x_2 + ix_3 \\ -x_2 + ix_3 & -ix_1 \end{pmatrix} \mid x_1, x_2, x_3 \in \mathbb{R} \right\}$$

Обозначим $z = x_2 + ix_3$, тогда $-\bar{z} = -x_2 + ix_3$ и $\mathbb{C}[x_1,x_2,x_3] = \mathbb{C}[x_1, z, -\bar{z}]$. Рассмотрим в $SU_2(\mathbb{C})$ матрицу $\exp(tiZ) = \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix}$ и поймем, как действует соответствующий этой матрице элемент в группе $SO_3(\mathbb{R})$:

$$g(t) = Ad\ \exp(tiZ)\colon\ (x_1, z) \mapsto \left(x_1, e^{2ti} z\right)$$

Т.е. кривая $g(t)$ в $SO_3(\mathbb{R})$ действует поворотом в плоскости (x_2, x_3) на угол $2t$.

Лекция 21. Универсальная обертывающая алгебра.

Гармонический анализ на сфере (продолжение).

Базис в A_n: $x_1^k z^l \bar{z}^m$, $k+l+m=n$. Заметим, что каждый такой вектор является собственным вектором для $g(t)$ с собственным значением $e^{2(m-l)ti}$. Переходя к представлению алгебры Ли $\mathfrak{su}_2(\mathbb{C})$, получаем, что вес элемента $x_1^k z^l \bar{z}^m$ равен $2(m-l)$. Самый старший из весов равен $2n$, соответствующий старший вектор: $\bar{z}^n$. Следовательно, в A_n есть инвариантное подпространство $H_n \simeq V(2n)$.

Заметим, что в A_n есть еще одно инвариантное подпространство qA_{n-2}, где $q = x_1^2 + x_2^2 + x_3^2$, причем $qA_{n-2} \simeq A_{n-2}$ (так как на q группа $SO_3(\mathbb{R})$ действует тривиально). В пространстве A_{n-2} нет веса $2n$, откуда следует, что пересечение подпространств qA_{n-2} и H_n тривиально: $qA_{n-2} \cap H_n = \{0\}$.

На прошлой лекции мы вычислили $\dim A_n = C_{n+2}^2 = \frac{(n+2)(n+1)}{2}$, откуда $\dim qA_{n-2} = \dim A_{n-2} = \frac{n(n-1)}{2}$. Так как H_n – неприводимое представление со старшим весом $2n$, то $\dim H_n = 2n+1$. Сумма размерностей этих подпространств дает $\frac{(n+2)(n+1)}{2}$, т.е. $\dim A_n$, поэтому

$$A_n = qA_{n-2} \oplus H_n$$

Далее мы можем проделать те же рассуждения для A_{n-2}, A_{n-4}, и т.д. В итоге получим:

$$A_n = H_n \oplus qH_{n-2} \oplus q^2 H_{n-4} \oplus \cdots$$

- разложение A_n в прямую сумму неприводимых подпространств.

Ограничение функций:

$$A_n \longrightarrow A_n|_{S^2}$$
$$f \mapsto f|_{S^2}$$

является изоморфизмом (легко видеть, что ядро этого отображения тривиально – если однородный многочлен равен нулю на сфере S^2, то он равен нулю и на $\mathbb{R}^3$). С другой стороны, $A_n|_{S^2} = A_{n-2}|_{S^2} \oplus \underbrace{H_n|_{S^2}}_{=U_n \simeq V(2n)}$ - применяя это разложение для $A_{n-2}|_{S^2}$, $A_{n-4}|_{S^2}$ и т.д., получим

$$A_{n-2}|_{S^2} = U_n \oplus U_{n-2} \oplus U_{n-4} \oplus \cdots$$

Тогда

$$\mathbb{C}[S^2] = \bigoplus_{n=0}^{\infty} U_n \simeq \bigoplus_{n=0}^{\infty} V(2n)$$

- изотипное разложение, следовательно, определено однозначно.

Базис в U_n: $f_{n,0}$, $f_{n,1}, \dots, f_{n,2n}$ (соответствующие веса: $2n,\ 2n-2, \dots, -2n$). Эти функции называются сферическими функциями Лапласа, они определены с точностью до пропорциональности. Один из способов их нормирования заключается в выборе инвариантного скалярного умножения на пространстве $A_n|_{S^2}$. Инвариантное эрмитово скалярное умножение:

$$(f_1 \mid f_2) = \int\limits_{S^2} \overline{f_1(x)}\, f_2(x) dx$$

Функции $f_{n,k}$ – собственные векторы для косоэрмитова оператора $\rho_{2n}(iZ)$ с разными собственными значениями $2(n-k)i$, следовательно, ортогональны друг другу при разных k.

Заметим также, что слагаемые U_k из разложения $\mathbb{C}[S^2]$ в прямую сумму тоже будут ортогональны друг другу: $U_n = (A_{n-2}|_{S^2})^{\perp} \cap A_n|_{S^2}$ – единственное инвариантное дополнение, откуда $U_n \perp U_m$ при $n < m$. В конечном счете получаем, что $\{f_{n,k}\}$ – ортогональный базис в $\mathbb{C}[S^2]$.

Мы не будем в явном виде вычислять сферические функции Лапласа, но отметим, что они широко используются в разных задачах, где играет роль сферическая симметрия (например, в математической физике, квантовой физике и т.д.).

На этом закончим изучение линейных представлений групп Ли (и части нашего курса, связанного с дифференциальной геометрией), и вернемся к более алгебраическим вопросам (которые, впрочем, касаются алгебр Ли).

Универсальная обертывающая алгебра.

Пусть A – ассоциативная алгебра. Можно ввести на A новое умножение (которое принято называть *коммутатором*): $[a,b] = ab - ba$, которое превращает A в алгебру Ли, обозначаемую $A^{(-)}$.

Пример. Пусть $A = Mat_n(K)$, тогда $A^{(-)} = \mathfrak{gl}_n(K)$.

Пусть $\mathfrak{g}$ – алгебра Ли над полем K. Возникает вопрос – можно ли вложить ее в качестве подалгебры $\mathfrak{g} \hookrightarrow A^{(-)}$ для некоторой ассоциативной алгебры A? Для алгебр Ли линейных групп Ли ответ положительный (следует из определения), оказывается, что это верно и в общем случае.

Рассмотрим все возможные вложения и поймем, существует ли среди них универсальное (понятие универсального вложения зафиксируем в следующем определении):

Определение. Ассоциативная алгебра с единицей U называется *универсальной обертывающей алгеброй* для алгебры Ли $\mathfrak{g}$, если существует гомоморфизм $\varphi_{uni}\colon \mathfrak{g} \longrightarrow U^{(-)}$, такой что для любой ассоциативной алгебры A и любого гомоморфизма $\varphi\colon \mathfrak{g} \longrightarrow A^{(-)}$ существует единственный гомоморфизм ассоциативных алгебр $\psi\colon U \longrightarrow A$, для которого $\varphi = \psi \circ \varphi_{uni}$ (т.е. существует единственный гомоморфизм ψ, делающий следующую диаграмму коммутативной):

$$\begin{tikzcd} \mathfrak{g} \arrow[r, "\varphi_{uni}"] \arrow[d, "\varphi"'] & U \arrow[dl, dashed, "\exists!\,\psi"] \\ A & \end{tikzcd}$$

Предложение. Универсальная обертывающая алгебра для данной алгебра Ли $\mathfrak{g}$ сущестует и единственна с точностью до изоморфизма. Обозначение: $U = U(\mathfrak{g})$.

Доказательство.
Единственность. Вытекает из универсального свойства: пусть U' – другая универсальная обертывающая алгебра для $\mathfrak{g}$. Воспользуемся языком коммутативных диаграмм:

$$\begin{tikzcd} & U \arrow[loop right, dashed, "\exists!\,\varphi'\varphi = id_U"] \arrow[d, dashed, shift right, "\exists!\,\varphi"'] \\ \mathfrak{g} \arrow[ur, "\varphi_{uni}"] \arrow[dr, "\varphi'_{uni}"'] & \\ & U' \arrow[loop right, dashed, "\exists!\,\varphi\varphi' = id_{U'}"] \arrow[u, dashed, shift right, "\exists!\,\varphi'"'] \end{tikzcd}$$

Для U существует единственный гомоморфизм $\varphi\colon U \longrightarrow U'$, который делает эту диаграмму коммутативной. Аналогично, для U' существует единственный гомоморфизм $\varphi'\colon U' \longrightarrow U$, который делает эту диаграмму коммутативной.

Рассмотрим композицию $\varphi' \circ \varphi\colon U \longrightarrow U$. Имеем: $\varphi' \circ \varphi \circ \varphi_{uni} = \varphi' \circ \varphi'_{uni} = \varphi_{uni}$, откуда следует, что $\varphi' \circ \varphi = id_U$. Аналогично получаем, что $\varphi \circ \varphi' = id_{U'}$. Отсюда следует, что φ и φ' - два взаимно обратных друг другу изоморфизма, т.е. $U \simeq U'$.

Существование. Рассмотрим тензорную алгебру $T(\mathfrak{g}) = K \oplus \mathfrak{g} \oplus (\mathfrak{g} \otimes \mathfrak{g}) \oplus \cdots$ (внешнюю прямую сумму всех тензорных степеней пространства $\mathfrak{g}$). Ее легко превратить в ассоциативную алгебру (в качестве умножения выступает тензорное умножение $\otimes$).

Имеется вложение $\mathfrak{g} \hookrightarrow T(\mathfrak{g})$ (в качестве второго слагаемого в приведенной выше прямой сумме). Предположим, существует гомоморфизм $\varphi\colon \mathfrak{g} \longrightarrow A$, где A – некоторая ассоциативная алгебра. Тогда существует единственный гомоморфизм ассоциативных алгебр $\tau\colon T(\mathfrak{g}) \longrightarrow A$, который делает следующую диаграмму коммутативной:

$$\begin{tikzcd}
\mathfrak{g} \arrow[r, hook] \arrow[d, "\varphi"'] & T(\mathfrak{g}) \arrow[dl, dashed, "\exists!\,\tau"] \\
A &
\end{tikzcd}$$

Легко понять, как τ должен быть устроен: $\forall v_1, \dots, v_m \in \mathfrak{g}$:

$$\tau(v_1 \otimes \cdots \otimes v_m) = \varphi(v_1) \cdots \varphi(v_m)$$

Т.е. мы сумели пропустить гомоморфизм $\varphi\colon \mathfrak{g} \longrightarrow A$ через гомоморфизм $\tau\colon T(\mathfrak{g}) \longrightarrow A$. Воспользуемся тем, что $\mathfrak{g}$ – алгебра Ли и φ – гомоморфизм алгебр Ли, т.е. выполнено $\varphi([v,w]) = \varphi(v)\varphi(w) - \varphi(w)\varphi(v)$, $\forall v, w \in \mathfrak{g}$. Так как приведенная выше диаграмма коммутативна, то $\varphi([v,w]) = \tau([v,w])$, а так как τ – гомоморфизм ассоциативных алгебр, то $\varphi(v)\varphi(w) - \varphi(w)\varphi(v) = \tau(v \otimes w - w \otimes v)$. Получаем

$$v \otimes w - w \otimes v - [v,w] \in Ker\,\tau$$

Рассмотрим $T(\mathfrak{g}) \rhd I$ – двусторонний идеал, порожденный всеми элементами вида $v \otimes w - w \otimes v - [v,w]$, где $v, w \in \mathfrak{g}$. Тогда $Ker\,\tau \supseteq I$, откуда следует, что существует единственный гомоморфизм $\psi\colon T(\mathfrak{g})/I \longrightarrow A$, такой что $\tau = \psi \circ \pi$ (π – каноническая проекция).

$$\begin{tikzcd}
 & T(\mathfrak{g})/I \arrow[d, dashed, "\exists!\,\psi"'] & \\
\mathfrak{g} \arrow[r, hook] \arrow[dr, "\varphi"'] & T(\mathfrak{g}) \arrow[ul, "\pi"'] \arrow[dl, dashed, "\exists!\,\tau"] & \\
 & A &
\end{tikzcd}$$

Отсюда ясно, что в качестве универсальной обертывающей можно взять алгебру $U(\mathfrak{g}) = T(\mathfrak{g})/I$, тогда $\varphi_{uni}(v) = \pi(v) = v + I$, $\forall v \in \mathfrak{g}$.

$$\begin{tikzcd}
 & T(\mathfrak{g})/I \arrow[dd, dashed, "\exists!\psi"] & \\
\mathfrak{g} \arrow[ur, "\varphi_{uni}"] \arrow[rr, hook] \arrow[dr, "\varphi"'] & & T(\mathfrak{g}) \arrow[ul, "\pi"'] \arrow[dl, dashed, "\exists!\tau"] \\
 & A &
\end{tikzcd}$$

■

Замечания.

- Всякое линейное представление $\rho\colon \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$ однозначно продолжается до линейного представления $\mathrm{P}\colon U(\mathfrak{g}) \longrightarrow L(V)$, такого что $\rho = \mathrm{P} \circ \varphi_{uni}$ (это частный случай универсального свойства).
  Таким образом, линейные представления алгебр Ли сводятся к универсальным представлениям их обертывающих алгебр. На языке модулей: $\mathfrak{g}$-модули $\Leftrightarrow$ $U(\mathfrak{g})$-модули. Это еще раз подчеркивает универсальную роль ассоциативных алгебр в теории представлений.

- Будет ли φ_{uni} вложением?

Обозначим для краткости $\varphi_{uni}(v) = \bar{v}$, $\forall v \in \mathfrak{g}$. Имеем следующее соотношение в $U(\mathfrak{g})$: $\bar{v}\bar{w} - \bar{w}\bar{v} = \overline{[v,w]}$. Если $\{e_1, \dots, e_n\}$ – базис в $\mathfrak{g}$, то $\bar{e_1}, \dots, \bar{e_n}$ порождают $U(\mathfrak{g})$ как ассоциативную алгебру с единицей, откуда следует, что произведения $\bar{e}_{i_1} \cdots \bar{e}_{i_m}$, где $1 \le i_1, \dots, i_m \le n$, $m \ge 0$ порождают $U(\mathfrak{g})$ как векторное пространство над K.

Теорема Пуанкаре–Бирхгофа–Витта. Произведения вида $\bar{e}_{i_1} \cdots \bar{e}_{i_m}$, где $1 \le i_1 \le \cdots \le i_m \le n$, $m \ge 0$ (*упорядоченные мономы*) образуют базис $U(\mathfrak{g})$.

В частности, $\bar{e_1}, \dots, \bar{e_n}$ линейно независимы, откуда следует, что φ_{uni} – вложение.

Лекция 22. Теорема Пуанкаре-Бирхгофа-Витта. Алгебра Клиффорда.

Теорема Пуанкаре–Бирхгофа–Витта. Произведения вида $\bar{e}_{i_1}\cdots\bar{e}_{i_m}$, где $1 \le i_1 \le \cdots \le i_m \le n$, $m \ge 0$ (*упорядоченные мономы*) образуют базис $U(\mathfrak{g})$.

Доказательство.
1) Поймем, что упорядоченные мономы порождают $U(\mathfrak{g})$ как векторное пространство. Как мы показали на прошлой лекции, $U(\mathfrak{g}) \simeq T(\mathfrak{g})/I$, поэтому $U(\mathfrak{g})$ порождена как векторное пространство всевозможными произведениями $\bar{e}_{j_1}\cdots\bar{e}_{j_m}$, где $1 \le j_1, \dots, j_m \le n$, $m \ge 0$. Выразим все такие произведения в виде линейной комбинации упорядоченных мономов, используя для этого двойную индукцию по m и по числу инверсий в последовательности $(j_1, \dots, j_m)$.

Пусть $j_k > j_{k+1}$. Рассмотрим произведение $\bar{e}_{j_1}\cdots\bar{e}_{j_k}\bar{e}_{j_{k+1}}\cdots\bar{e}_{j_m}$ и переставим $\bar{e}_{j_k}$ и $\bar{e}_{j_{k+1}}$ местами. Так как $\bar{e}_{j_k}\bar{e}_{j_{k+1}} = \bar{e}_{j_{k+1}}\bar{e}_{j_k} + \overline{[\bar{e}_{j_k}, \bar{e}_{j_{k+1}}]}$, то

$$\bar{e}_{j_1}\cdots\bar{e}_{j_k}\bar{e}_{j_{k+1}}\cdots\bar{e}_{j_m} = \underbrace{\bar{e}_{j_1}\cdots\bar{e}_{j_{k+1}}\bar{e}_{j_k}\cdots\bar{e}_{j_m}}_{\text{число инверсий на 1 меньше}} + \underbrace{\bar{e}_{j_1}\cdots\bar{e}_{j_{k-1}}\overline{[\bar{e}_{j_k}, \bar{e}_{j_{k+1}}]}\bar{e}_{j_{k+2}}\cdots\bar{e}_{j_m}}_{\text{степень } m-1}$$

- каждое слагаемое можно выразить через упорядоченные мономы по предположению индукции.

2) Докажем, что упорядоченные мономы линейно независимы. Предположим, что их линейная независимость уже доказана (т.е. мы уже доказали, что они образуют базис в $U(\mathfrak{g})$). Обозначим для краткости $\bar{e}_{i_1}\cdots\bar{e}_{i_m} = e_{i_1\dots i_m}$ $(1 \le i_1 \le \cdots \le i_m \le n)$. Рассмотрим $U(\mathfrak{g})$ как левый регулярный $U(\mathfrak{g})$-модуль – отсюда, в частности, следует, что это $\mathfrak{g}$-модуль. Запишем структуру $\mathfrak{g}$-модуля на $U(\mathfrak{g})$ в базисах:

- при $i \le i_1$: $e_i e_{i_1\dots i_m} = e_i e_{i_1\dots i_m} = e_{i i_1\dots i_m}$
- при $i > i_1$: $e_i e_{i_1\dots i_m} = e_i(e_{i_1} e_{i_2\dots i_m}) = e_{i_1}(e_i e_{i_2\dots i_m}) + [e_i, e_{i_1}]e_{i_2\dots i_m} = \cdots = e_{i_1\dots i_{\le}\dots i_{\le}\dots i_{\le}\dots i_{\le}m}$
  $+$ члены меньших степеней

Теперь, для того, чтобы доказать линейную независимость упорядоченных мономов, попоробуем сымитировать эту конструкцию, т.е. построим представление алгебры Ли $\mathfrak{g}$, базис в котором пронумерован так же, и на котором алгебра Ли $\mathfrak{g}$ действует по похожим формулам.

Пусть V – векторное пространство над K с базисом $v_{i_1 \dots i_m}$, где $1 \le i_1 \le \dots \le i_m \le n$, $m \ge 0$. Введем на V структуру $\mathfrak{g}$-модуля так, чтобы:

$$e_i v_{i_1 \dots i_m} = \underset{\le \le \le \le}{v_{i_1 \dots i \dots i_m}} + \text{члены меньших степеней}$$

Определим это действие индукцией по m.

<u>База индукции</u>: $m = 0$: $e_i v_\emptyset = v_i$.

<u>Шаг индукции</u>:

- при $i \le i_1$: $e_i v_{i_1 \dots i_m} = v_{i i_1 \dots i_m}$
- при $i > i_1$: $e_i v_{i_1 \dots i_m} = \underbrace{e_{i_1} \underbrace{\left(e_i v_{i_2 \dots i_m}\right)}_{\substack{\text{уже определено} \\ \text{и равно } \underset{\le \le \le \le}{v_{i_2 \dots i \dots i_m}} \\ + \text{члены младших} \\ \text{степеней}}}}_{\text{уже определено}} + \underbrace{\left[e_i, e_{i_1}\right] v_{i_2 \dots i_m}}_{\text{уже определено}}$

Достаточно доказать, что это правило определяет на V структуру $\mathfrak{g}$-модуля: в самом деле, тогда на V есть структура $U(\mathfrak{g})$-модуля, т.е. возникает гомоморфизм φ: $U(\mathfrak{g}) \longrightarrow L(V)$, который переводит $v_{i_1 \dots i_m}$ в $\varphi\left(\bar{e}_{i_1} \cdots \bar{e}_{i_m}\right) v_\emptyset$:

$$v_{i_1 \dots i_m} = e_{i_1}\left(e_{i_2}\left(\dots\left(e_{i_m} v_\emptyset\right)\dots\right)\right) = \varphi\left(\bar{e}_{i_1}\right) \cdots \varphi\left(\bar{e}_{i_m}\right) v_\emptyset = \varphi\left(\bar{e}_{i_1} \cdots \bar{e}_{i_m}\right) v_\emptyset$$

Тогда, так как $v_{i_1 \dots i_m}$ линейно независимы, то и $\bar{e}_{i_1} \cdots \bar{e}_{i_m}$ линейно независимы.

3) Проверка соотношений для $\mathfrak{g}$-модуля:

$$e_i\left(e_j v_{k_1 \dots k_m}\right) - e_j\left(e_i v_{k_1 \dots k_m}\right) = \left[e_i, e_j\right] v_{k_1 \dots k_m}$$

Используем индукцию по m (без ограничения общности можно считать, что $i > j$):

<u>База индукции</u>: $m = 0$: $e_i\left(e_j v_\emptyset\right) - e_j\left(e_i v_\emptyset\right) = e_i v_j - e_j v_i = \left[e_i, e_j\right] v_\emptyset$ - по определению действия $\mathfrak{g}$ на V.

<u>Шаг индукции</u>: обозначим $k_1 = k$, $(k_1, \dots, k_m) = M$. В этих обозначениях левая часть тождества, которое мы хотим доказать, записывается следующим образом:

$$e_i\left(e_j v_{k,M}\right) - e_j\left(e_i v_{k,M}\right)$$

При $j \leq k$ имеем: $e_i\underbrace{(e_j v_{k,M})}_{=v_{j,k,M}} - e_j(e_i v_{k,M}) = [e_i, e_j]v_{k,M}$ по определению действия. Осталось рассмотреть случай $j > k$:

$$e_i(e_j v_{k,M}) - e_j(e_i v_{k,M}) = e_i\left(e_j(e_k v_M)\right) - e_j\left(e_i(e_k v_M)\right) =$$

$$= e_i(e_k \underbrace{(e_j v_M)}_{\substack{\text{все}\\ \text{индексы}\\ \geq k \text{ либо}\\ \text{степени}\\ <m}} + [e_j, e_k]v_M) - e_j(e_k \underbrace{(e_i v_M)}_{\substack{\text{все}\\ \text{индексы}\\ \geq k \text{ либо}\\ \text{степени}\\ <m}} + [e_i, e_k]v_M) =$$

$$= e_k\left(e_i(e_j v_M)\right) + [e_i, e_k](e_j v_M) + e_i([e_j, e_k]v_M) -$$

$$-e_k\left(e_j(e_i v_M)\right) + [e_j, e_k](e_i v_M) + e_j([e_i, e_k]v_M) =$$

$$= e_k([e_i, e_j]v_M) + \left[[e_i, e_k], e_j\right]v_M + \left[e_i, [e_j, e_k]\right]v_M =$$

$$= [e_i, e_j]\underbrace{(e_k v_M)}_{=v_{k,M}} + \underbrace{\left[e_k, [e_i, e_j]\right]v_M + \left[e_j, [e_k, e_i]\right]v_M + \left[e_i, [e_j, e_k]\right]v_M}_{=0 \text{ по тождеству Якоби}} = [e_i, e_j]v_{k,M}$$

■

Алгебра Клиффорда.

Мы познакомились с универсальными обертывающими алгебрами, которые решают задачу вложения алгебры Ли (как подалгебры) в некоторую ассоциативную алгебру. Такого рода задачи (вложения в ассоциативную алгебру) можно ставить не только для алгебр Ли, но и для других алгебраических структур.

Пусть V – векторное пространство над K, $char\ K \neq 2$, и $\beta\colon\ V \times V \longrightarrow K$ – симметрическая билинейная форма, а $q\colon\ V \times V \longrightarrow K$ – соответствующая квадратичная форма. Возникает вопрос: можно ли вложить V в ассоциативную алгебру с единицей: $V \hookrightarrow A$ так, чтобы $\forall v \in V\colon\ v \cdot v = q(v)$ в A?

Определение 1. *Алгебра Клиффорда* пространства V с симметрической билинейной (квадратичной) формой β (или q) – это ассоциативная алгебра с единицей (обозначение: $Cl(V) = Cl(V, \beta) = Cl(V, q)$), удовлетворяющая универсальному свойству: существует линейное отображение $\varphi_{uni}\colon\ V \longrightarrow Cl(V)$, такое что $\forall v \in V\colon\ \varphi_{uni}(v)\varphi_{uni}(v) = q(v)$, и для любого линейного отображения $\varphi\colon\ V \longrightarrow A$ (где A – ассоциативная алгебра с единицей) со свойством $\forall v \in V\colon\ \varphi(v)\varphi(v) = q(v)$, существует единственный

гомоморфизм алгебр $\psi\colon Cl(V) \longrightarrow A$, такой что $\varphi = \psi \circ \varphi_{uni}$ (т.е. существует единственный гомоморфизм ψ, делающий следующую диаграмму коммутативной):

$$\begin{tikzcd} V \arrow[r, "\varphi_{uni}"] \arrow[d, "\varphi"'] & Cl(V) \arrow[dl, dashed, "\exists!\,\psi"] \\ A & \end{tikzcd}$$

Предложение 1. Алгебра Клиффорда векторного пространства с симметрической билинейной / квадратичной формой существует и единственна с точностью до изоморфизма.

Доказательство.
Единственность. Вытекает из универсального свойства (рассуждения аналогичны рассуждениям из доказательства единственности универсальной обертывающей алгебры – см. лекцию 21).

Существование. Построить алгебру Клиффорда можно следующим образом:

$$Cl(V) = T(V)/I,$$

где $T(V)$ – тензорная алгебра пространства V (ее определение см. предыдущий семинар), а $I \lhd T(V)$ порожден элементами вида $v \otimes v - q(v)$, $\forall v \in V$.

Рассуждения аналогичны рассуждениям из доказательства существования универсальной обертывающей алгебры (см. лекцию 21):

$$\begin{tikzcd} & T(V)/I \arrow[dd, dashed] & \\ V \arrow[ur, "\varphi_{uni}"] \arrow[rr, hook] \arrow[dr, "\varphi"'] & & T(V) \arrow[ul, "\pi"'] \arrow[dl, dashed, "\exists!\,\tau"] \\ & A & \end{tikzcd}$$

Имеем: $\tau(v \otimes v) = \tau(v)\tau(v) = \varphi(v)\varphi(v) = q(v)$, откуда следует, что $\tau\big((v \otimes v) - q(v)\big) = 0$. Тогда $Ker\,\tau \supseteq I$, откуда следует, что существует единственный гомоморфизм $\psi\colon T(V)/I \longrightarrow A$, такой что $\tau = \psi \circ \pi$ (π – каноническая проекция).

Отсюда ясно, что в качестве алгебры Клиффорда можно взять алгебру $T(V)/I$, тогда $\varphi_{uni}(v) = \pi(v) = v + I, \forall v \in V$. ■

Изучим свойства алгебры Клиффорда – для этого нам понадобятся некоторые соотношения, которые выполнены в этой алгебре.

Соотношения в алгебре Клиффорда.

Обозначим для краткости: $\varphi_{uni}(v) = \bar{v} \in Cl(V),\ \forall v \in V$. Имеем:

- $\bar{v}^2 = q(v)$

Тогда $\forall v, w \in V$:

$$(\overline{v+w})^2 = (\bar{v} + \bar{w})^2 = \bar{v}^2 + \bar{w}^2 + \bar{v}\bar{w} + \bar{w}\bar{v}$$

С другой стороны,

$$(\overline{v+w})^2 = q(v+w) = \beta(v+w, v+w) = q(v) + q(w) + \beta(v,w) + \beta(w,v)$$

Так как $q(v) = \bar{v}^2$ и $q(w) = \bar{w}^2$, то $\beta(v,w) + \beta(w,v) = \bar{v}\bar{w} + \bar{w}\bar{v}$. Воспользуемся тем, что β – симметрическая билинейная форма, т.е. $\beta(v,w) + \beta(w,v) = 2\beta(v,w)$, тогда

- $\bar{v}\bar{w} + \bar{w}\bar{v} = 2\beta(v,w) \Leftrightarrow \bar{v}\bar{w} = -\bar{w}\bar{v} + 2\beta(v,w)$

Заметим, что определение степени элемента (как, например, в алгебре многочленов) в алгебре Клиффорда корректно задать нельзя (это видно, например, из соотношения $\bar{v}^2 = q(v)$ – квадрат элемента алгебры Клиффорда равен скаляру). Однако, можно определить понятие четности элемента.

Разложим тензорную алгебру $T(V) = K \oplus V \oplus V^{\otimes 2} \oplus \cdots \oplus V^{\otimes k} \oplus \cdots$ в прямую сумму двух подпространств:

$$T(V) = T^+(V) \oplus T^-(V),$$

где

$$T^+(V) = K \oplus V^{\otimes 2} \oplus V^{\otimes 4} \oplus \cdots \text{ - четная часть } T(V)$$
$$T^-(V) = V \oplus V^{\otimes 3} \oplus V^{\otimes 5} \oplus \cdots \text{ - нечетная часть } T(V)$$

Так как $Cl(V) = T(V)/I$, где $I \lhd T(V)$ порожден элементами вида $v \otimes v - q(v), \forall v \in V$, т.е. четными элементами (а произведение четных элементов четно, произведение четного и нечетного элементов нечетно), то

$$I = I^+ \oplus I^-$$

где

$$I^\pm = I \cap T^\pm(V)$$

Тогда и алгебра Клиффорда раскладывается в прямую сумму своих четной и нечтеной частей:

$$Cl(V) = T(V)/I = Cl^+(V) \oplus Cl^-(V),$$

где

$$Cl^\pm = T^\pm(V)/I^\pm$$

Это разбиение удовлетворяет свойствам, которые мы формализуем в виде следующего определения:

Определение 2. Алгебра A *градуирована* $mod\ 2$, если $A = A^+ \oplus A^-$ так, что выполняются следующие свойства:

- $A^+A^+ \subseteq A^+$
- $A^+A^- \subseteq A^-$
- $A^-A^+ \subseteq A^-$
- $A^-A^- \subseteq A^+$

Четность:

$$|a| = \begin{cases} \bar{0} \in \mathbb{Z}/2\mathbb{Z}, & a \in A^+ \\ \bar{1} \in \mathbb{Z}/2\mathbb{Z}, & a \in A^- \end{cases}$$

$$|ab| = |a| + |b|, \forall a, b \in A^\pm$$

Градуированные $mod\ 2$ алгебры также называют *супералгебрами*. $Cl(V)$ – пример супералгебры.

Лекция 23. Свойства алгебры Клиффорда. Спинорная группа.

На прошлой лекции мы ввели понятие супералгебры. Для супералгебр есть варианты привычных нам алгебраических понятий и свойств, которые учитывают четность – мы не будем подробно на них останавливаться, так как для дальнейшего изучения алгебры Клиффорда нам понадобятся только понятия суперкоммутативности и тензорного произведения ассоциативных супералгебр. Пусть $A = A^+ \oplus A^-$ - супералгебра.

- Суперкоммутативность: элементы $a, b \in A^{\pm}$ суперкоммутируют, если

$$ab = (-1)^{|a||b|}ba$$

- Тензорное произведение ассоциативных супералгебр $A \widehat{\otimes} B$:
  $A \widehat{\otimes} B = A \otimes B$ как векторное пространство, умножение определяется по правилу:

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (-1)^{|b_1||a_2|}a_1a_2 \otimes b_1b_2$$

$A \widehat{\otimes} B$ – супералгебра, четность: $|a \otimes b| = |a| + |b|$. В $A \widehat{\otimes} B$ есть две естественные подалгебры: $A \otimes 1$ и $1 \otimes B$, которые суперкоммутируют.

Предложение 1. Пусть $V = V_1 \oplus V_2$, где $V_1 \underset{\beta}{\perp} V_2$ (т.е. V_1 и V_2 ортогональны относительно симметрической билинейной формы β: $V \times V \longrightarrow K$). Тогда $Cl(V) = Cl(V_1) \widehat{\otimes} Cl(V_2)$.

Доказательство.
Доказательство состоит в проверке универсального свойства: пусть $\varphi: V \longrightarrow A$ – линейное отображение из V в ассоциативную алгебру A с единицей, такое что $\varphi(v)^2 = q(v)$, $\forall v \in V$. Ограничим φ на каждое из слагаемых прямой суммы $V = V_1 \oplus V_2$, получим отображения $\varphi_1: V_1 \longrightarrow A$ и $\varphi_2: V_2 \longrightarrow A$, также обладающие свойством $\varphi_i(v)^2 = q(v), \forall v \in V_i$.

По универсальному свойству алгебры Клиффорда для V_i, существует универсальное отображение $V_i \longrightarrow Cl(V_i)$ и единственный гомоморфизм $\psi_i: Cl(V_i) \longrightarrow A$, такой что $\psi_i(\bar{v}_i) = \varphi_i(v_i), \forall v_i \in V_i$

$$\begin{tikzcd}
V \arrow[rr, "\varphi"] & & A \\
\cup & & \\
V_i \arrow[uurr, "\varphi_i"] \arrow[dr] & \exists!\, \psi_i & \\
& Cl(V_i) \arrow[uur, dashed] &
\end{tikzcd}$$

С другой стороны, имеются вложения $Cl(V_i) \underset{\substack{\otimes 1 \\ \text{или} \\ 1\otimes}}{\hookrightarrow} Cl(V_1) \widehat{\otimes} Cl(V_2)$. В силу свойства универсальности тензорного произведения, существует единственное линейное отображение ψ: $Cl(V_1) \widehat{\otimes} Cl(V_2) \longrightarrow A$, которое обладает следующим свойством:

$$\psi_1(c_1)\psi_2(c_2) = \psi(c_1 \otimes c_2), \qquad \forall c_i \in Cl(V_i)$$

$$\begin{tikzcd}
V \arrow[rr, "\varphi"] & & A \\
\cup & & \\
V_i \arrow[uurr, "\varphi_i"] \arrow[dr] & & \\
& Cl(V_i) \underset{\substack{\otimes 1 \\ \text{или} \\ 1\otimes}}{\hookrightarrow} Cl(V_1) \widehat{\otimes} Cl(V_2) \arrow[uur, dashed, "\exists!\,\psi_i"] \arrow[uur, dashed, "\exists!\,\psi"'] &
\end{tikzcd}$$

Итак, имеется отображение

$$\varphi_{uni}\colon V \longrightarrow Cl(V_1) \widehat{\otimes} Cl(V_2)$$
$$\varphi_{uni}(v_1 + v_2) = \bar{v}_1 \otimes 1 + 1 \otimes \bar{v}_2$$

Заметим, что слагаемые $\bar{v}_1 \otimes 1$ и $1 \otimes \bar{v}_2$ являются нечетными элементами в алгебрах Клиффорда $Cl(V_1)$ и $Cl(V_2)$ соответственно, т.е. они антикоммутируют, тогда

$$\varphi_{uni}(v_1 + v_2)^2 = \bar{v}_1^2 \otimes 1 + 1 \otimes \bar{v}_2^2 = q(v_1) + q(v_2) = q(v_1 + v_2)$$

Осталось убедиться, что отображение ψ является гомоморфизмом алгебр. Как было показано на прошлой лекции:

$$\varphi(v_1)\varphi(v_2) + \varphi(v_2)\varphi(v_1) = 2\beta(v_1, v_2)$$

Так как $V_1 \underset{\beta}{\perp} V_2$, то $\beta(v_1, v_2) = 0$, откуда следует, что $\varphi(v_1)$ и $\varphi(v_2)$ антикоммутируют. Имеем: $\varphi(v_1) = \varphi_1(v_1) = \psi_1(\bar{v}_1)$ и $\varphi(v_2) = \varphi_2(v_2) = \psi_2(\bar{v}_2)$, откуда следует, что $\psi_1\big(Cl(v_1)\big)$ и $\psi_2\big(Cl(v_2)\big)$ суперкоммутируют $\Longrightarrow \psi$ – гомоморфизмом алгебр. ■

Предложение 1 позволяет исследовать структуру алгебр Клифорда, разбивая пространство V на более простые составляющие. Следующая теорема, которая доказывается с помощью этого предложения, является аналогом теоремы Пуанкаре-Бирхгофа-Витта для алгебр Клиффорда.

Теорема 1. Пусть $\{e_1, \dots, e_n\}$ – базис V. Тогда произведения $\bar{e}_{i_1} \cdots \bar{e}_{i_k}$, где $k \geq 0$, $1 \leq i_1 \leq \cdots \leq i_k \leq n$ образуют базис $Cl(V)$; $\dim Cl(V) = 2^n$.

Доказательство.
1) Поймем, что такие произведения порождают $Cl(V)$ как векторное пространство. Всевозможные проивзедения $\bar{e}_{j_1} \cdots \bar{e}_{j_l}$, где $1 \leq j_1, \dots, j_l \leq n$, порождают $Cl(V)$ как векторное пространство. Вспомним соотношения в $Cl(V)$:

- $\bar{e_i}^2 = q(e_i)$
- $\bar{e_i}\bar{e_j} = -\bar{e_j}\bar{e_i} + 2\beta(e_i, e_j)$

С помощью этих соотношений можно выразить $\bar{e}_{j_1} \cdots \bar{e}_{j_l}$ через $\bar{e}_{i_1} \cdots \bar{e}_{i_k}$, где $i_1 < \cdots < i_k$.

2) Докажем, что $\bar{e}_{i_1} \cdots \bar{e}_{i_k}$ линейно независимы. Пусть $\{e_1, \dots, e_n\}$ – ортогональный базис V, тогда $V = V_1 \oplus \cdots \oplus V_n$, где $V_i = Ke_i$. Воспользуемся предложением 1:

$$Cl(V) = Cl(V_1) \widehat{\otimes} \cdots \widehat{\otimes} Cl(V_n)$$

Несложно понять, что $Cl(V_i) = K[e_i]/(\bar{e_i}^2 - q(e_i))$. Имеем: $\dim Cl(V_i) = 2$, базис: $\{1, \bar{e_i}\}$, откуда следует утверждение теоремы в этом случае.

3) Если $\{e_1, \dots, e_n\}$ не является ортогональным базисом (общий случай): $\bar{e}_{i_1} \cdots \bar{e}_{i_k}$ $(1 \leq i_1, \dots, i_k \leq n)$ порождают $Cl(V)$ как векторное пространство, их количество равно $2^n = \dim Cl(V)$ (то, что $\dim Cl(V) = 2^n$, мы доказали в п.2), следовательно, $\bar{e}_{i_1} \cdots \bar{e}_{i_k}$ образуют базис $Cl(V)$. ■

Следствие. $\bar{e}_1, \dots, \bar{e}_n$ линейно независимы, откуда следует, что отображение

$$\begin{aligned} \varphi_{uni}\colon V &\longrightarrow Cl(V) \\ v &\mapsto \bar{v} \end{aligned}$$

является вложением. Поэтому далее будем отождествлять $v \in V$ с его образом $\bar{v} \in Cl(V)$ и черту писать не будем.

Пусть $V_0 = Ker\ \beta$, тогда пространство V раскладывается в прямую сумму ортогональных подпространств: $V = V_0 \oplus V_1$, и на V_1 симметрическая билинейная форма β уже не вырождена. Тогда по предложению 1, $Cl(V) = Cl(V_0) \widehat{\otimes} Cl(V_1)$.

Пусть $\{e_1, \dots, e_p\}$ – базис V_0, тогда $e_i^2 = 0$ и $e_i e_j = -e_j e_i$ при $i \neq j$, откуда следует, что $Cl(V_0) = \Lambda^0(V_0)$ (внешняя алгебра V_0). Поэтому изучение $Cl(V)$ сводится к случаю, когда β невырождена – далее будем это предполагать. Будем обозначать: $\beta(v, w) = (v \mid w)$ (скалярное умножение).

Теорема 2. Если $\dim V$ четна, то $Cl(V)$ – центральная простая алгебра. Если $\dim V$ нечетна, то $Cl^+(V)$ – центральная простая алгебра.

Доказательство.
1) Пусть $\{e_1, \dots, e_n\}$ – ортогональный базис V. Тогда:

- $e_i^2 = (e_i \mid e_i) \neq 0$
- $e_i e_j = -e_j e_i$ при $i \neq j$

e_i являются обратимыми элементами $Cl(V)$ ($e_i^{-1} = \frac{e_i}{(e_i \mid e_i)}$), поэтому можно рассмотреть операцию сопряжения с e_i:

$$Ad(e_i)\colon\ Cl(V) \nrightarrow Cl(V)$$
$$c \mapsto e_i c e_i^{-1}$$

(мотивация обозначения: если мы рассматриваем V над $\mathbb{R}$ или $\mathbb{C}$, то $Cl(V)^\times$ является группой Ли (как группа обратимых элементов ассоциативной алгебры с единицей), ее алгебра Ли – это $Cl(V)^{(-)}$, тогда этот оператор задает присоединенное представление $Cl(V)^\times$ на самой себе).

Заметим, что операторы $Ad(e_i)$ коммутируют друг с другом, и $e_{i_1} \cdots e_{i_k}$ $(i_1 < \dots < i_k)$ – собственный вектор для $Ad(e_i)$:

- с собственным значением 1, если $\begin{cases} i \in \{i_1, \dots, i_k\}, k \text{ нечетно} \\ i \notin \{i_1, \dots, i_k\}, k \text{ четно} \end{cases}$
- с собственным значением -1, если $\begin{cases} i \in \{i_1, \dots, i_k\}, k \text{ четно} \\ i \notin \{i_1, \dots, i_k\}, k \text{ нечетно} \end{cases}$.

Более того, если n четно, то все $e_{i_1} \cdots e_{i_k}$ имеют разные наборы собственных значений для $Ad(e_i), \dots, Ad(e_n)$, если же n нечетно, то некоторые собственные значения совпадают только у $e_{i_1} \cdots e_{i_k}$ и $e_{j_1} \cdots e_{j_{n-k}}$, где $\{i_1, \dots, i_k, j_1, \dots, j_{n-k}\} = \{1, \dots, n\}$. Отсюда следует, что все $e_{i_1} \cdots e_{i_k}$ с четным k имеют различные наборы собственных значений.

2) Пусть $I \lhd Cl(V)$, $I \neq \{0\}$, тогда I инвариантен относительно $Ad(e_i)$, $i = 1, \dots, n$. Следовательно,

$$I = \bigoplus_{\varepsilon_1, \dots, \varepsilon_n = \pm 1} I_{\varepsilon_1, \dots, \varepsilon_n},$$

где $I_{\varepsilon_1, \dots, \varepsilon_n}$ – подпространство, состоящее из элементов идеала I, где $Ad(e_i)$ действует умножением на ε_i (существование такого разложения I в прямую сумму следует из того, что любое коммутирующее семейство диагонализуемых операторов одновременно приводится к диагональному виду).

Пусть n четно. Тогда из пункта 1) следует, что $I_{\varepsilon_1,\dots,\varepsilon_n} = Ke_{i_1}\cdots e_{i_k}$ или $\{0\}$. Так как $I \neq \{0\}$, то $I \ni \underbrace{e_{i_1}\cdots e_{i_k}}_{\text{обратимый элемент}}$ для некоторого набора $i_1,\dots,i_k$, следовательно, $I = Cl(V)$ и алгебра $Cl(V)$ проста. Центральность $Cl(V)$ следует из того, что единственный базисный элемент с набором собственных значений $(1,\dots,1)$ – это 1, откуда $Z\big(Cl(V)\big) = K$.

3) Аналогично для нечетного n. Рассмотрим $z = e_1\cdots e_n$ – этот элемент коммутирует с e_i, $\forall i$. Пусть $I \lhd Cl^+(V)$, $I \neq \{0\}$, тогда I инвариантен относительно $Ad\ \underbrace{(e_i z)}_{\text{четный элемент}} = Ad(e_i)$, $\forall i$. Отсюда следует, что

$$I = \bigoplus_{\varepsilon_1,\dots,\varepsilon_n=\pm 1} I_{\varepsilon_1,\dots,\varepsilon_n}$$

Тогда из пункта 1) следует, что $I_{\varepsilon_1,\dots,\varepsilon_n} = Ke_{i_1}\cdots e_{i_k}$ (k четно) или $\{0\}$. Так как $I \neq \{0\}$, то $I \ni \underbrace{e_{i_1}\cdots e_{i_k}}_{\text{обратимый элемент}}$ для некоторого набора $i_1,\dots,i_k$, следовательно, $I = Cl^+(V)$. Центральность $Cl^+(V)$ следует из того, что единственный четный базисный элемент с набором собственных значений $(1,\dots,1)$ – это 1, откуда $Z\big(Cl^+(V)\big) = K$. ■

Пространство спиноров.

Далее для простоты считаем, что $K = \mathbb{C}$. Обозначим $\dim V = n = 2m$ или $2m+1$. Из теоремы 2 следует, что либо $Cl(V)$ (если $n = 2m$), либо $Cl^+(V)$ (если $n = 2m+1$) изоморфна $Mat_N(\mathbb{C})$. Посмотрим на размерности:

- $\dim Mat_N(\mathbb{C}) = N^2$
- $\dim Cl(V) = 2^n = 2^{2m}$
- $\dim Cl^+(V) = 2^{n-1} = 2^{2m}$

Получаем $N^2 = 2^{2m}$, откуда $N = 2^m$.

Теперь вспомним теорию представлений: у алгебры $Mat_N(\mathbb{C})$ имеется одно неприводимое представление размерности N (в пространстве столбцов D^n, на котором $Mat_N(\mathbb{C})$ действует умножениями слева). Получаем, что у $Cl(V)$ (если $n = 2m$), либо у $Cl^+(V)$ (если $n = 2m+1$) существует единственное неприводимое представление в пространстве S, $\dim S = N = 2^m$.

Пространство S называется *пространством спиноров* векторного пространства V. Представление $Cl(V)$ или $Cl^+(V)$ в S называется *спинорным представлением*.

Модель спинорного представления.

Пусть $\{e_1, \dots, e_n\}$ – ортонормированный базис V. Выберем новый базис в V ($i^2 = -1, j = 1, \dots, m$):

$$u_j = e_{2j-1} + ie_{2j}$$
$$u_{-j} = e_{2j-1} - ie_{2j}$$
$$u_0 = e_n \text{ при } n = 2m + 1$$

В этом новом базисе базисные векторы антикоммутируют, кроме случаев u_j и u_{-j}:

$$u_j u_{-j} = -u_{-j} u_j + 4$$
$$u_j^2 = u_{-j}^2 = 0, \;\; u_0^2 = 1$$

Пусть $n = 2m$. Рассмотрим $u = u_1 \cdots u_m$ – заметим, что $u_j u = 0, \;\; \forall j = 1, \dots, m$, откуда следует, что левый идеал $S = Cl(V)u \subset Cl(V)$ имеет базис $u_{-j_1} \cdots u_{-j_k} u \;\; (j_1 > \cdots > j_k)$. S – подмодуль в $Cl(V)$, $\dim S = 2^m$, откуда следует, что S – простой $Cl(V)$-модуль, в котором реализуется спинорное представление.

Если $n = 2m + 1$, то обозначим $u = u_1 \cdots u_m \in Cl^+(V)$ или $u = u_0 u_1 \cdots u_m \in Cl^+(V)$. Как и в четном случае, выполнено $u_j u = 0, \;\; \forall j = 1, \dots, m$, следовательно, левый идеал $S = Cl^+(V)u \subset Cl^+(V)$ имеет базис $u_{-j_1} \cdots u_{-j_k} u$ (если k четно) или $u_{-j_1} \cdots u_{-j_k} u_0 u$ (если k нечетно). Отсюда следует, что $\dim S = 2^m$, а значит, S – простой $Cl^+(V)$-модуль, в котором реализуется спинорное представление.

Отметим, что при четном n спинорное представление реализуется в пространстве $S = Cl(V)u$, которое распадается в прямую сумму своей четной и нечетной части:

$$S = S^+ \oplus S^-,$$

где $S^\pm = S \cap Cl^\pm(V)$. Оба этих подпространства инвариантны относительно $Cl^+(V)$, в них реализуются т.н. *полуспинорные представления* $Cl^+(V)$.

Лемма 1. Полуспинорные представления $Cl^+(V)$ неприводимы.

Доказательство.
$e_1^2 = 1$, откуда следует, что операция умножения на e_1 (например, справа) переводит $Cl^+(V)$ в $Cl^-(V)$, и наоборот:

$$Cl^+(V) \overset{\times e_1}{\to} Cl^-(V)$$
$$Cl^-(V) \overset{\times e_1}{\to} Cl^+(V)$$

Другими словами, умножение на e_1 осуществляет изоморфизм векторных пространств $Cl^+(V)$ и $Cl^-(V)$. По тем же самым причинам $S^+ \simeq S^-$.

Пусть $U \subseteq S^+$, $U \neq \{0\}$ – инвариантное подпространство относительно $Cl^+(V)$, тогда $U \oplus e_1 U \subseteq S$ – инвариантное подпространство относительно $Cl(V)$, а так как спинорное представление неприводимо, то $U \oplus e_1 U = S$, следовательно, $U = S^+$. ■

Спинорная группа.

Рассмотрим в группе $Cl(V)^\times \supset G = \{g \mid Ad(g)V = V\}$ подгруппу $G^+ = G \cap Cl(V)^\times$ – *четная группа Клиффорда*. Разберемся с тем, как она устроена.

Лемма 2. Если $v \in V$, $(v \mid v) \neq 0$, то $v \in G$, также $Ad(v)|_V = -R_v$, где R_v – ортогональное отражение вдоль v.

Доказательство.
Пусть $v \in V$, $v \perp w$, тогда:

- $Ad(v)\colon\ v \mapsto vvv^{-1} = v$
- $Ad(w)\colon\ w \mapsto vwv^{-1} = -wvv^{-1} = -w$

Что и означает, что $Ad(v)|_V = -R_v$. ■

Лемма 3. $Ad|_V\colon\ G \longrightarrow O(V)$.

Доказательство.
$\forall g \in G, v \in V\colon\ \ (Ad(g)v \mid Ad(g)v) = gvg^{-1} \cdot gvg^{-1} = gv^2g^{-1} = (v \mid v)$. ■

Лемма 4. $O(V)$ порождена отражениями.

Доказательство.
Докажем индукцией по $\dim V$.

База индукции. $\dim V = 1$ – верно (всякий одномерный ортогональный оператор является отражением).

Шаг индукции. Выберем $v \in V$, $(v \mid v) \neq 0$. Пусть $A \in O(V)$, $w = Av$, тогда один из векторов $v \pm w$ имеет ненулевой скалярный квадрат (иначе скалярное умножение $(\cdot \mid \cdot)$ было бы нулевым на $< v + w, v - w > = < v, w >$ - противоречие).

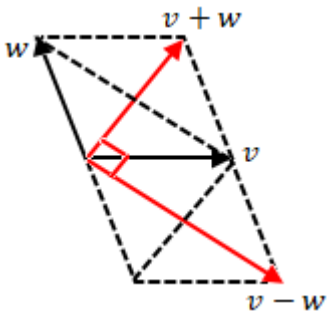


Рис. 23.1. К лемме 4

Выберем $v \pm w$ с ненулевым скалярным квадратом и рассмотрим следующие операторы:

$$R = R_{v\pm w}\colon\ v \mapsto \mp w$$
$$R' = R_w\colon -w \mapsto w$$

Тогда оператор $A' = AR^{-1}$ или $A(R'R)^{-1}$ переводит w в себя, а так как оператор A' ортогонален, то под его действием и $w^{\perp}$ переходит в себя. Но по предположению индукции, на $w^{\perp}$ оператор A' раскладывается в произведение отражений: $A' = R_1 \cdots R_k$, тогда и $A = R_1 \cdots R_k R$ или $R_1 \cdots R_k R' R$ раскладывается в проивзедение отражений. ■

Предложение 2.

- 1) $G^+ = \{\lambda v_1 \cdots v_{2k} \mid \lambda \in \mathbb{C}^\times, v_i \in V, (v_i \mid v_i) = 1\}$,
- 2) $Ad|_V\colon\ G^+ \longrightarrow SO(V)$ – сюръективный гомоморфизм,
- 3) $Ker\ (Ad|_V) = \mathbb{C}^\times$.

Доказательство.
Пусть $g \in G^+$, тогда по лемме 3: $Ad(g)|_V \in O(V)$, и по лемме 4: $Ad(g)|_V = R_{v_1} \cdots R_{v_l}$ (можно считать, что $(v_i \mid v_i) = 1$). Воспользуемся леммой 2, получим

$$Ad(g)|_V = (-1)^l Ad(v_1 \cdots v_l)$$

Если l нечетно, то $g^{-1}v_1 \cdots v_l \in Cl^-(V)$ и антикоммутирует с V – таких элементов не бывает. Следовательно, l четно, тогда

$$Ad(g)|_V = Ad(v_1 \cdots v_{2k}) = R_1 \cdots R_{2k} \in SO(V)$$

Если $Ad(g)|_V = id$, то g коммутирует с V, а значит, и с $Cl(V)$, также $g \in Cl^+(V)$. Отсюда следует, что $g \in \mathbb{C}^\times$. В частности, это означает, что $\underbrace{g^{-1}v_1 \cdots v_{2k}}_{\text{коммутирует с } V} = \mu \in \mathbb{C}^\times$, следовательно, $g = \frac{1}{\mu} v_1 \cdots v_{2k}$.

Итак, пункты 1 и 3 доказаны, осталось доказать, что $Ad|_V\colon\ G^+ \longrightarrow SO(V)$ – сюръективный гомоморфизм. Пусть $A \in SO(V)$, тогда по лемме 4, $A = R_{v_1} \cdots R_{v_{2k}}$, т.е. $A = Ad(v_1 \cdots v_{2k})|_V$, где $v_1 \cdots v_{2k} \in G^+$. ■

Спинорная норма.

Рассмотрим $Cl(V)^{op}$. Имеем: $V \hookrightarrow Cl(V)$ и $V \hookrightarrow Cl(V)^{op}$, тогда по универсальному свойству алгебры Клиффорда, существует единственный гомоморфизм $Cl(V) \longrightarrow Cl(V)^{op}$ (обозначим его $*$), который делает следующую диаграмму коммутативной:

$$\begin{tikzcd} & Cl(V) \arrow[d, dashed, "\exists!\text{гомоморфизм алгебр: } c \mapsto c^*"] \\ V \arrow[ur, hook] \arrow[r, hook] & Cl(V)^{op} \end{tikzcd}$$

Это отображение обладает следующими свойствами:

- $(c_1c_2)^* = c_2^*c_1^*$
- $v^* = v,\ \ \forall v \in V$

Теперь определим на G^+ отображение спинорной нормы. *Спинорная норма*:

$$N\colon\ G^+ \longrightarrow \mathbb{C}^\times$$
$$N(g) = gg^*$$

Проверка: если $g \in G^+$, $g = \lambda v_1 \cdots v_{2k}$, то $N(g) = gg^* = \lambda^2 v_1 \cdots v_{2k} v_{2k} \cdots v_1 = \lambda^2 \in \mathbb{C}^\times$. Более того, N – гомоморфизм:

$$N(g_1g_2) = g_1g_2(g_1g_2)^* = g_1 \underbrace{g_2g_2^*}_{N(g_2)} g_1^* = N(g_2) \underbrace{g_1g_1^*}_{N(g_1)} = N(g_1)N(g_2)$$

Теперь все готово для определения спинорной группы. *Спинорная группа*:

$$Spin(V) = KerN = \left\{g \in \left(Cl^+(V)\right)^\times \mid gVg^{-1} = V, gg^* = 1\right\}$$

Теорема 3.

- 1) $Spin(V) = \{v_1 \cdots v_{2k} \mid v_i \in V, (v_i \mid v_i) = 1\}$,
- 2) $Ad|_V\colon\ Spin(V) \longrightarrow SO(V)$ – сюръективный гомоморфизм, $Ker\ (Ad|_V) = \{\pm 1\}$ (векторное представление),
- 3) (Полу) спинорное представление группы $Spin(V)$ в пространстве S (в $S^\pm$) неприводимо в случае $\dim V = 2m + 1$ (соответственно, $\dim V = 2m$).

Доказательство.
1) Если $g \in Spin(V)$, то либо $g = v_1 \cdots v_{2k}$, либо $g = -v_1 \cdots v_{2k} = e_1 e_2 e_1 e_2 v_1 \cdots v_{2k}$.

2) Следует из предложения 2.

3) Заметим, что $Spin(V) \ni e_{i_1} \cdots e_{i_{2k}}$ – образуют базис в $Cl^+(V)$. Поэтому у $Spin(V)$ и $Cl^+(V)$ одни и те же инвариантные подпространства в S. Но ранее мы доказали утверждения, аналогичные пункту 3) для $Cl^+(V)$ – значит, они имеют место и для $Spin(V)$. ■

Замечание. Для $K = \mathbb{R}$ конструкция $Spin(V)$ для евклидова пространства V аналогична (но спинорное представление определено над $\mathbb{C}$!).

Пример. Пусть V – евклидово пространство, $\dim V = 3$.

$$Cl^+(V) = < 1,\ \ e_1 e_2,\ \ e_2 e_3,\ \ e_1 e_3 >$$

Обозначим $I = e_1 e_2$, $J = e_2 e_3$, $K = e_1 e_3$ – легко видеть, что их умножение устроено так же, как в алгебре кватернионов $\mathbb{H}$. Таким образом,

$$Cl^+(V) \simeq \mathbb{H} \subset Mat_2(\mathbb{C})$$

При этом операция $*$ на $Cl^+(V)$ совпадает с кватернионным сопряжением, а спинорная норма N равна кватернионной норме (определителю соответствующей матрицы). Также отметим, что:

- $G^+ = \mathbb{H}^\times$
- $Spin(V) = U_1(\mathbb{H}) \simeq SU_2(\mathbb{C})$
- $Ad|_V\colon\ Spin(V) \longrightarrow SO(V) = SO_3(\mathbb{R})$
- $Cl^+\left(V \underset{\mathbb{R}}{\otimes} \mathbb{C}\right) = \mathbb{H} \underset{\mathbb{R}}{\otimes} \mathbb{C} = Mat_2(\mathbb{C}) \curvearrowright \mathbb{C}^2$ – спинорное представление

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ