МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

АЛГЕБРА-4. СЕМИНАРЫ

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

Семинар 1. Вычисления в простых расширениях полей. Построение конечных полей. 6
Простое расширение поля 6
Задача. 7
Задача. 8
Задача. 8
Задача. 9
Семинар 2. Нахождение поля разложения многочлена. Круговой многочлен, его свойства. Круговое поле. 11
Разбор задач домашнего задания. 11
Задача 2 11
Задача 3a. 11
Задача 4c. 12
Задача 4b 12
Задача 5 13
Поле разложения 13
Круговое поле 14
Задача. 14
Семинар 3. Вычисление некоторых групп Галуа. 16
Разбор задач домашнего задания. 16
Задача 1b 16
Задача 6a. 16
Неприводимость над $\mathbb{Q}$ кругового многочлена 17
Задача. 17
Вычисление автоморфизмов расширений полей (групп Галуа) 17
Задача. 17
Задача. 18
Задача. 18
Общий метод вычисления групп автоморфизмов расширений полей 19
Предложение 21
Семинар 4. Вычисление группы Галуа с помощью резольвент. 22
Разбор задач домашнего задания. 22
Задача 3 22
Задача 4a. 22

Предложение ... 23
Вычисление группы Галуа с помощью резольвент ... 23
Задача ... 23
Семинар 5. Обратимые элементы и делители нуля в кольцах и алгебрах. Идеалы. ... 27
Разбор задач домашнего задания. ... 27
Задача 2c ... 27
Кольца ... 28
Задача ... 29
Идеалы в кольцах/алгебрах ... 30
Задача ... 30
Семинар 6. Идеалы в кольцах и алгебрах. Простые кольца, алгебры и модули. Алгебра Вейля. ... 32
Разбор задач домашнего задания. ... 32
Задача 2b,c ... 32
Задача 7 ... 32
Задача 6c ... 33
Идеалы в кольцах/алгебрах ... 33
Задача ... 33
Простые кольца и модули ... 34
Семинар 7. Тензорное произведение модулей, колец и алгебр. ... 36
Разбор задач домашнего задания. ... 36
Задача 4 ... 36
Задача 3 ... 36
Задача 6 ... 37
Тензорное умножение ... 38
Задача 1 ... 38
Задача 2 ... 38
Задача 3 ... 38
Задача 4 ... 38
Семинар 8. Модули гомоморфизмов. Нётеровы кольца. Евклидовы кольца. Кольцо гауссовых чисел. ... 40
Разбор задач домашнего задания. ... 40
Задача 2 ... 40
Задача 1b ... 40
Задача 1d ... 41

Модуль гомоморфизмов ... 42

Нётеровы кольца ... 43

Евклидовы кольца ... 44

Семинар 9. Пример неевклидова кольца главных идеалов. Простые элементы в кольце гауссовых чисел. ... 47

Разбор задач домашнего задания. ... 47

Задача 6. ... 47

Пример не евклидова кольца главных идеалов ... 48

Простые гауссовы числа ... 50

Семинар 10. Разложение натурального числа в сумму двух и четырех квадратов. Нормальная форма Фробениуса линейного оператора. ... 52

Разбор задач домашнего задания. ... 52

Задача 3d. ... 52

Задача 4. ... 52

Задача 1c. ... 52

Задача 5b,c ... 53

Задача 6. ... 54

Нормальная форма Фробениуса линейного оператора ... 55

Семинар 11. Классификация двумерных коммутативных ассоциативных алгебр над $\mathbb{C}$. Представления конечномерных ассоциативных алгебр. ... 58

Разбор задач домашнего задания. ... 58

Задача 2. ... 58

Классификация конечномерных ассоциативных алгебр ... 59

Одномерные ассоциативные алгебры ... 59

Двумерные коммутативные ассоциативные алгебры над $\mathbb{C}$ ... 59

Представления конечномерных ассоциативных алгебр ... 61

Семинар 12. Стандартное скалярное умножение на простом расширении поля. Тензорное произведение полупростых алгебр. ... 64

Разбор задач домашнего задания. ... 64

Задача 1. ... 64

Задача 6a,b ... 64

Задача 7. ... 65

Стандартное скалярное умножение ... 65

Задача ... 66

Простые и полупростые алгебры ... 67

Тензорное произведение полупростых алгебр 67

Семинар 13. Центральные простые алгебры и алгебры с делением. Группа Брауэра. Обобщённые кватернионы. 69

Разбор задач домашнего задания. 69

Задача 6b 69

Задача 3 69

Задача 1 70

Центральные простые алгебры и алгебры с делением 71

Утверждение 1 71

Утверждение 2 72

Группа Брауэра 73

Обобщенные алгебры кватернионов 73

Семинар 14. Свойства обобщённых кватернионных алгебр. Расширение скаляров, расщепление и степень центральной алгебры с делением. Групповые алгебры, их структура. 75

Разбор задач домашнего задания. 75

Задача 3 75

Задача 4 75

Расширение скаляров 77

Групповые алгебры 78

Семинар 15. Разложение групповой алгебры в прямую сумму простых идеалов. Группа обратимых кватернионных матриц как вещественная группа Ли. 80

Разбор задач домашнего задания. 80

Задача 4 80

Задача 6 80

Задача 7a 81

Группа обратимых кватернионных матриц как вещественная группа Ли 82

Семинар 16. Псевдоортогональная и симплектическая группы Ли. Связность групп Ли $GLn\mathbb{C}$ и $SOn\mathbb{C}$. 84

Задача 2 84

Группа обратимых кватернионных матриц как вещественная группа Ли 84

Разбор задач домашнего задания. 85

Задача 2 85

Задача 3 85

Задача 4 89

Задача ... 89

Семинар 17. Присоединённая алгебра Ли и группа Ли обратимых элементов конечномерной ассоциативной алгебры с единицей. Структура группы Ли обратимых кватернионов. ... 92

Разбор задач домашнего задания. ... 92

Задача 5b ... 92

Задача 6 ... 92

Структура группы Ли обратимых кватернионов ... 97

Задача ... 97

Семинар 18. Представления группы Ли $\mathbb{R}$. Стабилизатор вектора в линейном представлении группы Ли и группа автоморфизмов конечномерной алгебры — группы Ли, их касательные алгебры Ли. ... 98

Разбор задач домашнего задания. ... 98

Задача 5 ... 98

Задача 7c ... 98

Задача 6 ... 99

Линейное представление группы Ли $\mathbb{R}$ ... 101

При гомоморфизме групп Ли прообраз подгруппы Ли – подгруппа Ли ... 101

Семинар 19. Линейные представления группы Ли $SL2$ и алгебры Ли $\mathfrak{sl}2$: структура неприводимых представлений, характеры, формула Клебша-Гордана. ... 105

Разбор задач домашнего задания. ... 105

Задача 7a ... 105

Представления $SL2$ и $\mathfrak{sl}2$ ... 105

Формула Клебша-Гордана ... 109

Семинар 20. Вычисление сферических функций Лапласа, многочлены Лежандра. ... 111

Вычисление сферических функций Лапласа ... 112

Многочлены Лежандра ... 114

Остальные сферические функции ... 114

Семинар 21. Вычисления в алгебре Клиффорда. Алгебры Клиффорда размерностей 1 и 2. Отщепление двумерного подпространства. ... 117

Задача ... 117

Алгебры Клиффорда малых размерностей ... 117

Семинар 1. Вычисления в простых расширениях полей. Построение конечных 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.

Простое расширение поля

Начнем с того, что вспомним, как на практике работать в алгебраических расширениях полей. Так как всякое конечно порожденное алгебраическое расширение получается цепочкой последовательных простых расширений, то начнем с простых расширений.

Определение. Пусть L – поле, $K \subset L$ – подполе. Говорят, что L – *расширение* поля K. *Простое расширение*: $L = K(a \mid f(a) = 0)$, $f \in K[x]$ неприводим над K.

Как упоминалось в прошлом семестре, простое расширение поля определено единственным образом с точностью до изоморфизма: $L \cong K[x]/f \cdot K[x]$. Устроено оно следующим образом: пусть $n = \deg f$, тогда для любого $b \in L$ существует единственный $g \in K[x]$, $\deg g < n$, такой что $b = g(a)$.

Поймем, как устроены алгебраические операции в простом расширении поля. Со сложением и вычитанием проблем нет: если $b = g(a)$, $\deg g < n$ и $c = h(a)$, $\deg h < n$, то

$$b \pm c = g \pm h(a), \qquad \deg(g \pm h) < n$$

Умножение:

$$b \cdot c = g(a) \cdot h(a) = r(a), \quad \text{где} \quad g \cdot h = f \cdot q + r, \quad \deg r < n$$

Деление: пусть $c = h(a) \neq 0$. Тогда $\frac{b}{c} = b \cdot c^{-1}$. Найдем c^{-1}: из алгоритма Евклида следует, что существует единственные u, $\deg u < \deg h$ и v, $\deg v < \deg f$, такие что

$$(f, h) = 1 = u \cdot f + v \cdot h.$$

Подставим a:

$$1 = u(a) \cdot f(a) + v(a) \cdot h(a) = v(a) \cdot h(a),$$

откуда следует, что $c^{-1} = v(a)$.

Задача. Пусть $a \in \mathbb{C}$ удовлетворяет уравнению $a^3 - 3a + 1 = 0$. Избавиться от иррациональности в знаменателе дроби $\frac{a}{a+1}$.

Решение.
Несложная проверка показывает, что многочлен $f(x) = x^3 - 3x + 1 = 0$ не имеет рациональных корней. На языке простых расширений полей эту задачу можно переформулировать так: $f(x) \in \mathbb{Q}[x]$ неприводим, и элемент $\frac{a}{a+1}$ принадлежит простому расширению $\mathbb{Q}(a)$. Нужно вычислить значение выражения $\frac{a}{a+1}$ в $\mathbb{Q}(a)$.

Найдем $\frac{1}{a+1}$. Пусть $h(x) = x + 1$, тогда существуют u, $\deg u < \deg h$ и v, $\deg v < \deg f$, такие что

$$(f, h) = 1 = u \cdot f + v \cdot h$$

Найдем u и v методом неопределенных коэффициентов. Пусть $u(x) = e$, $v(x) = bx^2 + cx + d$. Получаем

$$1 = e(x^3 - 3x + 1) + (bx^2 + cx + d)(x + 1),$$

откуда

$$\begin{cases} e + b = 0 \\ b + c = 0 \\ -3e + c + d = 0 \\ e + d = 1 \end{cases}$$

Решая систему, получаем $b = -\frac{1}{3}, c = \frac{1}{3}, d = \frac{2}{3}$, т.е. $v(x) = -\frac{1}{3}x^2 + \frac{1}{3}x + \frac{2}{3}$. Следовательно,

$$\frac{1}{a+1} = v(a) = -\frac{1}{3}a^2 + \frac{1}{3}a + \frac{2}{3}$$

и

$$\frac{a}{a+1} = v(a) = \frac{1}{3}(-a^3 + a^2 + 2a) = \frac{1}{3}(-(3a-1) + a^2 + 2a) = \frac{1}{3}(a^2 - a + 1).$$

Ответ: $\frac{1}{3}(a^2 - a + 1)$. ■

Ранее мы отмечали, что всякое конечное поле является простым алгебраическим расширением простого подполя (поля из простого числа элементов): $\mathbb{F}_q = \mathbb{F}_p(a \mid f(a) = 0)$, $f \in \mathbb{F}_p[x]$ неприводим, $\deg f = n$, $q = p^n$. Покажем на примере, как с помощью расширения построить конечное поле.

Задача. Построить поле $\mathbb{F}_{16}$.

Решение.
Найдем все неприводимые многочлены $f \in \mathbb{F}_2[x]$, степени не выше 4. Для облегчения их нахождения воспользуемся следующим соображением: всякий многочлен $f \in \mathbb{F}_2[x]$ имеет вид:

$$f = x^{n_1} + x^{n_2} + \cdots + x^{n_k}, \qquad n_1 > n_2 > \cdots > n_k \geq 0,$$

поэтому $f(0) = 0 \Leftrightarrow n_k > 0$, и $f(1) = 0 \Leftrightarrow k$ четно. Поэтому многочлены, удовлетворяющие этим условиям, нас не интересуют – они приводимы. Также приводим будет многочлен степени 4, не имеющий корней, но являющийся квадратом единственного неприводимого многочлена второй степени: $x^4 + x^2 + 1 = (x^2 + x + 1)^2$

- $\deg f = 1$: x, $x + 1$
- $\deg f = 2$: $x^2 + x + 1$
- $\deg f = 3$: $x^3 + x^2 + 1$, $x^3 + x + 1$
- $\deg f = 4$: $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$

Выберем какой-нибудь неприводимый многочлен четвертой степени – например, $x^4 + x + 1$. Тогда

$$\mathbb{F}_{16} = \mathbb{F}_2(a \mid a^4 + a + 1 = 0)$$

■

Задача. Найти порождающие элементы $\mathbb{F}_{16}^{\times}$.

Решение.

Как мы знаем, мультипликативная группа поля является циклической, т.е. $\mathbb{F}_{16}^{\times} \simeq \mathbb{Z}_{15}$. Порядок любого элемента в $\mathbb{F}_{16}^{\times}$ может быть равен $1, 3, 5, 15$ – таким образом, если порядок неединичного элемента не равен 3 или 5, то это – порождающий элемент. Так как $a^3 \neq 1$ и $a^5 = a^4 \cdot a = (a+1)a = a^2 + a \neq 1$, получаем, что a – порождающий элемент, т.е. $\mathbb{F}_{16}^{\times} = < a >_{15}$. Все остальные порождающие элементы имеют вид a^n, где n не делится на 3 и 5, т.е. это:

- a^2
- $a^4 = a + 1$
- $a^7 = a^3 \cdot a^4 = a^3(a+1) = a^4 + a^3 = a^3 + a + 1$
- $a^8 = (a^4)^2 = (a+1)^2 = a^2 + 1$
- $a^{11} = a^8 \cdot a^3 = a^3(a^2+1) = a \cdot a^4 + a^3 = a(a+1) + a^3 = a^3 + a^2 + a$
- $a^{13} = a^{11} \cdot a^2 = a^2(a^3 + a^2 + 1) = a^5 + a^4 + a^3 = (a+1)^2 + a^3 = a^3 + a^2 + 1$
- $a^{14} = a^{13} \cdot a = a(a^3 + a^2 + 1) = a^4 + a^3 + a = a^3 + 1$

■

Отметим, что всякий порождающий элемент мультипликативной группы конечного поля будет примитивным элементом, но обратное, вообще говоря, неверно.

Действительно, рассмотрим элемент порядка 3 в $\mathbb{F}_{16}^{\times}$: пусть $b^3 = 1$, тогда $\mathbb{F}_2(b) = \mathbb{F}_4$. В самом деле, подполя в $\mathbb{F}_{16}$ устроены так: условие $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^m}$ равносильно тому, что $n \vdots m$. Так как $16 = 2^4$, получаем следующую цепочку вложений: $\mathbb{F}_{16} \supset \mathbb{F}_4 \supset \mathbb{F}_2$, причем поля порядка 2 и 4 единственны. Так как $\mathbb{F}_4^{\times} \simeq \mathbb{Z}_3$, то $\mathbb{F}_4^{\times} = < b >_3 = < b^{-1} >_3$, где b и b^{-1} – элементы порядка 3. Но $\mathbb{F}_{16}^{\times} \simeq \mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$, т.е. в $\mathbb{F}_{16}^{\times}$ всего два элемента порядка 3 (оба они лежат в $\mathbb{Z}_3$), стало быть, эти элементы – это b и b^{-1}, и $\mathbb{F}_2(b) = \mathbb{F}_4$.

Теперь рассмотрим элемент порядка 5 в $\mathbb{F}_{16}^{\times}$: пусть $b^5 = 1$, тогда $\mathbb{F}_2(b) = \mathbb{F}_{16}$ (действительно, $\mathbb{F}_2(b)$ – поле, но оно не изоморфно $\mathbb{F}_2$ и $\mathbb{F}_4$, значит, это $\mathbb{F}_{16}$). Таким образом, всякий элемент порядка 5 в $\mathbb{F}_{16}^{\times}$ будет примитивным элементом расширения, но не будет порождающим элементом для $\mathbb{F}_{16}^{\times}$.

Задача. Найти $\mu_a(x) \in \mathbb{Q}[x]$, где $a = \sqrt{2} + \sqrt{3}$.

Решение.
Подберем многочлен из $\mathbb{Q}[x]$, корнем которого является a:

$$a^2 = \left(\sqrt{2} + \sqrt{3}\right)^2 = 5 + 2\sqrt{6} \Longrightarrow (a^2 - 5)^2 = 24 \Leftrightarrow a^4 - 10a^2 + 1 = 0$$

Таким образом, многочлен $f(x) = x^4 - 10x^2 + 1$ – претендент на роль $\mu_a(x)$. Мы докажем, что это $\mu_a(x)$, если докажем, что $f(x)$ неприводим над $\mathbb{Q}$.

Неприводимость f: легко видеть, что f не имеет рациональных корней (переберем все дроби, числитель которых – делитель свободного члена, а знаменатель – делитель старшего коэффициента – в нашем случае достаточно проверить, что ± 1 не является корнем), также f не раскладывается в произведение неприводимых квадратных трехчленов.
Действительно, несложно найти разложение f над $\mathbb{C}$, так как несложно найти все комплексные корни f (пусть b – корень, тогда он удовлетворяет уравнению $b^2 = \left(\sqrt{2} \pm \sqrt{3}\right)^2$ – это ясно из способа подбора f, приведенного выше). Все корни f – это $b_{1,3} = \sqrt{2} \pm \sqrt{3}$ и $b_{2,4} = -\sqrt{2} \pm \sqrt{3}$. Получаем

$$f(x) = x^4 - 10x^2 + 1 = (x - b_1)(x - b_2)(x - b_3)(x - b_4)$$

Если бы f раскладывался в произведение квадратных трехчленов, неприводимых над $\mathbb{Q}$, то каждый из этих трехчленов имел бы вид $(x - b_i)(x - b_j)$. Но любой такой трехчлен не принадлежит $\mathbb{Q}[x]$.

Следовательно, $\mu_a(x) = x^4 - 10x^2 + 1$. ■

Приведем еще один способ доказательства того, что $f(x) = x^4 - 10x^2 + 1$ неприводим над $\mathbb{Q}$. Заметим, что $\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ – расширение $\mathbb{Q}$, являющееся полем разложения f. Группа автоморфизмов этого поля: $Aut\ (\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ – действительно, эта группа состоит из четырех автоморфизмов: $Aut\ (\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{id, g_1, g_2, g_3\}$, задаваемых следующим образом:

- $g_1(\sqrt{2}) = -\sqrt{2},\ g_1(\sqrt{3}) = \sqrt{3}$
- $g_2(\sqrt{2}) = \sqrt{2},\ g_2(\sqrt{3}) = -\sqrt{3}$
- $g_3(\sqrt{2}) = -\sqrt{2},\ g_3(\sqrt{3}) = -\sqrt{3}$

Следовательно, $(x) = x^4 - 10x^2 + 1$ неприводим над $\mathbb{Q}$.

Семинар 2. Нахождение поля разложения многочлена. Круговой многочлен, его свойства. Круговое поле.

Разбор задач домашнего задания.

Задача 2. Построить поле $\mathbb{F}_{27}$ как простое расширение поля $\mathbb{F}_3$ и найти в этой модели какой-нибудь порождающий элемент группы $\mathbb{F}_{27}^{\times}$ и какой-нибудь примитивный элемент, не порождающий группу $\mathbb{F}_{27}^{\times}$.

Решение.
$\mathbb{F}_{27} = \mathbb{F}_{3^3} = \mathbb{F}_3(a \mid f(a) = 0), f \in \mathbb{F}_3[x]$ неприводим, $\deg f = 3$. Для многочлена третьей степени неприводимость равносильна отсутствию корней, поэтому в качестве f можно выбрать многочлен $x^3 - x - 1$. Таким образом:

$$\mathbb{F}_{27} = \mathbb{F}_3(a \mid a^3 - a - 1 = 0)$$

Как мы знаем, мультипликативная группа поля является циклической, т.е. $\mathbb{F}_{27}^{\times} \simeq \mathbb{Z}_{26}$. Порядок любого элемента в $\mathbb{F}_{27}^{\times}$ может быть равен $1, 2, 13, 26$ – таким образом, если порядок неединичного элемента не равен 2 или 13, то это – порождающий элемент. Заметим, что a – элемент порядка 13:

$$a^{13} = (a^3)^4 \cdot a = (a+1)^4 \cdot a = (a+1)^3(a+1)a = (a^3+1)(a+1)a = \\ = (a-1)(a+1)a = (a^2-1)a = a^3 - a = 1$$

Воспользуемся тем ,что $\mathbb{F}_{27}^{\times} \simeq \mathbb{Z}_{26} = \mathbb{Z}_2 \times \mathbb{Z}_{13}$. Так как a порождает $\mathbb{Z}_{13}$, а -1 порождает $\mathbb{Z}_2$, то $\mathbb{F}_{27}^{\times} \simeq <-1>_2 \times <a>_{13}$. Следовательно, $-a$ порождает $\mathbb{F}_{27}^{\times} \simeq <-a>_{26}$. Все остальные порождающие элементы имеют вид $(-a)^n$, где n не делится на 2 и 13 – всего получаем 12 порождающих элементов.

Отметим, что заодно мы нашли примитивный элемент a, который порождает поле $\mathbb{F}_{27}$, но не является порождающим элементом группы $\mathbb{F}_{27}^{\times}$. ■

Задача 3а. Найти минимальный многочлен числа $\sqrt{2 + \sqrt[3]{3}}$ над полем $\mathbb{Q}$.

Решение.
Подберем многочлен из $\mathbb{Q}[x]$, корнем которого является $a = \sqrt{2 + \sqrt[3]{3}}$:

$$a^2 = 2 + \sqrt[3]{3} \Longrightarrow (a^2-2)^3 = 3 \Leftrightarrow (a^2-2)^3 - 3 = 0$$

Таким образом, многочлен $f(x) = (x^2-2)^3 - 3$ – претендент на роль $\mu_a(x)$.

Рассмотрим башню расширений $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{Q}(a)$. Из леммы о размерности башни расширений следует, что $(\mathbb{Q}(a):\mathbb{Q}) = (\mathbb{Q}(a):\mathbb{Q}(\sqrt[3]{3})) \cdot (\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q})$. Очевидно, что $\left(\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}\right) = 3$ (так как $\mu_{\sqrt[3]{3}}(x) = x^3 - 3$ – минимальный многочлен элемента $\sqrt[3]{3}$ над $\mathbb{Q}$ имеет степень 3). Если мы докажем, что $\left(\mathbb{Q}(a):\mathbb{Q}\left(\sqrt[3]{3}\right)\right) = 2$, то докажем, что $(\mathbb{Q}(a):\mathbb{Q}) = 6$ – это означает, что $\mu_a(x)$ имеет степень 6, т.е. $\mu_a(x) = f(x) = (x^2-2)^3 - 3$.

Доказательство того, что $\left(\mathbb{Q}(a):\mathbb{Q}\left(\sqrt[3]{3}\right)\right) = 2$, оставляется читателю. ■

Задача 4c. Найти группу автоморфизмов расширения $\mathbb{Q}(\sqrt{2+\sqrt[3]{3}}) \supset \mathbb{Q}$.

Решение.
Докажем, что $Aut\,(\mathbb{Q}(\sqrt{2+\sqrt[3]{3}})/\mathbb{Q}) = \{id, \varphi\} \simeq \mathbb{Z}_2$, где $\varphi\colon a \mapsto -a$. Действительно, $\mu_a(x) = (x^2-2)^3 - 3$ имеет только 2 вещественных корня: $a_{1,2} = \pm\sqrt{2+\sqrt[3]{3}} \in \mathbb{R}$ (так как $\mu_a(x) = (x-a_1)\cdots(x-a_6)$, где $a_k = \pm\sqrt{2+\varepsilon_j\sqrt[3]{3}}$, ε_j – корень степени 3 из единицы). Но всякий автоморфизм простого расширения примитивный элемент переводит в примитивный, т.е. если $\sigma \in Aut\,(\mathbb{Q}(\sqrt{2+\sqrt[3]{3}})/\mathbb{Q})$, то σ переставляет $a_1, \dots, a_6$, и при этом однозначно определяется тем, куда переходит $a_1 = \sqrt{2+\sqrt[3]{3}}$.

Так как $\mathbb{Q}(\sqrt{2+\sqrt[3]{3}}) \subset \mathbb{R}$, то a_1 при любом автоморфизме данного расширения должен переходить в вещественное число, т.е. в a_1 или в $a_2 = -a_1$ – всего два варианта. ■

Задача 4b. Найти группу автоморфизмов расширения $\mathbb{Q}(\sqrt{2+\sqrt{3}}) \supset \mathbb{Q}$.

Решение.
Так как $\sqrt{2+\sqrt{3}} = \frac{1+\sqrt{3}}{\sqrt{2}}$, то $\sqrt{2} \in \mathbb{Q}(\sqrt{2+\sqrt{3}})$ и $\sqrt{3} \in \mathbb{Q}(\sqrt{2+\sqrt{3}})$. Следовательно, $\mathbb{Q}(\sqrt{2+\sqrt{3}}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$. Как мы выяснили на прошлом семинаре, $\left(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\right) = 4$ и $Aut\,(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$. Найдем $\left(\mathbb{Q}\left(\sqrt{2+\sqrt{3}}\right):\mathbb{Q}\right)$.

Подберем многочлен из $\mathbb{Q}[x]$, корнем которого является $a = \sqrt{2+\sqrt{3}}$:

$$a^2 = 2+\sqrt{3} \Rightarrow (a^2-2)^2 = 3 \Leftrightarrow (a^2-2)^2 - 3 = 0$$

Так как $f(x) = (x^2-2)^2 - 3$ неприводим над $\mathbb{Q}$ (в этом несложно убедиться, так как у него нет рациональных корней, и он не раскладывается в произведение неприводимых сомножителей второй степени), то это $\mu_a(x)$, т.е. $\left(\mathbb{Q}\left(\sqrt{2+\sqrt{3}}\right):\mathbb{Q}\right) = 4$.

Таким образом, $\left(\mathbb{Q}\left(\sqrt{2+\sqrt{3}}\right):\mathbb{Q}\right) = \left(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\right) = 4$ и $\mathbb{Q}\left(\sqrt{2+\sqrt{3}}\right) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ – отсюда следует, что $\mathbb{Q}\left(\sqrt{2+\sqrt{3}}\right) = \mathbb{Q}(\sqrt{2},\sqrt{3})$, поэтому $Aut\left(\mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}\right) = Aut\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right) = V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$. ■

Задача 5. Доказать, что многочлен $f(x) = x^p - x - c$ полем K характеристики $p > 0$ либо неприводим, либо разлагается на линейные множители.

Решение.
1) Пусть x_0 – корень $f(x)$. Тогда $\{x_0 + k \mid k = 1, \dots, p-1\}$ – тоже корни. В самом деле:

$$f(x_0+k) = (x_0+k)^p - (x_0+k) - c = x_0^p + k^p - x_0 - k - c = \\ = x_0^p - x_0 - c = f(x_0) = 0$$

Получаем

$$f(x) = \prod_{k=0}^{p-1}(x - x_0 - k)$$

2) Пусть $f(x)$ не имеет корней в K, и g_1 – неприводимый множитель степени не меньше 2. Пусть a – какой-нибудь корень g_1. Присоединим его к K, т.е. рассмотрим расширение $K \subset K(a)$ – поле разложения для f (так как тогда a является также корнем f, а значит, все корни f лежат в $K(a)$ – см. пункт 1). Тогда $(K(a):K) = \deg g_1$.

Получаем, что все неприводимые множители f имеют одну и ту же степень $\deg g_1$ (так как присоединяя корень любого из них мы получаем поле разложения для f). Но тогда $\deg f = p$ должна делиться на эту степень, т.е. либо $\deg g_1 = 1$ и f имеет корни в K – противоречие, либо $\deg g_1 = p$ и f неприводим над K. ■

Поле разложения

Определение. Пусть K – поле, $f \in K[x]$, $\deg f > 0$. *Поле разложения* многочлена f над полем K – это такое расширение $K(f) \supseteq K$, для которого f разлагается на линейные множители над $K(f)$ и не существует промежуточных подполей $K(f) \supset M \supset K$ с тем же свойством. $K(f) = K(a_1, \dots, a_n)$, так что $f(x) = c(x-a_1)\cdots(x-a_n)$.

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

Пример. Пусть $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Найти $\mathbb{Q}(x^3 - 2)$.

Решение.
Используем то, что $\mathbb{Q} \subset \mathbb{C}$. В $\mathbb{C}$ $f(x)$ имеет корни $x_i = \sqrt[3]{2}\varepsilon_i$, где ε_i – корень степени 3 из единицы, т.е. $x_1 = \sqrt[3]{2}$, $x_{2,3} = \sqrt[3]{3}\left(\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right)$. Тогда $\mathbb{Q}(x^3 - 2) = \mathbb{Q}(x_1, x_2, x_3)$. Получаем следующую башню расширений:

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{Q}\left(\sqrt[3]{2}, \varepsilon_2\right) = \mathbb{Q}(x^3 - 2)$$

Воспользуемся леммой о размерности башни расширений:

- $\left(\mathbb{Q}\left(\sqrt[3]{2}\right): \mathbb{Q}\right) = 3$ (так как $\mu_{\sqrt[3]{2}}(x) = x^3 - 2$ – минимальный многочлен элемента $\sqrt[3]{2}$ над $\mathbb{Q}$ имеет степень 3)
- $\left(\mathbb{Q}\left(\sqrt[3]{2}, \varepsilon_2\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right) = 2$ (так как $\mu_{\varepsilon_2}(x) = x^2 + x + 1$ – минимальный многочлен элемента ε_2 над $\mathbb{Q}\left(\sqrt[3]{2}\right)$ имеет степень 2)

Следовательно, $(\mathbb{Q}(x^3 - 2): \mathbb{Q}) = 6$. ■

Круговое поле

Определение. Круговое поле – это поле $K_n = \mathbb{Q}(x^n - 1)$.

Данное поле называется круговым, так как корнями многочлена $x^n - 1$ являются корни степени n из 1, которые расположены на единичной окружности в комплексной плоскости в вершинах правильного n-угольника, т.е. делят единичную окружность на n равных частей.

Поймем, как устроено K_n. Несложно заметить, что $K_n = \mathbb{Q}(\varepsilon_1)$, где $\varepsilon_1 = e^{\frac{2\pi i}{n}}$. Вообще, $K_n = \mathbb{Q}(\varepsilon)$, где ε – любой первообразный корень степени n из 1.

Найдем $(K_n: \mathbb{Q})$. Для этого рассмотрим т.н. *круговой многочлен* (ε_k – первообразные корни степени n из 1):

$$\Phi_n(x) = \prod (x - \varepsilon_k),$$

Задача.

- 1) Найти $\deg \Phi_n$.
- 2) Доказать, что $\Phi_n \in \mathbb{Z}[x]$.

- 3) Доказать, что Φ_n неприводим над $\mathbb{Q}$.

Решение.
1) $\deg \Phi_n = \varphi(n)$, где φ – функция Эйлера. В самом деле, ε_k – первообразный корень степени n из единицы $\Leftrightarrow (n,k) = 1$. Всего первообразных корней $\varphi(n)$ штук.

2) Справедливо равенство:

$$x^n - 1 = \prod_{\varepsilon^n=1} (x - \varepsilon) = \prod_{m|n} \Phi_m(x)$$

- так как любой ε_k является первообразным для некоторого $m|n$.

Теперь индукцией по n докажем, что $\Phi_n(x) \in \mathbb{Z}[x]$, со старшим коэффициентом 1.

База индукции: $\Phi_1(x) = x - 1$.

Шаг индукции: из формулы, приведенной выше, следует, что

$$x^n - 1 = \Phi_n(x) \cdot \prod_{\substack{m|n, \\ m<n}} \Phi_m(x)$$

Так как каждый из $\Phi_m(x)$ по предположению индукции – целочисленный со старшим коэффициентом 1, то и $\prod_{\substack{m|n, \\ m<n}} \Phi_m(x) \in \mathbb{Z}[x]$, со старшим коэффициентом 1. Тогда и $\Phi_n(x) \in \mathbb{Z}[x]$, со старшим коэффициентом 1.

3) Указания к решению: пусть $\Phi_n = fg$, где f неприводим над $\mathbb{Q}$. Можно считать, что $f, g \in \mathbb{Z}[x]$, со старшим коэффициентом 1. Достаточно доказать, что для любого ε – примитивного корня степени n из 1 и для любого p, такого что $(p,n) = 1$ верно утверждение: если $f(\varepsilon) = 0$, то и $f(\varepsilon^p) = 0$. Это утверждение доказывается редукцией по $mod\ p$. Более подробно этот пункт мы разберем на следующем семинаре. ■

Из вышеприведенной задачи вытекает, что многочлен Φ_n является минимальным для любого первообразного корня степени n из 1. Следовательно, $(K_n: \mathbb{Q}) = \varphi(n)$.

Семинар 3. Вычисление некоторых групп Галуа.

Разбор задач домашнего задания.

Задача 1b. Найти степень поля разложения над $\mathbb{Q}$ многочлена $x^p - c$, где p – простое число, и $c \in \mathbb{Q}$ не является p-й степенью рационального числа.

Решение.
Разложим многочлен $x^p - c$ на множители над $\mathbb{C}$:

$$x^p - c = \left(x - \sqrt[p]{c}\right)\left(x - \varepsilon\sqrt[p]{c}\right)\cdots\left(x - \varepsilon^{p-1}\sqrt[p]{c}\right),$$

где ε – первообразный корень степени p из 1. Допустим, что над $\mathbb{Q}$ имеет место разложение: $x^p - c = f(x)g(x)$, где $\deg f = k,\ 1 < k < p$. Тогда модуль свободного члена f должен быть равен $\sqrt[p]{c^k} \notin \mathbb{Q}$ - противоречие.

Таким образом, $x^p - c$ неприводим над $\mathbb{Q}$, следовательно, $\mathbb{Q}(\sqrt[p]{c}, \varepsilon)$ – его поле разложения над $\mathbb{Q}$. Степень поля разложения равна $\left(\mathbb{Q}\left(\sqrt[p]{c}, \varepsilon\right): \mathbb{Q}\right) = p(p-1)$. ■

Задача 6a. Найти сумму коэффициентов кругового многочлена (ε_k – первообразные корни степени n из 1):

$$\Phi_n(x) = \prod(x - \varepsilon_k)$$

Решение.
Заметим, что сумма коэффициентов $\Phi_n(x)$ равна $\Phi_n(1)$. Если $n = p^k$, воспользуемся формулой:

$$\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right),\ \ p \text{ – простое}$$

Так как $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, то $\Phi_{p^k}(1) = \Phi_p(1) = p$.

Если $n \neq p^k$, воспользуемся формулой:

$$\Phi_n(x) = \Phi_m\left(x^{n/m}\right),\ \ m \text{ содержит все простые делители } n$$

Тогда $\Phi_n(1) = \Phi_m(1)$. Далее в качестве m можно выбрать произведение всех простых делителей, входящих в n, и воспользоваться формулой:

$$\Phi_{kp}(x) = \Phi_k(x^p)/\Phi_k(x),\ \ k \text{ не делится на } p$$

Тогда $\Phi_n(1) = \Phi_m(1) = \Phi_{kp}(1) = \Phi_k(1)/\Phi_k(1) = 1$.

Наконец, если $n = 1$, то $\Phi_n(1) = 0$. Подытожим:

сумма коэффициентов $\Phi_n(x)$ равна $\Phi_n(1) = \begin{cases} p, & \text{если } n = p^k \ (p \text{ простое}) \\ 1, & \text{если } n \neq p^k, n > 1 \\ 0, & \text{если } n = 1 \end{cases}$

■

Неприводимость над $\mathbb{Q}$ кругового многочлена

Задача. Доказать, что Φ_n неприводим над $\mathbb{Q}$.

Решение.
Разберем пункт 3 последней задачи прошлого семинара – докажем, что Φ_n неприводим над $\mathbb{Q}$. Пусть $\Phi_n = fg$, где f неприводим над $\mathbb{Q}$. Можно считать (см. лемма Гаусса), что $f, g \in \mathbb{Z}[x]$, со старшим коэффициентом 1. Достаточно доказать, что если ε – первообразный корень степени n из 1, такой что $f(\varepsilon) = 0$, тогда $f(\varepsilon^p) = 0$ для любого простого p, не делящего n (так как любой первообразный корень степени n из 1 имеет вид ε^k, где $(k, n) = 1$) – тем самым мы докажем, что $f = \Phi_n$.

Докажем от противного. Пусть $f(\varepsilon^p) \neq 0$, тогда $g(\varepsilon^p) = 0$. Следовательно, многочлен $g(x^p)$ имеет ε своим корнем, поэтому делится на $f(x)$ – минимальный многочлен ε.

Произведем редукцию коэффициентов многочленов по модулю p:

$$\overline{\Phi_n} = \bar{f}\bar{g}$$

Так как $g(x^p)$ делится на $f(x)$, и это целочисленные многочлены, то и для редуцированных многочленов это соотношение останется в силе: $\bar{g}(x^p)$ делится на $\bar{f}(x)$. Но $\bar{g}(x^p) = (\bar{g}(x))^p$, поэтому $(\bar{f}, \bar{g}) \neq 1$, откуда следует, что $\overline{\Phi_n}$ не сепарабелен. Но это не так: в самом деле, Φ_n делит $x^n - 1$, а значит, и после редукции это свойство сохранится: $\overline{\Phi_n}$ делит $x^n - \bar{1}$, а $x^n - \bar{1}$ сепарабелен в $\mathbb{F}_p[x]$. ■

Вычисление автоморфизмов расширений полей (групп Галуа)

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

Решение.

Отметим, что можно говорить о группе $Aut\,\mathbb{R}$, так как у $\mathbb{Q}$ нет нетривиальных автоморфизмов – любой автоморфизм любого объемлющего поля оставляет 0 и 1 на месте, а значит, и все элементы $\mathbb{Q}$ оставляет на месте.

Пусть φ – автоморфизм $\mathbb{R}$. Тогда:

- $x > 0 \Longrightarrow \varphi(x) > 0$. Действительно, если $y^2 = x$, то $(\varphi(y))^2 = \varphi(x) > 0$.
- $y > x \Longrightarrow \varphi(y) > \varphi(x)$. Действительно, если $y - x > 0$, то $\varphi(y - x) = = \varphi(y) - \varphi(x) > 0$.

Допустим, $\exists z$: $\varphi(z) \neq z$ (пусть для определенности $\varphi(z) > z$) Тогда на интервале $(z, \varphi(z))$ есть рациональная точка $q \in \mathbb{Q}$, и с одной стороны должно быть выполнено $\varphi(z) > \varphi(q) = q$, а с другой стороны $\varphi(q) > \varphi(z)$ (так как $q > z$) – противоречие, значит, $\varphi(z) = z$, $\forall z \in \mathbb{R}$, т.е. не существует нетривиальных автоморфизмов $\mathbb{R}$. ■

Задача. Рассмотрим поле $\mathbb{F}_q$, $q = p^n$, $p = char\ \mathbb{F}_q > 0$. Найти $Aut\ (\mathbb{F}_q/\mathbb{F}_p)$.

Решение.
Отметим, что $Aut\ (\mathbb{F}_q/\mathbb{F}_p) = Aut\ \mathbb{F}_q$, так как всякий автоморфизм $\mathbb{F}_q$ оставляет неподвижными элементы поля $\mathbb{F}_p$ (так как 0 и 1 неподвижны).

Рассмотрим автоморфизм Фробениуса $\Phi \in Aut\ \mathbb{F}_q$:

$$\Phi\colon \mathbb{F}_q \to \mathbb{F}_q$$
$$a \mapsto a^p$$

Имеем: $(\mathbb{F}_q\colon \mathbb{F}_p) = n \geq \left|Aut\ (\mathbb{F}_q/\mathbb{F}_p)\right|$ (так как $\mathbb{F}_q$ является n-мерным векторным пространством над $\mathbb{F}_p$), поэтому если мы докажем, что $ord(\Phi) = n$, то докажем, что Φ порождает $Aut\ (\mathbb{F}_q/\mathbb{F}_p)$.

Рассмотрим группу $\mathbb{F}_q^{\times} = < b >_{q-1}$. Это циклическая группа (как мультипликативная группа поля), $b^{q-1} = 1 \Longrightarrow b^q = b,\ b^k \neq b,\ 1 < k < q$. Таким образом, $b^{p^m} \neq b$ при $0 < m < n$ и

$$\Phi^m(a) = a^{p^m} \neq a \Longrightarrow ord(\Phi) = n$$

Таким образом, $Aut\ (\mathbb{F}_q/\mathbb{F}_p) \simeq \mathbb{Z}_n$, где $q = p^n$. ■

Задача. Рассмотрим круговое поле $K_n = \mathbb{Q}(x^n - 1)$. Найти $Aut\ (K_n/\mathbb{Q})$.

Решение.

Как было найдено ранее (см. предыдущий семинар), $|Aut\ (K_n/\mathbb{Q})| = |(K_n:\mathbb{Q})| = \varphi(n)$. Далее, как мы знаем, $K_n = \mathbb{Q}(x^n - 1) = \mathbb{Q}(\varepsilon)$, где ε – первообразный корень степени n из 1.

Пусть $\varphi \in Aut\ (K_n/\mathbb{Q})$, тогда φ однозначно определяется действием на ε, и $\varphi(\varepsilon)$ – тоже первообразный корень степени n из 1. Кроме того, любой другой первообразный корень ε' имеет вид $\varepsilon' = \varphi(\varepsilon) = \varepsilon^k$ для некоторого $\varphi \in Aut\ (K_n/\mathbb{Q})$ (так как $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\varepsilon')$) при условии $(k, n) = 1$. Таким образом, имеет место взаимно-однозначное соответствие:

$$\varphi \mapsto k\ mod\ n,\ \ (k,n) = 1$$
$$Aut\ (K_n/\mathbb{Q}) \leftrightarrow \mathbb{Z}_n^\times$$

Это изоморфизм групп. В самом деле, пусть $\varphi, \psi \in Aut\ (K_n/\mathbb{Q})$ и $\varphi(\varepsilon) = \varepsilon^k$, $\psi(\varepsilon) = \varepsilon^l$, тогда $\varphi\psi(\varepsilon) = \varphi\big(\psi(\varepsilon)\big) = \varphi(\varepsilon^l) = (\varphi(\varepsilon))^l = (\varepsilon^k)^l = \varepsilon^{kl} = \varphi(\varepsilon)\psi(\varepsilon)$. Итак,

$$Aut\ (K_n/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$$

■

Общий метод вычисления групп автоморфизмов расширений полей

Ограничимся сепарабельными расширениями $K \subseteq M$. Как мы знаем, для всякого конечного сепарабельного расширения $K \subseteq M$ существует расширение Галуа $K \subseteq L$, $L \supseteq M$, а всякое расширение Галуа является полем разложения сепарабельного многочлена: $L = K(f)$, $f \in K[x]$ – сепарабельный, $a_1, \dots, a_n \in L$ – все корни f.

Пусть $G = Aut\ (L/K)$. На лекциях мы доказали основную теорему теории Галуа:

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 $Aut\ (M/K) \cong G/H$.

Также в процессе доказательства мы выяснили, что $Aut\ (M/K) \simeq N_G(H)/H$, где $N_G(H)$ – нормализатор H в G. Таким образом, если мы умеем вычислять группу автоморфизмов расширения Галуа, то вычисление группы автоморфизмов расширения $K \subseteq M$ сводится к вопросу теории групп (найти нормализатор заданной подгруппы в заданной группе и профакторизовать по подгруппе).

Итак, вычисление группы автоморфизмов всякого конечного сепарабельного расширения сводится к вычислению группы Галуа. Далее будем рассматривать только бесконечные поля (случай конечных полей был рассмотрен ранее – см. задачу про нахождение $Aut\ (\mathbb{F}_q/\mathbb{F}_p)$).

Посмотрим, как действует G в поле $L = K(f) = K(a_1, \dots, a_n)$: всякий элемент $g \in G$ однозначно определяется своим действием на корнях многочлена f, т.е. перестановкой $a_1, \dots, a_n$. Таким образом, мы получаем вложение $G \hookrightarrow S_n$, оно единственно с точностью до сопряженности (зависит от нумерации корней f).

- Задача 1 (для самостоятельного решения). Доказать, что f неприводим над $K \iff G$ действует на $\{a_1, \dots, a_n\}$ транзитивно.

Рассмотрим $K[x_1, \dots, x_n]$ – кольцо многочленов от n переменных над полем K. На этом множестве действует группа подстановок S_n:

$$\text{если } q \in K[x_1, \dots, x_n], \text{ то } \sigma(q)(x_1, \dots, x_n) = q(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

Обозначим $H = St(q) \subseteq S_n$ – стабилизатор многочлена q в группе S_n (это множество всех перестановок из S_n, оставляющих q на месте). Тогда

$$\sigma(q) = \pi(q) \iff \sigma H = \pi H, \qquad \forall \sigma, \pi \in S_n$$

Рассмотрим многочлен $Q(x) = \prod(x - \sigma(q))$, где σ пробегает представителей всех левых смежных классов S_n по H. Понятно, что $Q \in K[x_1, \dots, x_{n+1}]$.

- Задача 2 (для самостоятельного решения). Доказать, что Q симметричен по $x_1, \dots, x_n$.

Подставим в Q вместо переменных $x_1, \dots, x_n$ корни $a_1, \dots, a_n$ многочлена f: рассмотрим многочлен R – *резольвенту* f (по отношению к $H = St(q)$):

$$R(x) = Q(x, a_1, \dots, a_n) = \prod_{\sigma H} (x - q(a_{\sigma(1)}, \dots, a_{\sigma(n)}))$$

Утверждение. $R \in K[x]$.

Доказательство.
Коэффициенты R – симметрические многочлены от $a_1, \dots, a_n$, а значит, являются многочленами от коэффициентов f (следует из основной теоремы о симметрических многочленах и теоремы Виета). Следовательно, коэффициенты R лежат в K. ■

Предложение. Пусть R сепарабельна. Тогда: $G \subseteq \sigma H \sigma^{-1}$ для некоторой $\sigma \in S_n \iff R$ имеет корень в K.

Доказательство.
Заметим, что $St\big(\sigma(q)\big) = \sigma H \sigma^{-1}$. Пусть R имеет корень в K, тогда $q(a_{\sigma(1)}, \dots, a_{\sigma(n)}) \in K$ для некоторой σ, т.е. $\sigma(q)(a_1, \dots, a_n) \in K$. Это равносильно тому, что $\forall g \in G$ выполнено:

$$g\big(\sigma(q)(a_1, \dots, a_n)\big) = \sigma(q)(a_1, \dots, a_n) \iff \sigma(g)(g(a_1), \dots, g(a_n)) = \sigma(q)(a_1, \dots, a_n)$$

Другими словами, перестановка корней, задаваемая элементом $g \in G$, не меняет значение многочлена $\sigma(q)$. Так как R сепарабелен, это равносильно тому, что $g\sigma(q) = \sigma(q)$, т.е. что $g \in \sigma H \sigma^{-1}$. ■

Доказанное предложение указывает, где искать группу Галуа конкретного многочлена – если резольвента сепарабельна, то группа Галуа содержится в подгруппе S_n. При малых n можно перебором подгрупп S_n понять, в каких из них группа Галуа содержится, и тем самым определить ее (с точностью до сопряженности). Этот метод неплохо работает для многочленов малых степеней (не выше 5).

Семинар 4. Вычисление группы Галуа с помощью резольвент.

Разбор задач домашнего задания.

Напоминание: рассматриваем сепарабельный $f \in K[x]$, $a_1, \dots, a_n$ – его корни в $L = K(f)$, $G = Aut\ (L/K) \hookrightarrow S_n$.

Задача 3. Доказать, что сепарабельный многочлен $f \in K[x]$ неприводим тогда и только тогда, когда группа Галуа расширения $K(f) \supseteq K$ транзитивно переставляет корни многочлена f в $K(f)$.

Доказательство.
Допустим, f неприводим над K, и G действует на $\{a_1, \dots, a_n\}$ не транзитивно: например, $Ga_1 = \{a_{i_1}, \dots, a_{i_k}\}$, $k < n$. Рассмотрим

$$\mu(x) = \prod_{\tilde{a} \in Ga_1} (x - \tilde{a}) = c_0 + c_1 x + \dots + x^k \in K[x]$$

- минимальный многочлен a_1 над K. Тогда f должен делиться на $\mu(x)$, но f неприводим над K – противоречие.

Обратно, если орбита какого-то корня содержит меньше n корней, то f должен делиться на минимальный многочлен этого корня, следовательно, f приводим. ■

Задача 4а. Пусть $f \in K[x]$ – сепарабельный многочлен, $a_1, \dots, a_n$ – все его корни в поле разложения $L = K(f)$, $G = Aut(L/K)$ – группа Галуа, рассматриваемая как подгруппа в группе S_n перестановок корней. Пусть $H \subseteq S_n$ – произвольная подгруппа, и $q \in K(x_1, \dots, x_n)$ – многочлен, стабилизатор которого при действии группы S_n равен H. Доказать, что многочлен $Q(x, x_1, \dots, x_n) = \prod_\sigma (x - q(x_{\sigma(1)}, \dots, x_{\sigma(n)}))$, где σ пробегает по одному элементу из каждого смежного класса в S_n по H, симметричен по отношению к переменным $x_1, \dots, x_n$.

Доказательство.
Многочлены $q(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ входят в орбиту многочлена q под действием группы S_n, поэтому всякая перестановка переменных $x_1, \dots, x_n$ лишь меняет порядок сомножителей в $\prod(x - q(x_{\sigma(1)}, \dots, x_{\sigma(n)}))$, но не меняет результат произведения. ■

Как было доказано на прошлом семинаре, $R \in K[x]$, где R – резольвента f (по отношению к $H = St(q)$):

$$R(x) = Q(x, a_1, \dots, a_n) = \prod_{\sigma H} (x - q(a_{\sigma(1)}, \dots, a_{\sigma(n)}))$$

Поподробнее разберем доказательство утверждения, приведенного в конце прошлого семинара.

Предложение. Пусть R сепарабельна. Тогда: $G \subseteq \sigma H \sigma^{-1}$ для некоторой $\sigma \in S_n \iff R$ имеет корень в K.

Доказательство.
Заметим, что $St\big(\sigma(q)\big) = \sigma H \sigma^{-1}$, поэтому $G \subseteq \sigma H \sigma^{-1} \iff g\sigma(q) = \sigma(q),\ \forall g \in G$, т.е.

$$q\big(x_{g\sigma(1)}, \dots, x_{g\sigma(n)}\big) = q\big(x_{\sigma(1)}, \dots, x_{\sigma(n)}\big), \qquad \forall g \in G.$$

Так как из совпадения многочленов следует совпадение их значений на любом наборе переменных, то из последнего равенства следует, что

$$q\big(a_{g\sigma(1)}, \dots, a_{g\sigma(n)}\big) = q\big(a_{\sigma(1)}, \dots, a_{\sigma(n)}\big), \qquad \forall g \in G$$

Обратное включение (т.е. то, что из совпадения значений многочленов на любом наборе переменных следует их равенство как функций) следует из сепарабельности резольвенты.

Заметим, что $q\big(a_{g\sigma(1)}, \dots, a_{g\sigma(n)}\big) = g\left(q\big(a_{\sigma(1)}, \dots, a_{\sigma(n)}\big)\right)$ – перестановка корней, задаваемая элементом $g \in G$, не меняет значение многочлена $\sigma(q)$. Далее, условие

$$g\left(q\big(a_{\sigma(1)}, \dots, a_{\sigma(n)}\big)\right) = q\big(a_{\sigma(1)}, \dots, a_{\sigma(n)}\big),\ \ \forall g \in G$$

равносильно тому, что $q\big(a_{\sigma(1)}, \dots, a_{\sigma(n)}\big)$ (т.е. один из корней резольвенты) лежит в K. ■

Вычисление группы Галуа с помощью резольвент

Задача. Пусть $f(x) = x^4 + 4x + 5$. Найти $G = Aut\ (\mathbb{Q}(f)/\mathbb{Q})$.

Решение.

1) Неприводимость над $\mathbb{Q}$.

Легко видеть, что у f нет корней в $\mathbb{Q}$ (переберем все дроби, числитель которых делит свободный член, а знаменатель – старший коэффициент, т.е. $\pm 1, \pm 1/5$). Следовательно,

если f приводим, то $f = (x^2 + ax \pm 1)(x^2 + bx \pm 5)$. Раскрывая скобки, получаем систему относительно a и b, которая не имеет решений в целых числах. Следовательно, f неприводим.

2) Транзитивные подгруппы в S_4.

Пусть H – транзитивная подгруппа в S_4. Она должна транзитивно действовать на множестве $\{1,2,3,4\}$, т.е. у нее должна быть орбита из 4 элементов. Так как порядок орбиты делит порядок группы, нужно искать подгруппы, чей порядок делится на 4 (и при этом является делителем $|S_4| = 24$). Получаем возможные варианты:

$$H = S_4,\ \ A_4,\ \ D_4,\ \ V_4,\ \ \mathbb{Z}_4$$

Действительно, делители 24, которые делятся на 4 – это числа $24, 12, 8, 4$.

- Подгруппа порядка 24 одна – это сама группа S_4.
- Подгруппа порядка 12 одна – это группа A_4 (действительно, подгруппа порядка 12 – это подгруппа индекса 2, т.е. абелева, поэтому она должна содержать коммутант группы S_4, т.е. A_4, следовательно, она равна A_4).
- Подгруппа порядка 8 одна (с точностью до сопряженности) – это группа D_4 (так как подгруппа порядка $8 = 2^3$ – силовская).
- Подгрупп порядка 4 две – это V_4 и $\mathbb{Z}_4$. Действительно, из второй теоремы Силова следует, что 2-подгруппы содержатся в силовской 2-подгруппе, т.е. в D_4, а подгруппы порядка 4 в D_4 найти уже проще – это либо циклическая группа, либо четверная группа Клейна.

Протестируем эти группы на их возможность быть группой Галуа $f(x) = x^4 + 4x + 5$.

- $H = A_4$.

Найдем резольвенту. Для этого вначале найдем многочлен $q(x_1, x_2, x_3, x_4)$, такой что $A_4 = St(q)$. Например:

$$q(x_1, x_2, x_3, x_4) = \prod_{i<j}(x_i - x_j)$$

Далее строим многочлен $Q(x) = \prod(x - \sigma(q))$, где σ пробегает представителей всех левых смежных классов S_4 по A_4:

$$Q(x, x_1, x_2, x_3, x_4) = (x - q)(x + q) = x^2 - q^2,$$

$$q^2(a_1, a_2, a_3, a_4) = \prod_{i<j}\left(a_i - a_j\right)^2 = D(f)$$

Получаем

$$R(x) = (x - \sqrt{D})(x + \sqrt{D})$$

Таким образом (см. задачу 3), $G \subseteq A_n \Leftrightarrow R$ имеет корень в K, т.е. $D(f)$ – полный квадрат в K. Найдем $D(f)$ – для этого нужно выразить его через элементарные симметрические многочлены от a_1, a_2, a_3, a_4. Заметим, что $\sigma_1 = \sigma_2 = 0$ (это коэффициенты при x и $-x^3$), поэтому нас будет интересовать только та часть выражения $D(f)$ через элементарные симметрические многочлены, которая содержит σ_3 и σ_4. Так как $\deg \prod_{i<j}(x_i - x_j)^2 = 12$, то

$$\prod_{i<j}(x_i - x_j)^2 = \alpha\sigma_3^4 + \beta\sigma_4^3 + \cdots$$

Подставляя вместо x_1, x_2, x_3, x_4 наборы $(1, \varepsilon, \varepsilon^2, 0)$, где ε – корень степени 3 из 1 и $(1, i, -1, -i)$ (т.е. такие наборы, на которых $\sigma_1 = \sigma_2 = 0$, $\sigma_3 = 1$, $\sigma_4 = 0$ и $\sigma_1 = \sigma_2 = 0$, $\sigma_3 = 0$, $\sigma_4 = -1$ соответственно), получаем, что $\alpha = -27$, $\beta = 256$. Получаем

$$D(x^4 + 4x + 5) = -27\sigma_3^4 + 256\sigma_4^3 = -27 \cdot (-4)^4 + 256 \cdot 5^3 = 2^9 \cdot 7^2$$

- не является квадратом в $K = \mathbb{Q}$, т.е. G не содержится в A_4.

- $H = D_4$.

Найдем резольвенту. Для этого вначале найдем многочлен $\tilde{q}(x_1, x_2, x_3, x_4)$, такой что $D_4 = St(\tilde{q})$. Например:

$$\tilde{q}(x_1, x_2, x_3, x_4) = q + q' + q'',$$

где $q = x_1x_3 + x_2x_4$, $q' = x_1x_2 + x_3x_4$, $q'' = x_1x_4 + x_2x_3$. Далее строим многочлен $Q(x) = \prod(x - \sigma(\tilde{q}))$, где σ пробегает представителей всех левых смежных классов S_4 по D_4:

$$Q(x, x_1, x_2, x_3, x_4) = (x - q)(x - q')(x - q'')$$

Имеем:

$$\sigma_1(q, q', q'') = \sum_{i<j} x_ix_j = \sigma_2$$

$$\sigma_2(q, q', q'') = \sum x_i^2x_jx_k = \sigma_1\sigma_3 - 4\sigma_4$$

$$\sigma_3(q, q', q'') = \sum x_i^3x_jx_kx_l + \sum x_i^2x_j^2x_k^2 = \sigma_4(\sigma_1^2 - 2\sigma_2) + \sigma_3^2 + \underbrace{\cdots}_{\text{функция от } \sigma_1 \text{ и } \sigma_2}$$

Так как $\sigma_1 = \sigma_2 = 0$, то

$\sigma_1(q, q', q'') = 0$

$\sigma_2(q, q', q'') = -4\sigma_4 = -20$

$\sigma_3(q, q', q'') = \sigma_3^2 = 16$

Получаем

$$R(x) = x^3 - 20x - 16$$

Так как $R(x)$ имеет рациональный корень $x = -4$, то G содержится в D_4 (но при этом G не содержится в A_4, как мы выяснили ранее). Таким образом, осталось проверить, не содержится ли G в $\mathbb{Z}_4$ – если содержится, то $G = \mathbb{Z}_4$, а если не содержится, то $G = D_4$. ■

Семинар 5. Обратимые элементы и делители нуля в кольцах и алгебрах. Идеалы.

Разбор задач домашнего задания.

Продолжим решение задачи, начатой на прошлом семинаре (найти группу Галуа $G = Aut\,(\mathbb{Q}(f)/\mathbb{Q})$ для $f(x) = x^4 + 4x + 5$). Нам осталось проверить, содержится ли G в $\mathbb{Z}_4$.

Ранее мы нашли резольвенту для случая $H = D_4$:

$$R(x) = x^3 - 20x - 16 = (x+4)(x^2 - 4x - 4) = (x+4)\left(x - 2 + 2\sqrt{2}\right)\left(x - 2 - 2\sqrt{2}\right)$$

Так как $R(x) = \left(x - q(a_1, a_2, a_3, a_4)\right)\left(x - q'(a_1, a_2, a_3, a_4)\right)(x - q''(a_1, a_2, a_3, a_4))$, то без ограничения общности можно считать, что:

$q(a_1, a_2, a_3, a_4) = a_1a_2 + a_3a_4 = -4$
$q'(a_1, a_2, a_3, a_4) = a_1a_3 + a_2a_4 = 2 - 2\sqrt{2}$
$q''(a_1, a_2, a_3, a_4) = a_1a_4 + a_2a_3 = 2 + 2\sqrt{2}$

Кроме того, $a_1a_2a_3a_4 = 5$ (свободный член $f(x)$). Этого достаточно, чтобы найти, чему равны попарные произведения корней: например, a_1a_2 и a_3a_4 являются корнями квадратного уравнения $y^2 + 4y + 5 = 0$, откуда $a_1a_2 = -2 \pm i$, $a_3a_4 = -2 \mp i$.

Далее, рассмотрим $\mathbb{Q}(f)$ – поле разложения многочлена f. Как мы ранее выяснили, имеется две возможности: $Aut\,(\mathbb{Q}(f)/\mathbb{Q}) = D_4$ или $\mathbb{Z}_4$. Если $Aut\,(\mathbb{Q}(f)/\mathbb{Q}) = \mathbb{Z}_4$, то $(\mathbb{Q}(f):\mathbb{Q}) = 4$. В $\mathbb{Z}_4$ есть ровно одна подгруппа порядка 2 (так как $\mathbb{Z}_4$ - циклическая), тогда из основной теоремы теории Галуа следует, что существует ровно одно промежуточное поле M, такое что $\mathbb{Q}(f) \supset M \supset \mathbb{Q}$ и $(M:\mathbb{Q}) = 2$, $(\mathbb{Q}(f):M) = 2$.

На самом деле, в $\mathbb{Q}(f)$ есть как минимум два промежуточных подполя, удовлетворяющих этому условию. Действительно, ранее мы нашли попарные произведения корней f, откуда следует, что $i \in \mathbb{Q}(f)$ и $\sqrt{2} \in \mathbb{Q}(f)$, а значит, $\mathbb{Q}(i) \in \mathbb{Q}(f)$ и $\mathbb{Q}(\sqrt{2}) \in \mathbb{Q}(f)$. Следовательно, $Aut\,(\mathbb{Q}(f)/\mathbb{Q}) = D_4$. ■

Задача 2с. Вычислить группу Галуа поля разложения многочлена $x^4 + 4x^2 + 9$ над $\mathbb{Q}$.

Решение.
Так как уравнение $f(x) = 0$ является биквадратным, корни находятся легко:

$$x^4 + 4x^2 + 9 = 0 \Leftrightarrow (x^2+2)^2 = -5 \Leftrightarrow x^2 = -2 \pm i\sqrt{5} \Leftrightarrow x = \pm\sqrt{-2 \pm i\sqrt{5}}$$

- корни $f(x)$ разбиваются на пары: $a_1, a_2, -a_1, -a_2$. Поэтому дискриминант находится сразу:

$$D(f) = \prod_{i<j}(a_i - a_j)^2 = 16(a_1^2 - a_2^2)^4 a_1^2 a_2^2$$

$D(f)$ – полный квадрат в $\mathbb{Q}$, следовательно, $G \subseteq A_4$. Далее, легко видеть, что $(\mathbb{Q}(f):\mathbb{Q}) = 4$ (так как с присоединением любого корня f присоединяются и остальные корни), поэтому остаются два варианта: $Aut\,(\mathbb{Q}(f)/\mathbb{Q}) = V_4$ или $\mathbb{Z}_4$. Вариант $G = \mathbb{Z}_4$ отпадает (см. дискриминант), следовательно, $G = V_4$. ■

Кольца

Далее будем рассматривать ассоциативные кольца. Пусть A – ассоциативное кольцо\алгебра над полем K. Вообще, A может и не содержать единицу, однако, любое ассоциативное кольцо можно вложить в кольцо с единицей путем присоединения единицы.

Присоединение единицы: $\tilde{A} = A \oplus \mathbb{Z}$ (в случае колец), или $\tilde{A} = A \oplus K$ (в случае алгебр) – ассоциативное кольцо/алгебра с единицей $\tilde{1} = (0,1)$. Умножение определяется следующим образом: пусть $\tilde{a} = (a, \lambda)$, $\tilde{b} = (b, \mu)$. Тогда

$$\tilde{a}\tilde{b} = (ab + \mu a + \lambda b, \lambda\mu)$$

Поэтому далее будем рассматривать ассоциативные кольца с 1. Тогда естественным образом возникает группа обратимых элементов $A^\times = \{a \in A \mid \exists b \in A:\ ab = ba = 1\}$, которая является важной характеристикой кольца.

Примеры групп обратимых элементов:

1) $\mathbb{Z}^\times = \{\pm 1\}$,

2) Рассмотрим кольцо гауссовых чисел $\mathbb{Z}[i] = \{a + bi \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$. Тогда

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$$

Действительно, рассмотрим норму комплексного числа $\gamma = a + bi$ (квадрат его модуля): $N(\gamma) = |\gamma|^2 = \gamma\bar{\gamma} = a^2 + b^2$. Так как $N(\gamma_1\gamma_2) = N(\gamma_1)N(\gamma_2)$, то $\gamma \in \mathbb{Z}[i]^\times \Leftrightarrow N(\gamma) = 1$.

3) $K[x_1, \dots, x_n]^\times = K^\times$,

4) Рассмотрим алгебру формальных степенных рядов $K[\![x_1, \dots, x_n]\!]$, элементами которой являются степенные ряды вида

$$f = \sum_{k_1,\dots,k_n \geq 0} c_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n} = f_0 + f_1 + \cdots + f_k + \cdots,$$

где $c_{k_1 \dots k_n} \in K$, f_k – однородный многочлен степени k. Тогда

$$K[\![x_1, \dots, x_n]\!]^\times = \{f \mid f_0 \neq 0\}$$

Действительно, пусть $f = f_0 + f_1 + \cdots + f_k + \cdots$. Найдем $g = g_0 + g_1 + \cdots + g_k + \cdots$, удовлетворяющий равенству

$$1 = fg = \sum_{n=0}^{\infty} \sum_{k=0}^{n} f_k g_{n-k} = f_0 g_0 + (f_0 g_1 + f_1 g_0) + \cdots$$

Получаем $g_0 = f_0^{-1}$, $g_1 = -\frac{f_1 g_0}{f_0}$, и так далее.

5) Рассмотрим кольцо p-адических чисел $\mathbb{Z}_p$ (p-простое), состоящее из чисел вида $a = a_0 + a_1 p + a_2 p^2 + \cdots$, где $0 \leq a_i < p$. Определение сложения и умножения таких чисел особых трудностей не вызывает, для определения вычитания достаточно понять, что $-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$.

- а) Доказать, что $\mathbb{Z}_p$ – коммутативное ассоциативное кольцо с 1, содержащее $\mathbb{Z}$,
- б) Найти $\mathbb{Z}_p^\times$,
- в) Найти все идеалы в $\mathbb{Z}_p$.

Задача. Пусть A – конечномерная алгебра с 1. Доказать, что:

- (1) левые делители нуля $\Leftrightarrow$ правые делители нуля,
- (2) обратимые слева элементы $\Leftrightarrow$ обратимые справа элементы,
- (3) неделитель нуля $\Leftrightarrow$ обратимый элемент.

Решение.
Пусть $a \in A$. Рассмотрим оператор умножения на a слева:

$$L_a \colon A \to A$$
$$x \mapsto ax$$

1) Если a – левый делитель нуля $\Longrightarrow Ker\, L_a \neq \{0\}$, т.е. L_a вырожден. Рассмотрим его минимальный многочлен

$$\mu_{L_a}(t) = t^n + c_1 t^{n-1} + \cdots + c_{n-1} t$$

(здесь свободный член $c_n = 0$, так как $c_n = \det L_a$). Из теоремы Гамильтона-Кэли следует, что $\mu_{L_a}(L_a) = 0$ – если посмотреть на это равенство как на равенство операторов, то получим, что $x \mapsto (a^n + c_1 a^{n-1} + \cdots + c_{n-1} a)x = 0$ для любого x. Выбирая $x = 1$, получаем, что $a^n + c_1 a^{n-1} + \cdots + c_{n-1} a = 0$ – но отсюда следует, что $(a^{n-1} + c_1 a^{n-2} + \cdots + c_{n-1})a = 0$, т.е. a – правый делитель нуля.

То, что всякий правый делитель нуля является также и левым делителем нуля, доказывается аналогично, только нужно рассмотреть оператор умножения на a справа.

2) Если a обратим слева/справа $\Longrightarrow Ker\, L_a = \{0\}$, т.е. L_a невырожден. Пусть, например, a обратим слева, т.е. $\exists b$: $ba = 1$, тогда $L_b L_a = id \Longrightarrow L_b = L_a^{-1}$, откуда следует, что $L_a L_b = id \Longrightarrow ab = 1$, т.е. a обратим справа.

3) Если a неделитель нуля $\Longrightarrow Ker\, L_a = \{0\}$, т.е. L_a невырожден. Рассмотрим его минимальный многочлен

$$\mu_{L_a}(t) = t^n + c_1 t^{n-1} + \cdots + c_{n-1} t + c_n$$

(здесь свободный член $c_n \neq 0$, так как все собственные значения L_a отличны от нуля). Далее, рассуждая как в п.1, получаем, что $a^n + c_1 a^{n-1} + \cdots + c_{n-1} a + c_n = 0$, откуда $a^{-1} = -\frac{1}{c_n} a^{n-1} - \frac{c_1}{c_n} a^{n-2} - \cdots - \frac{c_{n-1}}{c_n}$. ■

Идеалы в кольцах/алгебрах

Пусть $I \subset A$ – левый/правый/двусторонний идеал. Тогда $I \not\ni 1$ (так как идеал собственный), откуда следует, что I не содержит обратимых элементов.

Задача. Когда все необратимые элементы кольца/алгебры образуют идеал?

Решение.
Вспомним примеры колец, которые мы рассматривали ранее, и проверим, образуют ли необратимые элементы этих колец идеал:

- $\mathbb{Z}$ – нет,
- $\mathbb{Z}[i]$ – нет,
- $K[x_1, \ldots, x_n]$ – нет,
- $K[\![x_1, \ldots, x_n]\!]$ – да.

Определение. Кольцо A локально, если $A\backslash A^\times$ - идеал (автоматически двусторонний).

Оказывается, для локальности достаточно того, чтобы $A\backslash A^\times$ было аддитивной подгруппой / подпространством. Ясно, что $A\backslash A^\times$ - наибольший из собственных идеалов (левых, правых, двусторонних). Это мы докажем на следующем семинаре (см. задачу 7).
■

Семинар 6. Идеалы в кольцах и алгебрах. Простые кольца, алгебры и модули. Алгебра Вейля.

Разбор задач домашнего задания.

Задача 2b,c. Пусть $\mathbb{Z}_p$ – кольцо p-адических чисел (p-простое), состоящее из чисел вида $a = a_0 + a_1 p + a_2 p^2 + \cdots$, где $0 \le a_i < p$.

- (b) Найти группу обратимых элементов $\mathbb{Z}_p^\times$.
- (c) Описать все идеалы в $\mathbb{Z}_p$.

Решение.
1) Докажем, что $a = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p^\times \Leftrightarrow a_0 \neq 0$. Действительно, импликация "$\Longrightarrow$" очевидна. Докажем в обратную сторону – найдем $b = b_0 + b_1 p + b_2 p^2 + \cdots$, такой что $ab = 1$.

Так как $a_0 \neq 0$, то $\overline{a_0}$ обратим в $\mathbb{Z}/p\mathbb{Z}$, т.е. существует $\overline{b_0}$ в $\mathbb{Z}/p\mathbb{Z}$, такой что $\overline{a_0}\overline{b_0} = \overline{1}$, т.е. $a_0 b_0 = 1 + pc_0$ для некоторого c_0. Получаем

$$ab = 1 + (a_0 b_1 + a_1 b_0 + c_0)p + \cdots$$

где a_0, b_0, c_0, a_1 известны, а b_1 подбираем так, чтобы $a_0 b_1 + a_1 b_0 + c_0 \equiv 0 \ (mod\ p)$. И так далее – в итоге мы для каждого i сможем найти b_i, т.е. построить b, такой что $ab = 1$.

2) Докажем, что в кольце p-адических чисел $\mathbb{Z}_p$ все идеалы имеют вид $p^k \cdot \mathbb{Z}_p$. Действительно, ясно, что все числа вида $p^k \cdot \mathbb{Z}_p$ образуют идеал, а других идеалов нет: пусть $I \subset \mathbb{Z}_p$ – произвольный идеал. Если $a_k p^k + a_{k+1} p^{k+1} + \cdots \in I$, $a_k \neq 0$, то и $p^k \in I$ – в самом деле, $a_k p^k + a_{k+1} p^{k+1} + \cdots = p^k (a_k + a_{k+1} p + \cdots)$, а элемент $a_k + a_{k+1} p + \cdots$ является обратимым (как мы выяснили в п.1) – домножая на обратный к нему, получаем, что $p^k \in I$. Отсюда следует, что $I = p^k \cdot \mathbb{Z}_p$. ■

Задача 7. Доказать, что если в ассоциативном кольце (или алгебре) с единицей все необратимые элементы образуют аддитивную подгруппу (или подпространство), то это множество – двусторонний идеал. Такие кольца (алгебры) называются *локальными*.

Решение.
Пусть A – ассоциативное кольцо (или алгебра) с единицей, и $A \backslash A^\times$ образует аддитивную подгруппу (или подпространство). Докажем, что если $a \in A \backslash A^\times$ и $b \in A$, то $ab \in A \backslash A^\times$ (доказательство того, что $ba \in A \backslash A^\times$ проводится аналогично). Рассмотрим два случая.

1) $b \in A^\times$. Если бы $ab \in A^\times$, то $a = ab \cdot b^{-1}$, откуда следует, что $a \in A^\times$ - противоречие.

2) $b \in A \backslash A^\times$. Тогда $1 - b \in A^\times$ (так как $b + (1 - b) = 1$ – обратимый элемент, а по условию все необратимые элементы образуют аддитивную подгруппу). Но тогда из п.1. следует, что $a(1 - b) = a - ab \in A \backslash A^\times$, поэтому и $a - (a - ab) = ab \in A \backslash A^\times$. ■

Задача 6с. Пусть A – ассоциативное кольцо с единицей и $a, b \in A$. Доказать, что в общем случае из обратимости ab не следует обратимость a и b.

Решение.
Пусть V – счетномерное векторное пространство с базисом $e_1, e_2, \dots$ Рассмотрим $A = L(V)$ – алгебру операторов на V. Пусть $a \in A$ сдвигает базисные векторы вправо: $e_i \mapsto e_{i+1}$, а $b \in A$ влево: $e_i \mapsto e_{i-1}$, $e_1 \mapsto 0$. Тогда $ba = id$ – обратимый оператор, но оператор ab: $e_i \mapsto e_i$, $e_1 \mapsto 0$ не будет обратимым, также не будут обратимыми a и b. ■

Идеалы в кольцах/алгебрах

Рассмотрим $A = C(X)$ – алгебру (K-значных, $K = \mathbb{R}$ или $\mathbb{C}$) непрерывных функций на топологическом пространстве X и поймем, как в ней устроены идеалы.

Рассмотрим $I(Y) = \{f \in C(X) \mid f_Y = 0\}$ – множество непрерывных функций, обращающихся в ноль на Y, где Y – замкнутое подмножество X. Легко видеть, что $I(Y) \lhd C(X)$. В частности, (считаем X достаточно “хорошим” пространством, в котором выполнены аксиомы отделимости), рассмотрим $I(x_0)$, где x_0 – точка пространства X.

Легко видеть, что $I(x_0) \lhd C(X)$ – максимальный (собственный) идеал. Действительно, из основной теоремы о гомоморфизмах следует, что $C(X)/I(x_0) \simeq K$: рассмотрим гомоморфизм φ: $C(X) \to K$, $\varphi(f) = f(x_0)$, тогда $I(x_0) = Ker\ \varphi$.

Задача. Доказать, что если X компактно, то любой максимальный идеал $I \lhd C(X)$ имеет вид $I = I(x_0)$ для некоторой точки $x_0 \in X$.

Решение.
От противного: пусть $\forall x_0 \in X\ \ \exists f_0 \in I$: $f_0(x_0) \neq 0$. Тогда существует окрестность $U_0 \ni x_0$, такая что f_0 не обращается в ноль на U_0. Следовательно, можно выбрать конечное покрытие $X = U_1 \cup \dots \cup U_s$ так что $\exists f_1, \dots, f_s \in I$, $f_i|_{U_i}$ не обращается в ноль.

Рассмотрим функцию $f = |f_1|^2 + \dots + |f_s|^2 = f_1\bar{f_1} + \dots + f_s\bar{f_s}$. Легко видеть, что $f \in I$, но при этом $f(x) > 0$, $\forall x \in X$. Следовательно, f обратима в $C(X)$ – противоречие (собственный идеал не содержит обратимых элементов). ■

Простые кольца и модули

Определение. Кольцо/алгебра A *просто*, если не существует ненулевых двусторонних идеалов, отличных от A. Модуль M *прост*, если не существует ненулевых подмодулей, отличных от M.

Утверждение 1. Коммутативное (ассоциативное с 1) кольцо A просто $\Leftrightarrow$ A – поле.

Отметим, что для некоммутативных колец утверждение 1 неверно – пример этому содержится в следующем утверждении.

Утверждение 2. Алгебра квадратных матриц $A = Mat_n(K)$ проста.

Также приведем пример бесконечномерной простой алгебры – построим алгебру Вейля.

Определение. Алгебра Вейля $A_n(K) = \{\partial\colon\ K[x_1, \dots, x_n] \to K[x_1, \dots, x_n]\}$, где

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

$f_{k_1,\dots,k_n} \in K[x_1, \dots, x_n]$.

Утверждение 3. Алгебра $A_n(K)$ проста, если $char\ K = 0$.

Указание: $A_n(K)$ порождается (как алгебра с 1) элементами $p_i = \frac{\partial}{\partial x_i}$ и q_i – операторами умножения на переменную x_i. В качестве первого шага доказательства утверждения 3 рассмотрим соотношения между порождающими: очевидно, что $p_i p_j = p_j p_i$ и $q_i q_j = q_j q_i$, однако $p_i q_j = q_j p_i$ только при $i \neq j$. Если $i = j$, то

$$(p_i q_i - q_i p_i)(f) = \frac{\partial}{\partial x_i}(x_i f) - x_i \frac{\partial}{\partial x_i}(f) = f + x_i \frac{\partial f}{\partial x_i} - x_i \frac{\partial f}{\partial x_i} = f,$$

то есть, $p_i q_i - q_i p_i = 1$.

Таким образом, любой элемент алгебры Вейля имеет вид $\partial = F(q_1, \dots, q_n, p_1, \dots, p_n)$ и этот вид определен однозначно. Базис $A_n(K)$ составляют одночлены $q_1^{l_1} \cdots q_n^{l_n} p_1^{k_1} \cdots k_n^{k_n}$.

Простые модули

Поймем, как проверить, что модуль M прост. Если бы существовал ненулевой подмодуль $N \subset M$, то выбрав ненулевой элемент $n \in N$, мы получили бы $An = \{an \mid a \in A\}$ – циклический подмодуль в M. При этом если $n \in N$, то и $An \subseteq N$.

Таким образом, для того, чтобы модуль M был прост, необходимо и достаточно, чтобы было выполнено $\forall m \in M\colon\ Am = M$.

Пример. Рассмотрим алгебру Вейля $A = A_n(K)$ (при условии, что $char\ K = 0$) и модуль $M = K[x_1, \dots, x_n]$. Доказать, что это простой модуль.

Доказательство.
Рассмотрим произвольный многочлен $f \in K[x_1, \dots, x_n]$. Применяя к нему операторы $p_1, \dots, p_n$ мы можем получить некоторую константу $\lambda \in K$, а затем, применяя операторы $q_1, \dots, q_n$ можем получить произвольный одночлен $\lambda_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}$, т.е. и весь модуль $M = K[x_1, \dots, x_n]$. Следовательно, M прост. ■

Семинар 7. Тензорное произведение модулей, колец и алгебр.

Разбор задач домашнего задания.

Задача 4. Доказать, что если поле K имеет нулевую характеристику, то любой простой $A_n(K)$-модуль бесконечномерен над K.

Доказательство.
Докажем от противного. Пусть M – конечномерный $A_n(K)$-модуль (как модуль над алгеброй с единицей). Как мы выяснили на прошлом семинаре, $A_n(K)$ порождена элементами $p_i = \frac{\partial}{\partial x_i}$ и q_i – операторами умножения на переменную x_i, которые удовлетворяют соотношению $p_i q_i - q_i p_i = 1$. Этим операторам соответствуют операторы $P_i \in L(M)$ и $Q_i \in L(M)$, которые удовлетворяют соотношению $P_i Q_i - Q_i P_i = E$. Но с одной стороны,

$$tr(P_i Q_i - Q_i P_i) = tr(P_i Q_i) - tr(Q_i P_i) = 0$$

а с другой –

$$tr(P_i Q_i - Q_i P_i) = tr(E) = \det M \neq 0$$

- противоречие. ■

Задача 3. Пусть $p_i = \frac{\partial}{\partial x_i}$ и $q_i =$ (умножение на x_i) – порождающие элементы алгебры Вейля $A_n(K)$ и $f = f(q_1, \dots, q_n, p_1, \dots, p_n) \in A_n(K)$ – произвольный элемент алгебры Вейля, канонически записанный в виде многочлена от порождающих элементов, т.е. линейной комбинации одночленов вида $q_1^{l_1} \cdots q_n^{l_n} p_1^{k_1} \cdots k_n^{k_n}$. Доказать, что

$$p_i f - f p_i = \frac{\partial f}{\partial q_i}, \qquad q_i f - f q_i = -\frac{\partial f}{\partial p_i}, \qquad \forall i = 1, \dots, n$$

Доказательство.
Достаточно доказать для одночленов $f = q_1^{l_1} \cdots q_n^{l_n} p_1^{k_1} \cdots k_n^{k_n}$. Имеем:

$$p_i f = p_i q_1^{l_1} \cdots q_n^{l_n} p_1^{k_1} \cdots k_n^{k_n} = q_1^{l_1} \cdots q_{n-1}^{l_{n-1}} p_i q_n^{l_n} p_1^{k_1} \cdots k_n^{k_n} = f p_i + l_i q_1^{l_1} \cdots q_{n-1}^{l_{n-1}} =$$

$$= f p_i + \frac{\partial f}{\partial q_i}$$

Для $q_i f - f q_i$ доказательство аналогичное. ■

Из задач 3 и 4 следует, что $A_n(K)$ проста в случае $char\ K = 0$. Действительно, пусть $A_n(K) \rhd I \neq 0$. Если $I \ni f \neq 0$, тогда и $\frac{\partial f}{\partial p_i}, \frac{\partial f}{\partial q_i} \in I$, следовательно, и $1 \in I$, т.е. $I = A_n(K)$.

Отметим, что из простоты $A_n(K)$ сразу вытекает, что любой простой $A_n(K)$-модуль бесконечномерен над K. В самом деле, всякий $A_n(K)$-модуль задает гомоморфизм $\varphi\colon A_n(K) \to L(M)$, где $L(M)$ – алгебра линейных операторов на M. Если $A_n(K)$-модуль конечномерен, то и алгебра $L(M)$ конечномерна. Но $A_n(K)$ бесконечномерна, следовательно, $Ker\ \varphi \neq \{0\}$. Так как $Ker\ \varphi \lhd A_n(K)$, то $Ker\ \varphi = A_n(K)$ и $\varphi = 0$, т.е. любое подпространство в $L(M)$ будет подмодулем. Противоречие.

Задача 6. (*Китайская теорема об остатках*). Пусть A – коммутативное ассоциативное кольцо с единицей, $I_1, \dots, I_s \lhd A$, причем $I_i + I_j = A$ при $i \neq j$. Доказать:

- (a) $I_1 \cdots I_{s-1} + I_s = A$ (под произведением идеалов понимается идеал, состоящий из всевозможных сумм элементов вида $a_1 \cdots a_{s-1}$, $a_i \in I_i$ – почему это идеал?)
- (b) $I_1 \cap \cdots \cap I_s = I_1 \cdots I_s$,
- (c) гомоморфизм $\varphi\colon A \to A/I_1 \oplus \cdots \oplus A/I_s$, $\varphi(a) = (a + I_1, \dots, a + I_s)$ сюръективен,
- (d) $A/(I_1 \cdots I_s) \simeq A/I_1 \oplus \cdots \oplus A/I_s$.

Доказательство.
(a) Так как $I_i + I_j = A$ при $i \neq j$, то $I_1 + I_s = \cdots = I_{s-1} + I_s = A$, откуда $1 = a_i + b_i$, где $a_i \in I_i,\ b_i \in I_s,\quad i = 1, \dots, s-1$. Тогда с одной стороны,

$$(a_1 + b_1)(a_2 + b_2) \cdots (a_{s-1} + b_{s-1}) = 1$$

а с другой стороны,

$$(a_1 + b_1)(a_2 + b_2) \cdots (a_{s-1} + b_{s-1}) = \underbrace{a_1 \cdots a_{s-1}}_{\in I_1 \cdots I_{s-1}} + \underbrace{\cdots \cdots \cdots}_{\in I_s}$$

(b) Очевидно, что $I_1 \cap \cdots \cap I_s \supseteq I_1 \cdots I_s$. Обратное включение доказывается по индукции. База индукции ($s = 1$) очевидна.
Шаг индукции: пусть $I_1 \cap \cdots \cap I_{s-1} = I_1 \cdots I_{s-1}$, тогда осталось доказать, что $I_1 \cdots I_{s-1} \cap I_s = I_1 \cdots I_{s-1} I_s$. Как мы знаем из пункта (a), $I_1 \cdots I_{s-1} + I_s = A$, тогда $A(I_1 \cdots I_{s-1} \cap I_s) = (I_1 \cdots I_{s-1} + I_s)(I_1 \cdots I_{s-1} \cap I_s) \subseteq I_1 \cdots I_{s-1} I_s$, откуда следует требуемое включение.

(c) Достаточно проверить, что $Im\ \varphi \ni (0, \dots, \underbrace{1}_{i}, \dots, 0)$. Из пункта (a) следует, что $1 = a + b$, где $a \in I_1 \cdots I_{i-1} I_{i+1} \cdots I_s,\ b \in I_i$, тогда $(0, \dots, \underbrace{1}_{i}, \dots, 0) = \varphi(a)$.

(d) Ядро гомоморфизма φ из пункта (c) равно $I_1 \cap \cdots \cap I_s$. Но $I_1 \cap \cdots \cap I_s = I_1 \cdots I_s$ (см. пункт b), поэтому из основной теоремы о гомоморфизмах следует, что $A/(I_1 \cdots I_s) \simeq A/I_1 \oplus \cdots \oplus A/I_s$. ■

Тензорное умножение

Задача 1. Пусть M – левый A-модуль, $A \rhd I$. Доказать, что существует канонический изоморфизм $A/I \underset{A}{\otimes} M \simeq M/IM$.

Доказательство.
Рассмотрим отображение

$$A/I \underset{A}{\otimes} M \to M/IM$$
$$(a + I, m) \mapsto (am + IM)$$

Как нетрудно видеть, свойство билинейности выполнено (элементы $(a + I, bm)$ и $(ab + I, m)$ переходят в $(abm + Im)$) доделать

Задача 2. Пусть $I, J \lhd A$. Выяснить, чему изоморфно тензорное произведение $A/I \underset{A}{\otimes} A/J$.

Решение.
Используем результат предыдущей задачи: $A/I \underset{A}{\otimes} A/J \simeq (A/J)/(I \cdot A/J)$. Избавимся от двойной факторизации: вместо того, чтобы сначала факторизовать A по J, а затем результат факторизовать по $I \cdot A/J$, можно сразу факторизовать по $I + J$. Таким образом, $A/I \underset{A}{\otimes} A/J \simeq A/(I + J)$. ■

Задача 3. Вычислить $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$.

Решение.
Используем результат предыдущей задачи: $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/(m\mathbb{Z} + n\mathbb{Z})$. Но $m\mathbb{Z} + n\mathbb{Z} \simeq d\mathbb{Z}$, где $d = \text{НОД}(m, n)$. Таким образом, $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \simeq d\mathbb{Z}$. ■

Задача 4. Выяснить, чему изоморфно тензорное произведение $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C}$ (рассматриваем $\mathbb{C}$ как двумерную алгебру над $\mathbb{R}$).

Решение.
Докажем, что $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C} \simeq \mathbb{C} \oplus \mathbb{C}$. В самом деле:

$$\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1) \underset{\mathbb{R}}{\otimes} \mathbb{C} \simeq \mathbb{C}[x]/(x^2 + 1) \simeq \mathbb{C}[x]/(x - i) \oplus \mathbb{C}[x]/(x + i) \simeq \mathbb{C} \oplus \mathbb{C}$$

Поясним переходы:

- $\mathbb{C} \bigotimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{R}[x]/(x^2+1) \bigotimes_{\mathbb{R}} \mathbb{C}$ следует из того, что $\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)$ – известный факт, обсуждавшийся в прошлом семестре.
- $\mathbb{R}[x]/(x^2+1) \bigotimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}[x]/(x^2+1)$ следует из того, что факторалгебра $\mathbb{R}[x]/(x^2+1)$ является векторным пространством с базисом из смежных классов одночленов $1, x$, при этом умножение в ней задается по правилу $x \cdot x = -1$. При тензорном умножении базис переходит в базис, поэтому смежные классы $1, x$ будут базисом $\mathbb{R}[x]/(x^2+1) \bigotimes_{\mathbb{R}} \mathbb{C}$ над $\mathbb{C}$, при этом на $\mathbb{R}[x]/(x^2+1) \bigotimes_{\mathbb{R}} \mathbb{C}$ можно ввести умножение на базисных элементах так же, как и в $\mathbb{C}[x]/(x^2+1)$.
- $\mathbb{C}[x]/(x^2+1) \simeq \mathbb{C}[x]/(x-i) \oplus \mathbb{C}[x]/(x+i)$ следует из пункта d задачи 6 (Китайская теорема об остатках).

Также можно было доказать, что $\mathbb{C} \bigotimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \oplus \mathbb{C}$ напрямую: базис в $\mathbb{C} \bigotimes_{\mathbb{R}} \mathbb{C}$ состоит из элементов $1 \otimes 1$, $1 \otimes i$, $i \otimes 1$, $i \otimes i$, перейдем от него к базису $e = \frac{1}{2}(1 \otimes 1 + i \otimes i)$, $f = \frac{1}{2}(1 \otimes i - i \otimes 1)$, $e' = \frac{1}{2}(1 \otimes 1 - i \otimes i)$, $f' = \frac{1}{2}(1 \otimes i - i \otimes 1)$.

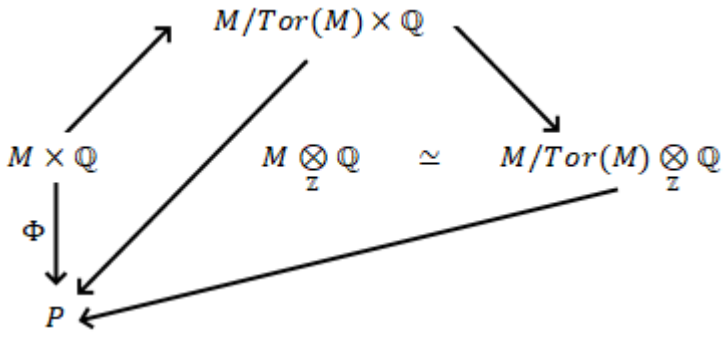
Непосредственно проверяется, что $e^2 = e$, $f^2 = -e$, $ef = f$ (аналогично для e' и f'), также $ee' = ef' = fe' = ff' = 0$, т.е. умножение в $\mathbb{C} \bigotimes_{\mathbb{R}} \mathbb{C}$ устроено так же, как и в $\mathbb{C} \oplus \mathbb{C}$. ■

Семинар 8. Модули гомоморфизмов. Нётеровы кольца. Евклидовы кольца. Кольцо гауссовых чисел.

Разбор задач домашнего задания.

Задача 2. Пусть M – абелева группа в аддитивной записи, т.е. $\mathbb{Z}$-модуль. Доказать, что $M \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \simeq M/Tor(M) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$, где $Tor(M)$ – подгруппа кручения (состоящая из всех элементов конечного порядка в M).

Доказательство.
По универсальному свойству тензорного произведения, любое билинейное над $\mathbb{Z}$ отображение $M \times \mathbb{Q} \longrightarrow P$ пропускается через отображение $M \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \longrightarrow P$. Рассмотрим отображение $M \times \mathbb{Q} \longrightarrow M/Tor(M) \times \mathbb{Q} \longrightarrow M/Tor(M) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$. Докажем, что оно удовлетворяет универсальному свойству, т.е. существует единственный гомоморфизм $\varphi\colon\ M/Tor(M) \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \longrightarrow P$, делающий следующую диаграмму коммутативной:



Рассмотрим элемент $(m,r) \in M \times \mathbb{Q}$, где $m \in Tor(M)$, $r \in \mathbb{Q}$. Так как $m \in Tor(M)$, то $\exists k \in \mathbb{N}\colon\ km = 0$. Тогда

$$\Phi(m,r) = \Phi\left(m, k \cdot \frac{r}{k}\right) = \Phi\left(km, \frac{r}{k}\right) = 0,$$

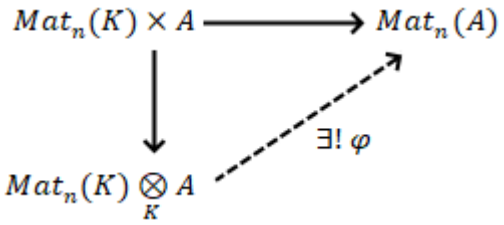
поэтому существует единственное билинейное отображение $M/Tor(M) \times \mathbb{Q} \longrightarrow P$, делающее приведенную диаграмму коммутативной. Тогда, по универсальному свойству тензорного произведения, существует единственный гомоморфизм $\varphi\colon\ M/Tor(M) \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \longrightarrow P$, делающий приведенную диаграмму коммутативной. Следовательно, $M \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \simeq M/Tor(M) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$. ■

Задача 1b. Доказать, что $Mat_n(K) \underset{K}{\otimes} A \simeq Mat_n(A)$ для любой ассоциативной алгебры A над полем K.

Доказательство.
Рассмотрим отображение

$$Mat_n(K) \times A \longrightarrow Mat_n(A)$$
$$\left(\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}, a\right) \mapsto \begin{pmatrix} ab_{11} & \cdots & ab_{1n} \\ \vdots & \ddots & \vdots \\ ab_{n1} & \cdots & ab_{nn} \end{pmatrix}$$

- оно является K-билинейным, поэтому (по универсальному свойству) существует единственный гомоморфизм φ: $Mat_n(K) \underset{K}{\otimes} A \longrightarrow Mat_n(A)$, делающий следующую диаграмму коммутативной:



Так как $E_{ij} \otimes a \mapsto aE_{ij}$ и $Mat_n(K) = \bigoplus\limits_{i,j} KE_{ij}$, то $Mat_n(A) = \bigoplus\limits_{i,j} aE_{ij}$, поэтому φ является изомомрфизмом векторных пространств. Покажем, что φ является изоморфизмом алгебр: пусть

$$M \otimes a \mapsto aM$$
$$M' \otimes a' \mapsto a'M',$$

тогда

$$MM' \otimes aa' \mapsto aa'MM'$$

- следует из правила умножения матриц. ■

Задача 1d. Доказать, что $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{H} \simeq Mat_2(\mathbb{C})$.

Доказательство.
Рассмотрим стандартную матричную модель кватернионов:

$$\mathbb{H} \simeq \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \subset Mat_2(\mathbb{C})$$

- это вещественная подалгебра (над $\mathbb{R}$) в алгебре $Mat_2(\mathbb{C})$. Изоморфизм задается на базисе следующим соответствием:

$$1 \leftrightarrow E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i \leftrightarrow I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \leftrightarrow J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad k \leftrightarrow K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Теперь рассмотрим алгебру $Mat_2(\mathbb{C})$ над полем $\mathbb{C}$. Так как пересечение $\mathbb{H}$ и $i\mathbb{H}$ тривиально и $\dim \mathbb{H} = \dim i\mathbb{H} = 4$, $\dim Mat_2(\mathbb{C}) = 8$, то

$$\mathbb{H} \oplus i\mathbb{H} = Mat_2(\mathbb{C})$$

Поэтому матрицы E, I, J, K будут являться также базисом алгебры $Mat_2(\mathbb{C})$ над полем $\mathbb{C}$. Отсюда и следует, что $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{H} \simeq Mat_2(\mathbb{C})$. ■

Модуль гомоморфизмов.

Мы обсудили конструкцию тензорного произведения модулей. Есть еще одна важная и связанная с ней конструкция – конструкция модуля гомоморфизмов.

Пусть M – (B, A)-бимодуль, N – (C, A)-бимодуль. Тогда совокупность гомоморфизмов $Hom_A(M, N)$ сама обладает естественной структурой модуля: $Hom_A(M, N)$ – это (C, B)-бимодуль: если $\varphi, \psi \in Hom_A(M, N)$, то:

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$
$$c\varphi b(m) = c\varphi(bm)$$

Аналогично, если M – (A, B)-бимодуль, N – (A, C)-бимодуль, то $Hom_A(M, N)$ – (B, C)-бимодуль:

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$
$$b\varphi c(m) = \varphi(mb)c$$

Обсудим некоторые простейшие свойства модуля гомоморфизмов (они будут в некотором смысле параллельны свойствам тензорного произведения модулей).

Свойства модуля гомоморфизмов.

1)
$$Hom(M_1 \oplus \cdots \oplus M_s, N) \simeq Hom(M_1, N) \oplus \cdots \oplus Hom(M_s, N)$$
$$\varphi = \varphi_1 \oplus \cdots \oplus \varphi_s \leftrightarrow (\varphi_1, \dots, \varphi_s)$$

2)
$$Hom(M, N_1 \oplus \cdots \oplus M_t) \simeq Hom(M, N_1) \oplus \cdots \oplus Hom(M, N_t)$$
$$\psi = \psi_1 \times \cdots \times \psi_t \leftrightarrow (\psi_1, \dots, \psi_t)$$

3)
$$Hom(A, N) \simeq N$$
$$\varphi \mapsto \varphi(1)$$

Задача. Найти:

- $Hom(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$
- $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$
- $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$

Решение.
$Hom(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ - по свойству 3).

$Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \{0\}$ – так как все элементы в $\mathbb{Z}/m\mathbb{Z}$ имеют конечный порядок, то при гомоморфизме они должны переходить в 0 (как единственный элемент конечного порядка в $\mathbb{Z}$).

$Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(m,n)\mathbb{Z}$. В самом деле, при гомоморфизме порождающий элемент $\bar{1}_m$ группы $\mathbb{Z}/m\mathbb{Z}$ переходит в элемент $\bar{k}_n$ группы $\mathbb{Z}/n\mathbb{Z}$ такой, что $m\bar{k}_n = \bar{0}_n$, откуда следует, что $mk \vdots n \Leftrightarrow k \vdots \frac{n}{(m,n)} = n_0$. Тогда $ord\,(\bar{n}_0)_n = (m,n)$ – при гомоморфизме образы порождающего элемента группы $\mathbb{Z}/m\mathbb{Z}$ образуют в $\mathbb{Z}/n\mathbb{Z}$ циклическую группу порядка (m,n). ■

4)

$$Hom\big(M, Hom(N,P)\big) \cong \{M \times N \to P, \text{билинейных}\} \simeq Hom(M \otimes N, P)$$

Нётеровы кольца.

Коммутативный случай: одной из основных теорем, позволяющих строить нётеровы кольца, является теорема Гильберта о базисе идеала (доказанная на лекциях): если кольцо A нётерово, то кольцо многочленов $A[x]$ нётерово.

Задача. Доказать, что если кольцо A нётерово, то кольцо формальных степенных рядов $A[[x]]$ нётерово.

Эта задача оставляется читателю в качестве упражнения, она доказывается почти так же, как теорема Гильберта о базисе идеала (только вместо идеала старших коэффициентов для произвольного идеала нужно рассматривать идеал младших коэффициентов).

Следствие. $K[x_1, \dots, x_n]$ и $K[[x_1, \dots, x_n]]$ нётеровы (K – поле), также любое конечно порожденное кольцо / алгебра нётеровы.

Задача. Нётерово ли $C[a,b]$ – кольцо непрерывных функций на отрезке $[a,b]$?

Некоммутативный случай: нётеровость = нётеровость слева и справа. Отличие некоммутативного случая от коммутативного рассмотрим на следующем примере.

Пример. Рассмотрим кольцо некоммутативных многочленов от двух переменных $K < x, y >$. Это кольцо не нётерово слева.

В самом деле, рассмотрим идеал $I \subset K < x, y >$, порожденный одночленами $x, xy, xy^2, xy^3, \dots, xy^n, \dots$ Среди многочленов, порожденных $x, xy, xy^2, xy^3, \dots, xy^n$ нет xy^{n+1} (так как отсутствует коммутативность), следовательно, из бесконечной системы порождающих этого идеала нельзя выбрать конечную подсистему порождающих (а значит, конечной системы порождающих не существует, и I не конечно порожден). Аналогично доказывается, что $K < x, y >$ не нётерово справа. ■

Однако, теорема Гильберта о базисе идеала для некоммутативного случая формулируется и доказывается так же, как и для коммутативного. С другой стороны, кольцо $A < x >$ некоммутативных многочленов от одной переменной (т.е. если переменная x не коммутирует с коэффициентами) уже, вообще говоря, не будет нётеровым (см. пример выше). Однако, если наложить некоторое условие на умножение x на элементы из A, ситуация меняется. Например:

Пример. Рассмотрим кольцо косых многочленов (частный случай): положим $xa = ax + \partial(a)$. Из дистрибутивности умножения следует, что $\partial(a + b) = \partial(a) + \partial(b)$. Теперь воспользуемся ассоциативностью:

- $x(ab) = (ab)x + \partial(ab)$
- $x(ab) = (xa)b = \big(ax + \partial(a)\big)b = a(xb) + \partial(a)b = a\big(bx + \partial(b)\big) + \partial(a)b =$
  $= (ab)x + a\partial(b) + \partial(a)b$

Получаем $\partial(ab) = \partial(a)b + a\partial(b)$ – правило Лейбница. Такие отображения из кольца в себя (аддитивные и удовлетворяющие правилу Лейбница) называются дифференцированиями кольца.

Задача. Доказать, что если кольцо A нётерово, то кольцо косых многочленов $A < x \mid \partial >$ нётерово с той же стороны.

Задача. Доказать, что алгебра Вейля $A_n(K)$ нётерова с обоих сторон.

Евклидовы кольца.

В курсе лекций в классе нётеровых коммутативных колец мы выделили важный класс подколец – кольца главных идеалов. Вообще, можно выделить три простейших класса коммутативных (ассоциативных с единицей без делителей нуля) колец:

евклидовы кольца $\subset$ кольца главных идеалов $\subset$ факториальные кольца.

То, что выполняется включение “кольца главных идеалов $\subset$ факториальные кольца”, было доказано в курсе лекций; то, что это включение строгое, легко видеть, на примере кольца $K[x,y]$ – оно факториально, но не является кольцом главных идеалов (например, идеал I, состоящий из многочленов без свободного члена, не является главным).

Определение. Целостное кольцо A называется *евклидовым*, если задана функция (норма): $N\colon\ A\backslash\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ со свойствами:

- $N(ab) \geq N(a)$, причем равенство достигается только в том случае, если b обратим
- $\forall a \in A\ \ \forall b \in A\backslash\{0\}\ \ \exists q, r \in A$, такие что $a = bq + r$, и $N(r) < N(b)$ или $r = 0$

Докажем включение “евклидовы кольца $\subset$ кольца главных идеалов”: пусть $A \rhd I$. Рассмотрим элемент $b \in I$ с наименьшей нормой, тогда $\forall a \in I$ выполнено $a = bq + r \Longrightarrow r \in I \Longrightarrow r = 0$ (так как $N(b) = min$). Следовательно, $I = Ab$.

Примеры евклидовых колец.

- $\mathbb{Z}$, $N(k) = |k|$
- $K[x]$, $N(f) = \deg f$
- Кольцо гауссовых чисел $\mathbb{Z}[i] = \{z = x + iy \mid x, y \in \mathbb{Z}\}$: в качестве нормы выберем $N(z) = |z|^2 = z\bar{z} = x^2 + y^2$. Проверим свойства нормы:

1) $N(zw) = N(z)N(w)$ (откуда следует, что $\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$)
2) Пусть $a, b \in \mathbb{Z}[i]$ - покажем, как осуществляется деление a на b с остатком. Числа, кратные b (т.е. идеал, порожденный b) образуют подрешетку в $\mathbb{Z}[i]$:

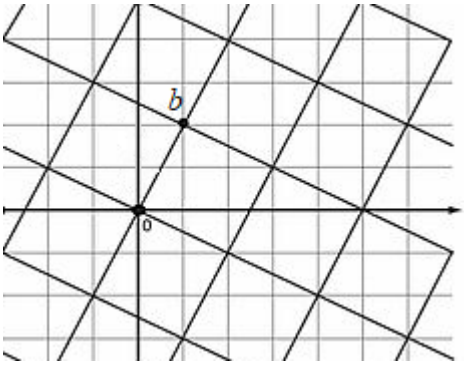


Рис. 8.1. Числа, кратные b, образуют подрешетку в $\mathbb{Z}[i]$

Число $a \in \mathbb{Z}[i]$ содержится в некотором квадрате этой подрешетки, и расстояние от a до некоторой вершины этого квадрата будет меньше стороны квадрата: $a - bq = r$,

$|r| < |b|$. Таким образом, мы нашли q, r, такие что $a = bq + r$ и $N(b) > N(r)$ или $r = 0$.

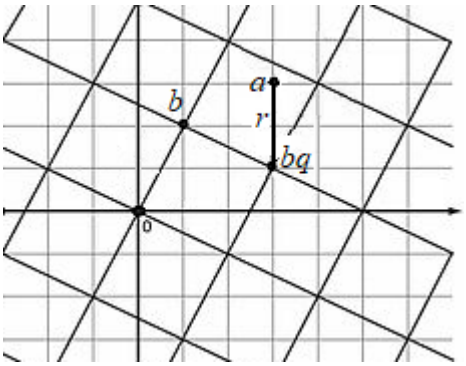


Рис. 8.2. Деление a на b с остатком в $\mathbb{Z}[i]$

Семинар 9. Пример неевклидова кольца главных идеалов. Простые элементы в кольце гауссовых чисел.

Разбор задач домашнего задания.

Задача 6. Какие из колец евклидовы?
(a) $\mathbb{Z}[\sqrt{2}]$,
(b) $\mathbb{Z}[(1+i\sqrt{3})/2]$,
(c) $\mathbb{Z}[i\sqrt{5}]$.

Решение.
(a) $\mathbb{Z}[\sqrt{2}]$ евклидово. Докажем, что в качестве нормы в $\mathbb{Z}[\sqrt{2}]$ можно рассмотреть функцию $N(a+b\sqrt{2}) = |a^2-2b^2|$. Это мультипликативная функция, поэтому первое свойство нормы выполнено, осталось проверить, что $\forall z \in \mathbb{Z}[\sqrt{2}] \quad \forall w \in \mathbb{Z}[\sqrt{2}]\backslash\{0\}$ $\exists q, r \in \mathbb{Z}[\sqrt{2}]$, такие что $z = wq + r$, и $N(r) < N(w)$ или $r = 0$.

Временно представим, что мы рассматриваем $\mathbb{Q}[\sqrt{2}]$, тогда равенство $z = wq + r$ можно записать в виде

$$\frac{z}{w} = q + \frac{r}{w},$$

где $\frac{z}{w} \in \mathbb{Q}[\sqrt{2}]$, $\frac{r}{w} \in \mathbb{Q}[\sqrt{2}]$, $q \in \mathbb{Z}[\sqrt{2}]$ и $N\left(\frac{r}{w}\right) < 1$. Таким образом, наша задача свелась к такой: определить, для любого ли элемента из $\mathbb{Q}[\sqrt{2}]$ существует аналог целой части числа. На этот вопрос уже легко ответить: для $v = \alpha + \beta\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ в качестве такого $q \in \mathbb{Z}[\sqrt{2}]$ выберем $q = a + b\sqrt{2}$, где $|\alpha - a| \le \frac{1}{2}$ и $|\beta - b| \le \frac{1}{2}$ (т.е. в качестве a выберем целое число, ближайшее к α, а в качестве b выберем целое число, ближайшее к β). Тогда $r = v - q = \gamma + \delta\sqrt{2}$, где $|\gamma|, |\delta| \le \frac{1}{2}$, следовательно, $N(r) \le \frac{1}{2}$.

(b) $\mathbb{Z}[(1+i\sqrt{3})/2]$ евклидово (доказательство аналогично доказательству того, что кольцо $\mathbb{Z}[i]$ евклидово – см. предыдущий семинар)

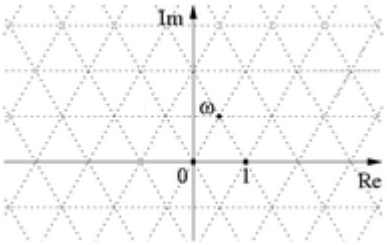


Рис. 9.1. $\mathbb{Z}[(1+i\sqrt{3})/2]$ образует треугольную решетку в $\mathbb{C}$

Деление чисел из $\mathbb{Z}\left[(1+i\sqrt{3})/2\right]$ с остатком проводится аналогично делению с остатком чисел из $\mathbb{Z}[i]$ с той лишь разницей, что теперь элементами решетки будут не квадраты, а треугольники.

(c) $\mathbb{Z}\left[i\sqrt{5}\right]$ не евклидово, так как оно не факториально: например, существует два разложения 6 на необратимые множители: $6 = 2 \cdot 3$ и $6 = (1+i\sqrt{5})(1-i\sqrt{5})$.

То, что эти множители действительно необратимы, показывает следующее рассуждение: в качестве нормы в $\mathbb{Z}\left[i\sqrt{5}\right]$ можно выбрать функцию $N\left(a+ib\sqrt{5}\right) = a^2+5b^2$, которая принимает значения $1, 4, 5, 6, 9$ ... Это мультипликативная функция, и если бы какое-то из чисел $1+i\sqrt{5}$ и $1-i\sqrt{5}$ разлагалось на множители, то 6 делилось бы на нормы этих множителей (меньшие 6) – но 6 делится только на 2 и 3, а эти значения функция N не принимает. ■

Пример не евклидова кольца главных идеалов.

На прошлом семинаре мы приводили пример факториального кольца, которое не является кольцом главных идеалов. Привести пример кольца главных идеалов, которое не является евклидовым, существенно сложнее.

Рассмотрим кольцо $A = \mathbb{R}[x,y]/I$, где $\mathbb{R}[x,y]$ – кольцо многочленов от двух переменных с вещественными коэффициентами, $I = \mathbb{R}[x,y] \cdot (x^2+y^2+1)$. Обозначая $\tilde{x}, \tilde{y}$ образы переменных x, y в кольце A при факторизации, получаем $A = \mathbb{R}[\tilde{x}, \tilde{y}]$, где $\tilde{x}^2 + \tilde{y}^2 + 1 = 0$.

1) Докажем, что A – кольцо главных идеалов. Расширим поле скаляров – рассмотрим алгебру $A \underset{\mathbb{R}}{\otimes} \mathbb{C} = \mathbb{C}[x,y]/\mathbb{C}I$, где $I = \mathbb{R}[x,y] \cdot (x^2+y^2+1)$. Над $\mathbb{C}$ многочлен $\tilde{x}^2+\tilde{y}^2$ уже разлагается на множители: $\tilde{x}^2+\tilde{y}^2 = (i\tilde{x}+\tilde{y})(-i\tilde{x}+\tilde{y})$. Обозначая $t = i\tilde{x}+\tilde{y}$, получаем, что в $A \underset{\mathbb{R}}{\otimes} \mathbb{C}$ обратный к нему элемент равен $t^{-1} = i\tilde{x}-\tilde{y} = -(-i\tilde{x}+\tilde{y})$, т.е. $A \underset{\mathbb{R}}{\otimes} \mathbb{C}$ порождено элементами t и t^{-1}:

$$A \underset{\mathbb{R}}{\otimes} \mathbb{C} \simeq \mathbb{C}[t, t^{-1}] \text{ – кольцо многочленов Лорана}$$

Но $\mathbb{C}[t,t^{-1}]$ является кольцом главных идеалов: в самом деле, пусть $J \lhd \mathbb{C}[t,t^{-1}]$, тогда $(J \cap \mathbb{C}[t]) \cdot \mathbb{C}[t,t^{-1}]^{\times} = J$, т.е. любой элемент идеала J можно представить в виде произведения элемента из кольца многочленов от одной переменной над $\mathbb{C}$ на обратимый множитель в $\mathbb{C}[t,t^{-1}]$, т.е. на элемент вида λt^k, $\lambda \in \mathbb{C}^{\times}$, $k \in \mathbb{Z}$. Но $\mathbb{C}[t]$ – главный идеал, следовательно, и J является главным идеалом.

Теперь поймем, что и A является кольцом главных идеалов. Если $J \lhd A$, то $\mathbb{C}J \lhd A \underset{\mathbb{R}}{\otimes} \mathbb{C}$, причем $\mathbb{C}J$ порожден многочленом $f(t) = (t - z_1)^{k_1} \cdots (t - z_s)^{k_s}$ (так как $A \underset{\mathbb{R}}{\otimes} \mathbb{C}$ является кольцом главных идеалов, как мы доказали выше).

Комплексное сопряжение переводит t в $\bar{t} = -t^{-1}$. Так как идеал $\mathbb{C}J$ инвариантен относительно комплексного сопряжения, то он наряду с $f(t)$ содержит и многочлен $\bar{f}(t) = (-t^{-1} - \overline{z_1})^{k_1} \cdots (-t^{-1} - \overline{z_s})^{k_s}$. При этом z_j имеет в многочлене f ту же кратность, что и $-\frac{1}{\overline{z_j}}$, т.е. корни f разбиваются на пары (при этом корни в паре не равны друг другу). Отсюда следует, что

$$f = \prod_j (t - z_j)^{k_j} (-t^{-1} - \overline{z_j})^{k_j} = \bar{f} \in A \Longrightarrow J = Af$$

Итак, A является кольцом главных идеалов.

2) Элемент $(t - z)(-t^{-1} - \bar{z})$ сопряжен сам себе, поэтому $(t - z)(-t^{-1} - \bar{z}) \in A$. Раскроем скобки:

$$(t - z)(-t^{-1} - \bar{z}) = -\bar{z}t + zt^{-1} - 1 + |z|^2 = a\tilde{x} + b\tilde{y} + c,$$

где $a, b, c \in \mathbb{R}$ и a или $b \neq 0$. Элементы p такого вида являются простыми в A. В самом деле, рассмотрим факторкольцо A/Ap. Имеем: $A/Ap \simeq \mathbb{R}[\tilde{\tilde{x}}, \tilde{\tilde{y}}]$, где $\tilde{\tilde{x}}^2 + \tilde{\tilde{y}}^2 + 1 = 0$ и $a\tilde{\tilde{x}} + b\tilde{\tilde{y}} + c = 0$. Так как из этих соотношений можно выразить $\tilde{\tilde{x}}$ через $\tilde{\tilde{y}}$ (получим квадратичную зависимость), то

$$A/Ap \simeq \mathbb{R}[\tilde{\tilde{x}}, \tilde{\tilde{y}}] \cong \mathbb{R}[x]/\mathbb{R}[x] \cdot (\alpha x^2 + \beta x + \gamma),$$

где $\alpha x^2 + \beta x + \gamma$ получается из $x^2 + y^2 + 1$ заменой $y = (-ax - c)/b$, при этом $D(\alpha x^2 + \beta x + \gamma) < 0$. Но тогда

$$A/Ap \simeq \mathbb{R}[\tilde{\tilde{x}}, \tilde{\tilde{y}}] \cong \mathbb{R}[x]/\mathbb{R}[x] \cdot (\alpha x^2 + \beta x + \gamma) \simeq \mathbb{C}$$

Следовательно, p прост (так как $\mathbb{C}$ поле). При этом других простых элементов в A нет (с точностью до умножения на обратимые), так как мы доказали, что любой идеал в A порождается произведением многочленов вида $p = a\tilde{x} + b\tilde{y} + c$, а значит, любой элемент A является произведением множителей такого вида (с точностью до обратимого множителя).

3) Докажем, что A не евклидово.

Лемма. В евклидовом кольце существует простой элемент $p \in A$, такой что каноническая проекция $\pi\colon\ A \longrightarrow A/Ap$ отображает обратимые элементы A сюръективно на обратимые элементы поля A/Ap:

$$\pi\colon\ A \longrightarrow A/Ap$$
$$\pi(A^\times) = A/Ap\backslash\{0\}$$

Доказательство.
Возьмем $p \in A\backslash A^\times$ с наименьшей нормой: $N(p) = min$. Из этого условия автоматически следует простота p (иначе норма его множителей была бы меньше p - противоречие).

Пусть $a + Ap \neq 0$, тогда a не делится на p, т.е. $a = pq + r$, где $r \neq 0$ и $N(r) < N(p)$. Отсюда следует, что $r \in A^\times$, при этом $\pi(r) = a + Ap$. ■

В нашем случае $p = a\tilde{x} + b\tilde{y} + c$ и $A/Ap \simeq \mathbb{C}$. Обратимые элементы:

$$A^\times = (A \underset{\mathbb{R}}{\otimes} \mathbb{C})^\times \cap A = \{\lambda t^k \mid \lambda \in \mathbb{C}^\times, k \in \mathbb{Z}\} \cap A = \mathbb{R}^\times$$

Так как отображение $\pi\colon\ \mathbb{R}^\times \longrightarrow \mathbb{C}$ не сюръективно, то A не евклидово.

Простые гауссовы числа.

Как мы доказали на прошлом семинаре, гауссовы числа $\mathbb{Z}[i] = \{z = x + iy \mid x, y \in \mathbb{Z}\}$ образуют евклидово кольцо, т.е. любой элемент в $\mathbb{Z}[i]$ единственным образом раскладывается в произведение простых (с точностью до их перестановки и умножения на обратимые элементы). Возникает естественный вопрос – какие элементы в $\mathbb{Z}[i]$ являются простыми. Приведем несколько вспомогательных утверждений:

1) Если $\pi \in \mathbb{Z}[i]$ простое, то $\bar{\pi}$ простое (в самом деле, операция сопряжения является автоморфизмом $\mathbb{Z}[i]$, а при автоморфизме все кольцевые свойства сохраняются, в т.ч. свойство “быть простым”).

2) Если $\pi \in \mathbb{Z}[i]$ простое, то либо $\pi \sim p \in \mathbb{N}$ - простое натуральное число, либо $\pi\bar{\pi} = N(\pi) = p \in \mathbb{N}$ - простое натуральное число (если бы p было составным, то получили бы два разложения на простые множители в $\mathbb{Z}[i]$).

3) Обратно, если $p \in \mathbb{N}$ - простое натуральное число, то либо p просто в $\mathbb{Z}[i]$, либо $p = \pi\bar{\pi}$, где π просто в $\mathbb{Z}[i]$.

Доказательство.
Пусть $p \vdots \pi$, где π просто в $\mathbb{Z}[i]$, тогда $N(p) = p^2$ делится на $N(\pi) = \pi\bar{\pi} \in \mathbb{N}$. Отсюда следует, что либо $\pi\bar{\pi} = p^2$ (и тогда $\pi \sim p \in \mathbb{N}$ и p просто в $\mathbb{Z}[i]$), либо $\pi\bar{\pi} = p$. ■

Рассмотрим три случая:

- а) $p = 2$. Тогда $p = 2 = (1 + i)(1 - i)$, при этом $(1 - i)i = 1 + i$, т.е. с точки зрения теории делимости, 2 является квадратом гауссова простого числа.

- б) $p = 4k + 3$. Тогда p просто в $\mathbb{Z}[i]$.

Доказательство.
Если $p = \pi\bar{\pi}$, где $\pi = a + bi$, то $\pi\bar{\pi} = a^2 + b^2 \equiv 0{,}1{,}2\ (mod\ 4)$ (так как $a^2 \equiv 0{,}1\ (mod\ 4)$ и $b^2 \equiv 0{,}1\ (mod\ 4)$), т.е. $p \neq 4k + 3$. ■

- в) $p = 4k + 1$. Тогда $p = \pi\bar{\pi}$, где π просто в $\mathbb{Z}[i]$.

Доказательство.
В $\mathbb{F}_p[x]$:

$$x^p - x = x(x^{2k} + \bar{1})(x^{2k} - \bar{1})$$

Многочлен $x^p - x$ разлагается на линейные множители над $\mathbb{F}_p$, следовательно, и $x^{2k} + \bar{1}$ разлагается на линейные множители над $\mathbb{F}_p$, т.е. имеет корень в $\mathbb{F}_p$: $\exists \bar{a} \in \mathbb{F}_p$: $\bar{a}^2 + \bar{1} = 0$. Это означает, что $\exists a \in \mathbb{N}$: $a^2 + 1$ делится на p. Но $a^2 + 1 = (a + i)(a - i)$ – так как $a \pm i$ не делится на p в $\mathbb{Z}[i]$, то p не является простым в $\mathbb{Z}[i]$ и $p = \pi\bar{\pi}$, где π просто в $\mathbb{Z}[i]$. ■

Семинар 10. Разложение натурального числа в сумму двух и четырех квадратов. Нормальная форма Фробениуса линейного оператора.

Разбор задач домашнего задания.

Задача 3d. Кватернион $q = a + bi + cj + dk$ называется *целым*, если либо $a, b, c, d \in \mathbb{Z}$, либо $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$. Доказать:

- (a) Множество целых кватернионов $\mathbb{H}_{int}$ – ассоциативное кольцо с единицей без делителей нуля, на котором кватернионная норма $N(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2$ принимает целые неотрицательные значения;
- (b) Для любого $q \in \mathbb{H}$ существует такой $q_0 \in \mathbb{H}_{int}$, что $N(q - q_0) < 1$;
- (c) (*деление с остатком*) для любых $q_1, q_2 \in \mathbb{H}_{int} \backslash \{0\}$ существуют такие $q_0, r \in \mathbb{H}_{int}$, что $q_1 = q_2 q_0 + r$ и $N(r) < N(q_2)$;
- (d) Все левые и правые идеалы в $\mathbb{H}_{int}$ – главные.

Доказательство.
Будем считать, что пункты a)-c) доказаны. Пусть $I \subset \mathbb{H}_{int}$ – правый идеал. Выберем $q \in I$ – ненулевой элемент наименьшей нормы. Тогда $\forall q' \in I$ выполнено: $q' = qq_0 + r$, где $N(r) < N(q)$. Так как $q' \in I$ и $qq_0 \in I$, то и $r \in I$, следовательно, $r = 0$. Отсюда следует, что I порожден q. Для левых идеалов рассуждения аналогичные. ■

Задача 4. Найти группу $\mathbb{H}_{int}^{\times}$.

Решение.
Понятно, что все элементы группы $\mathbb{H}_{int}^{\times}$ удовлетворяют условию $N(q) = 1$ (так как $qq^{-1} = 1$, откуда $N(q)N(q^{-1}) = N(1) = 1$). Это же условие является и достаточным – следует из формулы $q^{-1} = \frac{\bar{q}}{N(q)}$: если $N(q) = 1$, то $q^{-1} = \bar{q}$ и $q \in \mathbb{H}_{int}^{\times}$. Все элементы из $\mathbb{H}_{int}$ с единичной нормой перечислить несложно:

$$\mathbb{H}_{int}^{\times} = \left\{\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k\right\}$$

■

Задача 1c. С помощью разложения на простые множители в кольце $\mathbb{Z}[i]$ найти число способов разложить натуральное число n в сумму двух квадратов $n = a^2 + b^2, a, b \in \mathbb{Z}_{\geq 0}$ (порядок слагаемых не учитывается):

- (a) если n имеет натуральный простой делитель $p = 4k + 3$ нечетной кратности, то в сумму двух квадратов не разлагается;

- (b) если все натуральные простые делители вида $p = 4k + 3$ числа n имеют четную кратность, и других нечетных простых делителей нет, то n имеет единственное разложение;
- (c) в остальных случаях число способов разложения равно $\lceil (m_1 + 1) \cdots (m_s + 1)/2 \rceil$, где $m_1, \dots, m_s$ – кратности простых делителей $p_1, \dots, p_s$ вида $4k + 1$ числа n ($\lceil \cdot \rceil$ обозначает *верхнюю целую часть* числа, т.е. ближайшее сверху целое число).

Решение.
Пусть $n = 2^k \cdot q_1^{2k_1} \cdots q_t^{2k_t} \cdot p_1^{m_1} \cdots p_s^{m_s}$, где $q_i \equiv 3\ (mod\ 4)$, $p_j \equiv 1\ (mod\ 4)$. Воспользуемся тем, что разложение n в сумму двух квадратов $n = a^2 + b^2$, $a, b \in \mathbb{Z}_{\geq 0}$ можно представить в виде $n = (a + bi)(a - bi)$, т.е. в виде произведения сопряженных гауссовых чисел. Осталось вычислить, сколькими способами n можно разложить в такое произведение (с точностью до ассоциированности).

Всякое такое разложение получается из разложения n на простые сомножители в $\mathbb{Z}[i]$ путем группирования простых сомножителей. Разложение n на простые (u – некоторый обратимый множитель) выглядит так:

$$n = u \cdot (1 + i)^{2k} \cdot q_1^{2k_1} \cdots q_t^{2k_t} \cdot \pi_1^{m_1} \bar{\pi}_1^{m_1} \cdots \pi_s^{m_s} \bar{\pi}_s^{m_s}$$

Для того, чтобы из этого разложения получилось разложение $n = (a + bi)(a - bi)$, нужно простые сомножители сгруппировать по двум произведениям так, чтобы они были сопряжены друг другу (с точностью до обратимых множителей: например, $1 + i$ сопряжено самому себе с точностью до умножения на обратимый множитель $-i$). Сомножители вида $(1 + i)^k$ и $q_j^{k_j}$ распределяются по произведениям однозначно, сомножители из произведения $\pi_1^{m_1} \bar{\pi}_1^{m_1} \cdots \pi_s^{m_s} \bar{\pi}_s^{m_s}$ можно распределить так:

- $a + bi = (1 + i)^k \cdot q_1^{k_1} \cdots q_t^{k_t} \cdot \pi_j^{l_j} \bar{\pi}_j^{m_j - l_j}$
- $a - bi = (1 + i)^k \cdot q_1^{k_1} \cdots q_t^{k_t} \cdot \bar{\pi}_j^{l_j} \pi_j^{m_j - l_j}$

где $l_j = 0, \dots, m_j$.

Так как нас не интересует порядок сомножителей $a + bi$ и $a - bi$, а также учитывая, что при четном m_j число $\pi_j^{l_j} \bar{\pi}_j^{m_j - l_j}$ сопряжено самому себе, получаем, что число способов разложения равно $\lceil (m_1 + 1) \cdots (m_s + 1)/2 \rceil$. ■

Задача 5b,c. Пусть $p \in \mathbb{N}$ - простое число. Доказать:

- (a) существуют такие $n, m \in \mathbb{Z}$, что $m^2 + n^2 + 1$ делится на p (*указание*: рассмотреть уравнение $x^2 + y^2 + \bar{1} = \bar{0}$ над $\mathbb{F}_p$);
- (b) $p = N(\pi)$ для некоторого $\pi \in \mathbb{H}_{int}$ (*указание*: в обозначениях пункта 5a, для $q = mi + nj$ рассмотреть правый идеал $q\mathbb{H}_{int} + p\mathbb{H}_{int} = \pi\mathbb{H}_{int}$);
- (c) если $\pi = a + bi + cj + dk$, где $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$, то для некоторого $\rho = \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$ целый кватернион $\pi\rho$ имеет целые координаты в базисе $\{1, i, j, k\}$ и ту же норму p.

Решение.
(b) Воспользуемся пунктом (a): существуют такие $n, m \in \mathbb{Z}$, что $m^2 + n^2 + 1$ делится на p. Заметим, что $m^2 + n^2 + 1 = q\bar{q}$, где $q = 1 + mi + nj$ и докажем, что существует делитель q, норма которого равна p.

Рассмотрим правый идеал $q\mathbb{H}_{int} + p\mathbb{H}_{int}$ – из задачи 3(d) следует, что этот идеал является главным, т.е. $q\mathbb{H}_{int} + p\mathbb{H}_{int} = \pi\mathbb{H}_{int}$ для некоторого $\pi \in \mathbb{H}$. Это означает, что π делит слева q и p, т.е. $p = \pi\tau$ для некоторого $\tau \in \mathbb{H}$, откуда $N(p) = N(\pi)N(\tau)$. Так как $N(p) = p^2$, то теоретически возможны три варианта:

- $N(\pi) = 1,\ N(\tau) = p^2$. Так как $N(\pi) = 1$, то π обратим и $\pi\mathbb{H}_{int} = \mathbb{H}$, поэтому $1 \in \pi\mathbb{H}_{int}$ и $\exists\, u, v$, такие что $qu + pv = 1$. Домножая это равенство слева на $\bar{q}$, получаем $\underbrace{\bar{q}qu}_{\text{делится на } p} + \underbrace{\bar{q}pv}_{\text{делится на } p} = \bar{q} = \underbrace{1 - mi - nj}_{\text{не делится на } p}$ - противоречие.
- $N(\pi) = p^2,\ N(\tau) = 1$. Так как $N(\tau) = 1$, то τ обратим, откуда следует, что q делится на p (так как q делится на π, а $p = \pi\tau$) – противоречие.
- $N(\pi) = p,\ N(\tau) = p$ – единственный возможный вариант.

(c) Пусть $\pi = a + bi + cj + dk$, где $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$, тогда $\pi = \pi' + \rho$, где:

- $\pi' = 2(a'' + b''i + c''j + d''k) = \pi'',\ \pi'' \in \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$
- $\rho = \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$

т.е. $\pi = 2\pi'' + \rho$. Тогда $\pi\bar{\rho} = \underbrace{2\bar{\rho}\pi''}_{\in \mathbb{Z}+\mathbb{Z}i+\mathbb{Z}j+\mathbb{Z}k} + \underbrace{\rho\bar{\rho}}_{=1}$, т.е. $\pi\bar{\rho}$ имеет целые координаты в базисе $\{1, i, j, k\}$ и ту же норму p, что и кватернион π. ■

Задача 6. Доказать, что любое натуральное число n представимо в виде суммы четырех квадратов: $n = a^2 + b^2 + c^2 + d^2$, $a, b, c, d \in \mathbb{Z}_{\geq 0}$.

Доказательство.
Рассмотрим разложение n на простые множители: $n = p_1 \cdots p_N$. Каждое простое число p_i является нормой некоторого кватерниона с целыми координатами (следует из

предыдущей задачи): $p_1 = N(\pi_1), \dots, p_N = N(\pi_N)$, где $\pi_s \in \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$. Так как норма – мультипликативная функция, то

$$n = p_1 \cdots p_N = N(\pi_1 \cdots \pi_N) \in \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$$

■

Нормальная форма Фробениуса линейного оператора.

Из основной теоремы о структуре конечно порожденных модулей над кольцом главных идеалов (см. курс лекций, лекцию №9): следует, что матрица любого линейного оператора при подходящем выборе базиса имеет специальный вид (т.н. нормальная форма Фробениуса – см. курс лекций, лекцию №10). Напоминание:

Пусть V – векторное пространство над полем K, $\dim V = n < \infty$. 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 лекции №9 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).

Пусть $(e_1, \dots, e_n)$ – базис V, и $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$ – матрица оператора $\mathcal{A}$ в этом базисе. $g_1, \dots, g_m$ ищем, приводя матрицу $xE - A$ квазиэлементарными преобразованиями к диагональному виду $\begin{pmatrix} g_1(x) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & g_n(x) \end{pmatrix}$, $g_i \mid g_{i+1}$.

Пример. Найти нормальную форму Фробениуса оператора, заданного в базисе (e_1, e_2, e_3) матрицей

$$A = \begin{pmatrix} 2 & -2 & 1 \\ 1 & 0 & 1 \\ -2 & 1 & -2 \end{pmatrix}$$

Решение.
Приведем матрицу $xE - A$ квазиэлементарными преобразованиями к диагональному виду:

$$xE - A = \begin{pmatrix} x-2 & -2 & -1 \\ -1 & x & -1 \\ 2 & -1 & x+2 \end{pmatrix} \sim \begin{pmatrix} 0 & x^2-2x+2 & 1-x \\ -1 & x & -1 \\ 0 & 2x-1 & x \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} -1 & x & -1 \\ 0 & 2x-1 & x \\ 0 & x^2-2x+2 & 1-x \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2x-1 & x \\ 0 & x^2-2x+2 & 1-x \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 2x-1 \\ 0 & 1-x & x^2-2x+2 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 2x-1 \\ 0 & 1 & x^2+1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x^2+1 \\ 0 & 0 & -x^3+x-1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^3-x+1 \end{pmatrix}$$

Нормальная форма Фробениуса:

$$A' = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

■

Из основной теоремы о структуре конечно порожденных модулей над кольцом главных идеалов следует, что $g_n(x) = \mu_{\mathcal{A}}$ – минимальный многочлен оператора $\mathcal{A}$, также на лекциях отмечалось (без доказательства), что $g_1 \cdots g_n = \chi_{\mathcal{A}}$ – характеристический многочлен оператора $\mathcal{A}$. Докажем этот факт.

При приведении матрицы $xE - A$ квазиэлементарными преобразованиями к диагональному виду, $\det(xE - A) = \chi_{\mathcal{A}}(x)$ умножается на ненулевую константу λ, т.е. имеет место равенство $\lambda\chi_{\mathcal{A}}(x) = g_1 \cdots g_n$. Так как старший коэффициент каждого g_i равен 1, то и у многочлена $g_1 \cdots g_n$ старший коэффициент равен 1. Но у $\chi_{\mathcal{A}}(x)$ старший коэффициент также равен 1 (по определению), поэтому $\lambda = 1$.

Нормальная форма Фробениуса над конечным полем.

Число линейных операторов над конечным полем F в конечномерном векторном пространстве V конечно (равно q^{n^2}, где $q = |F|, n = \dim V$). Поймем, на сколько классов подобия разбиваются все такие линейные операторы (два линейных оператора называются подобными, если существуют базисы V, в которых их матрицы совпадают). Обсудим частный случай: $V = (\mathbb{F}_2)^3$.

Задача. Сколько существует классов подобия линейных операторов в $V = (\mathbb{F}_2)^3$?

Решение.
У подобных операторов одинаковые формы Фробениуса, и наоборот – операторы, имеющие одинаковые формы Фробениуса, являются подобными. Поэтому задача сводится к подсчету возможных нормальных форм Фробениуса.

Варианты расположения инвариантных множителей (индекс означает степень):

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & g_3 \end{pmatrix}, \quad \begin{pmatrix} 1 & & \\ & g_1 & \\ & & g_2 \end{pmatrix}, \quad \begin{pmatrix} g_1 & & \\ & f_1 & \\ & & h_1 \end{pmatrix}$$

- Так как каждый последующий инвариантный множитель должен делиться на предыдущий, то либо $g_1 = f_1 = h_1 = x$, либо $g_1 = f_1 = h_1 = x + 1$.
- $g_2 = g_1^2$, либо $g_2 = g_1 f_1$. Получаем четыре варианта:
  - $g_1 = x, g_2 = x^2$
  - $g_1 = x, g_2 = x(x + 1)$
  - $g_1 = x + 1, g_2 = (x + 1)^2$
  - $g_1 = x + 1, g_2 = x(x + 1)$
- Всего существует $2^3 = 8$ вариантов выбора g_3 (все многочлены третьей степени над $\mathbb{F}_2$)

Всего получаем $2 + 4 + 8 = 14$ классов подобия. ■

Семинар 11. Классификация двумерных коммутативных ассоциативных алгебр над $\mathbb{C}$. Представления конечномерных ассоциативных алгебр.

Разбор задач домашнего задания.

Задача 2. Пусть $M = F/N$ – фактормодуль свободного модуля F с базисом $f_1, \dots, f_n$ над кольцом главных идеалов A по подмодулю N, порожденному элементами $n_j = a_{1j}f_1 + \dots + a_{nj}f_n,\ j = 1, \dots, k$ и $u_1, \dots, u_m \in A$ – инвариантные множители модуля M. Доказать, что произведение $u_1, \dots, u_r$ равно наибольшему общему делителю всех миноров порядка r матрицы (a_{ij}).

Доказательство.
Как мы знаем, матрицу (a_{ij}) можно квазиэлементарными преобразованиями привести к виду

$$\begin{pmatrix} u_1 & \cdots & 0 & \cdots & \cdots & 0 \\ \cdots & \ddots & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & u_m & \cdots & \cdots & \vdots \\ \cdots & \cdots & \cdots & 0 & \cdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

Для этой матрицы утверждение задачи очевидно. Осталось доказать, что при квазиэлементарных преобразованиях НОД всех миноров порядка r не меняется.

Поймем, что происходит с минорами данного порядка при квазиэлементарных преобразованиях матриц. Рассмотрим две произвольные строки в матрице (a_{ij}) – без ограничения общности можно считать, что это строки m_i и m_{i+1}. При замене каждой из этих строк на их линейную комбинацию ($am_i + bm_{i+1}$ и $cm_i + dm_{i+1}$ соответственно, так что $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \in A^\times$) возможны три варианта:

- если минор не задевает строки m_i и m_{i+1}, то он не меняется
- если минор задевает обе строки m_i и m_{i+1}, то он умножится на $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \in A^\times$
- если минор задевает одну из строк m_i или m_{i+1}, то он раскладывается в сумму двух миноров по этой строке. Пара миноров, отличающихся пересечением с m_i или m_{i+1}, переходит в пару линейных комбинаций этих миноров с коэффициентами a, b, c, d.

НОД всех миноров порядка r порождает идеал, порожденный этими минорами (так как A является кольцом главных идеалов). Но при перечисленных выше преобразованиях этот идеал не меняется, следовательно, и НОД всех миноров порядка r не меняется. ■

Классификация конечномерных ассоциативных алгебр.

Одномерные ассоциативные алгебры.

Как мы знаем, для того, чтобы задать умножение любых элементов алгебры, достаточно указать, как перемножаются базисные элементы, т.е. задать структурные константы. В одномерном случае базис состоит из одного элемента e, и умножение в алгебре полностью определяется тем, как он умножается сам на себя:

$$e^2 = \lambda e, \quad \lambda \in K$$

Посмотрим, при каких λ получаются изоморфные алгебры: сделаем замену $e \mapsto e' = \mu e$. Тогда

$$(e')^2 = \mu^2 e^2 = \mu^2 \lambda e = \lambda \mu e'$$

- Если $\lambda = 0$, то получаем алгебру с нулевым умножением: $e^2 = 0$. Например: $A \simeq xK[x]/x^2K[x] \simeq \left\{\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}\right\}$.
- Если $\lambda \neq 0$, то выберем $\mu = \frac{1}{\lambda}$ и получим алгебру с умножением $(e')^2 = e'$. В этом случае $A \simeq K$.

Таким образом, любая одномерная алгебра изоморфна одной из этих двух. ■

Двумерные коммутативные ассоциативные алгебры над $\mathbb{C}$.

Мы не будем полностью классифицировать двумерные ассоциативные алгебры (хоть это и можно сделать), и ограничимся случаем $K = \mathbb{C}$, причем коммутативным.

Примеры:

- $\mathbb{C} \oplus \mathbb{C} \simeq \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}$
- алгебра с нулевым умножением $\simeq \mathbb{C}[x,y]_{\geq 1}/\mathbb{C}[x,y]_{\geq 2} \simeq \left\{\begin{pmatrix} 0 & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}$
- $\mathbb{C}[x]/x^2\mathbb{C}[x]$

Пусть A – коммутативная ассоциативная алгебра над $\mathbb{C}$ с базисом e, f. Структурные константы:

$$e^2 = \alpha e + \beta f$$

$$f^2 = \gamma e + \delta f$$
$$ef = \lambda e + \mu f$$

Рассмотрим регулярное представление A на самой себе:

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

Посмотрим, как может быть устроено ядро этого гомоморфизма:

- Если $Ker\,\mathcal{L} = A$, то A – алгебра с нулевым умножением: $e^2 = f^2 = ef = 0$. Обозначая $\mathbb{C}_0$ – одномерную алгебру с нулевым умножением, получаем

$$A = A_1 = \mathbb{C}_0^2$$

- Если $Ker\,\mathcal{L}$ - одномерная подалгебра: $Ker\,\mathcal{L} = \mathbb{C}e$, то выберем базис e, f – в нем умножение будет устроено так:

$$e^2 = ef = 0$$
$$f^2 = \alpha e + \beta f,\ \ (\alpha, \beta) \neq (0,0)$$

Если $\beta \neq 0$, то заменим f на $\frac{f}{\beta}$, т.е. можно считать, что $\beta = 1$. Далее, заменим f на $f' = f + \alpha e$, тогда $(f')^2 = f^2 = f'$ и в новом базисе (штрихи не используем, чтобы не загромождать запись):

$$e^2 = ef = 0$$
$$f^2 = f$$

Получаем

$$A = A_2 = \mathbb{C}_0 \oplus \mathbb{C}$$

Если $\beta = 0$, $\alpha \neq 0$, то заменим e на αe, тогда

$$e^2 = ef = 0$$
$$f^2 = e$$

Получаем

$$A = A_3 = x\mathbb{C}[x]/x^3\mathbb{C}[x]$$

- Если $Ker\,\mathcal{L} = \{0\}$, то $A \hookrightarrow Mat_2(\mathbb{C})$. Выясним, какие бывают двумерные коммутативные подалгебры в $Mat_2(\mathbb{C})$.

Как мы знаем из линейной алгебры, любые два коммутирующих линейных оператора имеют общий собственный вектор (так как собственное подпространство одного оператора будет инвариантным подпространством для другого).

Коммутирующие операторы e и f имеют вид $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, и можно считать, что хотя бы один из этих операторов имеет ненулевое собственное значение (иначе диагональные элементы, которые в этом случае равны собственным значениям, равны нулю, и рассматриваемая алгебра одномерна).

Пусть $e = \begin{pmatrix} \lambda & * \\ 0 & * \end{pmatrix}$. Рассмотрим два случая:

- если $e = \begin{pmatrix} \lambda & * \\ 0 & \mu \end{pmatrix}$, где $\lambda \neq \mu$, то (так как e и f коммутируют), e будет иметь вид $e = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, а f будет иметь вид $f = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$. В этом случае
$$A = A_4 = \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\} \simeq \mathbb{C} \oplus \mathbb{C}$$
- если все операторы в A имеют одинаковые собственные значения, т.е. $e = \begin{pmatrix} \lambda & \mu \\ 0 & \lambda \end{pmatrix}$, $f = \begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix}$, тогда $A \subseteq \left\{\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}\right\}$, откуда следует, что
$$A = A_5 = \left\{\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}\right\} \simeq \mathbb{C}[x]/x^2\mathbb{C}[x]$$

Таким образом, с точностью до изоморфизма имеется всего 5 коммутативных двумерных алгебр над $\mathbb{C}$. ■

Представления конечномерных ассоциативных алгебр.

Когда мы рассматриваем линейное представление некоторой алгебры, т.е. гомоморфно отображаем ее в алгебру линейных операторов, информация о исходной алгебре может теряться, так как у соответствующего гомоморфизма может быть ненулевое ядро. Введем новый термин:

Определение. Представление $\mathcal{R}$ называется *точным*, если $Ker\ \mathcal{R} = \{0\}$.

Задача 1. Доказать, что у каждой конечномерной алгебры существует точное конечномерное линейное представление.

Доказательство.
Заметим, что регулярное представление $\mathcal{L}\colon A \longrightarrow L(A)$ точно, если $1 \in A$. В самом деле: если $a \in Ker\ \mathcal{L}$, то $\mathcal{L}(a) = 0$, а значит, $\mathcal{L}(a) \cdot 1 = 0 \Leftrightarrow a \cdot 1 = a = 0$.

Если A не содержит единицу, то воспользуемся конструкцией присоединения единицы: рассмотрим алгебру $\tilde{A} = A \oplus K$, для которой, как мы доказали выше, регулярное представление $\tilde{\mathcal{L}}\colon \tilde{A} \longrightarrow L(\tilde{A})$ точно. Тогда и представление $\mathcal{R} = \tilde{\mathcal{L}}\big|_A\colon A \hookrightarrow L(\tilde{A})$ точно. ■

Задача 2. Пусть $\mathcal{R}$: $A \longrightarrow L(V)$ – линейное представление нильпотентной конечномерной ассоциативной алгебры. Доказать, что при некотором выборе базиса в V соответствующее матричное представление $R(A)$ будет задаваться (верхними) нильтреугольными матрицами.

Доказательство.
Воспользуемся леммой из курса лекций (см. курс лекций “Алгебра-4”, лекция 12, лемма 1): алгебра A нильпотентна $\Longrightarrow \exists n \in \mathbb{N}$: $\forall a_1, \dots, a_n \in A$ выполнено $a_1 \cdots a_n = 0$.

Расмотрим цепочку подпространств $V \supseteq AV \supseteq A^2V \supseteq \cdots \supseteq A^nV = \{0\}$ и заметим, что если $A^kV = A^{k+1}V$, то $A^{k+1}V = A^{k+2}V = \cdots$. Так как $A^nV = \{0\}$, то цепочка устроена таким образом: $V \supset AV \supset A^2V \supset \cdots \supset A^{m+1}V = \{0\}$.

Теперь выберем базис V, согласованный с этой цепочкой подпространств – в этом базисе $\forall a \in A$:

$$R(a) = \left(\begin{array}{c|c|c|c} 0 & * & \cdots & * \\ \hline 0 & \ddots & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & * \\ \hline 0 & \cdots & 0 & 0 \end{array}\right)$$

■

Задача 3. Доказать, что у нильпотентной алгебры существует единственное неприводимое представление; оно одномерно.

Доказательство.
Воспользуемся предыдущей задачей: $V \supseteq Ke_1$ – инвариантное подпространство. Так как $\mathcal{R}$ неприводимо, то $V = Ke_1$, т.е. $\mathcal{R}$ одномерно, и все операторы в нем действуют нулевым образом – такое представление единственно. ■

Задача 4. Вычислить стандартное скалярное умножение в $A = Mat_n(K)$.

Решение.
Напоминание: рассмотрим левое регулярное представление

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

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

Пространство $Mat_n(K)$ раскладывается в прямую сумму: $Mat_n(K) = V_1 \oplus \cdots \oplus V_n$, где V_i – инвариантное подпространство, состоящее из матриц, у которых все столбцы, кроме i-ого, нулевые. Значит,

$$\mathcal{L} \simeq \underbrace{\mathcal{R} \oplus \cdots \oplus \mathcal{R}}_{n \text{ слагаемых}},$$

где $\mathcal{R}$ – стандартное представление $Mat_n(K)$ в K^n. Тогда

$$(a \mid b) = tr\big(\mathcal{L}(a)\mathcal{L}(b)\big) = tr\ \mathcal{L}(ab) = n \cdot tr\ \mathcal{R}(ab) = n \cdot tr(ab)$$

■

На лекциях мы доказали следующую теорему (см. теорему в лекции 12): если $char\ K = 0$, то $Rad(A) = A^{\perp}$ - ядро стандартного скалярного умножения. Покажем, что он неверна, если характеристика поля положительна. Пусть $char\ K = p > 0$ – рассмотрим $A = Mat_p(K)$, тогда $(\cdot \mid \cdot) = 0$ и $Rad(A) = \{0\}$.

Семинар 12. Стандартное скалярное умножение на простом расширении поля. Тензорное произведение полупростых алгебр.

Разбор задач домашнего задания.

Задача 1. Перечислить с точностью до изоморфизма все двумерные коммутативные ассоциативные алгебры над полем $\mathbb{R}$.

Решение.
На прошлом семинаре мы классифицировали все двумерные коммутативные ассоциативные алгебры над $\mathbb{C}$. Если $Ker\ \mathcal{L} \neq \{0\}$, то случаи $\mathbb{R}$ и $\mathbb{C}$ рассматриваются аналогично.

Если $Ker\ \mathcal{L} = \{0\}$, то $A \hookrightarrow Mat_2(\mathbb{R})$, и нужно рассмотреть три случая (а не два, как мы рассматривали для поля $\mathbb{C}$): первые два случая (когда в A существует оператор, имеющий различные собственные значения, и когда в A существует оператор, у которого собственные значения совпадают, и они вещественны) рассматриваются так же, как и для поля $\mathbb{C}$.

Если в A существует оператор, у которого нет вещественных собственных значений, тогда его комплексные собственные значения сопряжены: обозначим их $\alpha + i\beta$ и $\alpha - i\beta$. Как известно из линейной алгебры, существует базис, в котором матрица такого оператора имеет вид $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} = \gamma \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$ для некоторого φ, т.е. это оператор, являющийся композицией гомотетии с коэффициентом γ и поворота на угол φ (также можно вспомнить, что комплексные числа вкладываются в $Mat_2(\mathbb{R})$ как раз с помощью матриц вида $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$, и применение оператора с такой матрицей соответсвует умножению на $\alpha + i\beta$).

Но операторы поворота коммутируют только с операторами поворота и гомотетии, поэтому если в A существует оператор, у которого нет вещественных собственных значений, и A коммутативна, то A – это алгебра, состоящая из всех поворотных гомотетий, или, что то же самое, алгебра, изоморфная $\mathbb{C}$ (как алгебра над $\mathbb{R}$). ■

Задача 6a,b. Доказать, что радикал конечномерной ассоциативной алгебры A с единицей совпадает с пересечением:
(a) всех максимальных левых идеалов;
(b) всех максимальных правых идеалов.

Решение.
Пусть $A \supset N$ – максимальный левый идеал. Рассмотрим $V = A/N$ – простой A-модуль и заметим, что $Ann(v_0) = N$, где $v_0 = 1 + N$. Обратно, пусть V – простой модуль, рассмотрим произвольный ненулевой вектор $v \in V$, тогда $Av = V$. Таким образом, любой простой модуль порождается любым своим ненулевым вектором (как циклический модуль) и $N = Ann(v) \subset A$ – максимальный левый идеал, так как $V = Av \simeq A/N$.

Таким образом, максимальные левые идеалы – это то же самое, что аннуляторы элементов в простых модулях. Пересечение аннуляторов всех элементов в простом модуле дают ядро представления A в этом модуле, потому пересечение всех максимальных левых идеалов совпадает с пересечением всех ядер неприводимых представлений A.

Для доказательства пункта (b) достаточно перейти к противоположному кольцу. ■

Задача 7. Вычислить матрицу стандартного скалярного умножения алгебры $\mathbb{C}$ над $\mathbb{R}$ в базисе $(1, i)$.

Решение.

$$\mathcal{L}(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathcal{L}(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Стандартное скалярное умножение: $(a \mid b) = tr\big(\mathcal{L}(a)\mathcal{L}(b)\big) = tr\ \mathcal{L}(ab)$. Получаем:

- $(1 \mid 1) = tr\ \mathcal{L}(1) = 2$
- $(1 \mid i) = tr\ \mathcal{L}(i) = 0$
- $(i \mid i) = tr\ \mathcal{L}(-1) = -2$

Тогда матрица стандартного скалярного умножения:

$$\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$$

■

Стандартное скалярное умножение.

Рассмотрим алгебру $A = K[x]/K[x] \cdot f$, где $f(x) = x^n + c_1 x^{n-1} + \cdots + c_n$. Опишем стандартное скалярное умножение на A в базисе из смежных классов $(1, x, x^2, \dots, x^{n-1})$. Имеем:

$$([x^k] \mid [x^l]) = tr\Big(\mathcal{L}([x^k])\mathcal{L}([x^l])\Big) = tr\ \mathcal{L}([x^k][x^l]) = tr\ \mathcal{L}([x^{k+l}])$$

Осталось вычислить $\mathcal{L}([x^m]) = \big(\mathcal{L}([x])\big)^m$. Обозначим $\mathcal{L}([x]) = \mathcal{B}$ - оператор умножения на x. Несложно видеть, что $f = \mu_{\mathcal{B}} = \chi_{\mathcal{B}}$. Обозначим $\lambda_1, \dots, \lambda_n$ – корни f в поле разложения = собственные значения $\mathcal{B}$, тогда

$$tr\ \mathcal{L}([x^m]) = \lambda_1^m + \dots + \lambda_n^m = s_m(\lambda_1, \dots, \lambda_n) \in K$$

Тогда матрица стандартного скалярного умножения в базисе $(1, x, x^2, \dots, x^{n-1})$ имеет вид:

$$\begin{pmatrix} s_0 & s_1 & \cdots & \cdots & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & \cdots & \cdots & s_n \\ s_2 & s_3 & \ddots & \cdots & \cdots & s_{n+1} \\ \cdots & \cdots & \cdots & s_{i+j-2} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \ddots & \vdots \\ s_{n-1} & s_n & s_{n+1} & \cdots & \cdots & s_{2n-2} \end{pmatrix}$$

Задача. Доказать, что скалярное умножение $(\cdot \mid \cdot)$ невырождено тогда и только тогда, когда f сепарабелен.

Решение.
В матрице стандартного скалярного умножения, приведенной выше, на $(i+j)$-ом месте стоит элемент $s_{i+j-2} = \lambda_1^{i+j-2} + \dots + \lambda_n^{i+j-2}$, что приводит к мысли о представлении этой матрицы в виде произведения двух матриц:

$$\begin{pmatrix} & & \vdots & \\ \cdots & \cdots & s_{i+j-2} & \cdots \\ & & \vdots & \end{pmatrix} = \begin{pmatrix} & & \vdots & \\ \lambda_1^{i-1} & \lambda_2^{i-1} & \cdots & \lambda_n^{i-1} \\ & & \vdots & \end{pmatrix} \begin{pmatrix} & & \lambda_1^{j-1} & \\ & & \lambda_2^{j-1} & \\ \cdots & \cdots & \vdots & \cdots \\ & & \lambda_n^{j-1} & \end{pmatrix}$$

В первом сомножителе несложно узнать определитель Вандермонда, а второй сомножитель получается из первого транспонированием, поэтому определитель матрицы стандартного скалярного умножения равен квадрату определителя Вандермонда, который, в свою очередь, равен дискриминанту многочлена f:

$$\det = \prod_{i<j} \big(\lambda_i - \lambda_j\big)^2 = D(f)$$

Этот определитель отличен от нуля тогда и только тогда, когда среди корней многочлена f нет одинаковых, т.е. когда f сепарабелен. ■

Упражнение. Пусть $K = \mathbb{R}$, f сепарабелен. Доказать, что количество вещественных корней f равно $p - q$, где p, q – индексы инерции $(\cdot \mid \cdot)$.

Простые и полупростые алгебры.

На лекциях была доказана (см. лекцию 14) 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.

Возникает естественный вопрос – являются ли n и D инвариантами алгебры A, т.е. можно ли охарактеризовать n и D в терминах алгебры A?

Как мы знаем из лекций (см. лекцию 14, предложение 1), существует единственный простой A-модуль $V = D^n$. Воспользуемся тем, что $D = (End_A V)^{op}$ и рассмотрим произвольный эндоморфизм этого модуля, т.е. линейное отображение $\varphi\colon V \longrightarrow V$, обладающее свойством $\varphi(av) = a\varphi(v)$. Докажем, что φ – это умножение справа на некоторый элемент тела D, т.е. $\exists \delta \in D \ \ \forall v \in V\colon \ v\varphi = v\delta$, другими словами, невозможно равенство $v\varphi = w \notin vD$.

В самом деле, рассмотрим оператор, удовлетворяющий условию $av = v$, $aw = v$, тогда равенство $(av)\varphi = a(v\varphi)$ превратится в $w = v$ – противоречие. Таким образом, $v\varphi = v\delta$, где $\delta \in D$ может зависеть от v – покажем, что этой зависимости нет, т.е. если выполнено $w\varphi = w\delta'$, то $\delta = \delta'$. Для этого рассмотрим оператор, удовлетворяющий условию $av = w$, тогда равенство $(av)\varphi = a(v\varphi)$ превратится в $w\delta' = w\delta$, откуда $\delta = \delta'$.

Таким образом, D является инвариантом алгебры A. Число n также является инвариантом алгебры A, так как n – это размерность модуля $V = D^n$ над телом $D = (End_A V)^{op}$.

Тензорное произведение полупростых алгебр.

Из теоремы Веддербёрна-Артина вытекает, что прямая сумма полупростых алгебр также будет полупростой алгеброй. Посмотрим, что можно сказать про тензорное произведение $A \underset{K}{\otimes} B$ полупростых алгебр A и B.

Задача 1. Доказать, что $A \underset{K}{\otimes} B$ полупроста, если $char\ K = 0$.

Поймем, как устроено $A \underset{K}{\otimes} B$. Из теоремы Веддербёрна-Артина следует, что $A \simeq Mat_{n_1}(D_1) \oplus \cdots \oplus Mat_{n_s}(D_s)$, и $B \simeq Mat_{m_1}(E_1) \oplus \cdots \oplus Mat_{m_t}(E_t)$ где D_j, E_j – конечномерные алгебры с делением над K. Тогда

$$A \underset{K}{\otimes} B \simeq \underset{i,j}{\oplus} \left(Mat_{n_i}(D_i) \underset{K}{\otimes} Mat_{m_j}(E_j) \right)$$

Осталось разобраться, как устроено тензорное произведение матричных алгебр $Mat_n(D) \underset{K}{\otimes} Mat_m(E)$. Воспользуемся тем, что $Mat_n(D) \simeq Mat_n(K) \underset{K}{\otimes} D$, а $Mat_m(E) \simeq Mat_m(K) \underset{K}{\otimes} E$. Тогда

$$Mat_n(D) \underset{K}{\otimes} Mat_m(E) \simeq \underbrace{Mat_n(K) \underset{K}{\otimes} Mat_m(K)}_{Mat_{nm}(K)} \underset{K}{\otimes} D \underset{K}{\otimes} E \simeq Mat_{nm}(D \underset{K}{\otimes} E)$$

Таким образом, вопрос сводится к тензорному произведению алгебр с делением. Более подробно обсудим этот вопрос на следующем семинаре.

Семинар 13. Центральные простые алгебры и алгебры с делением. Группа Брауэра. Обобщённые кватернионы.

Разбор задач домашнего задания.

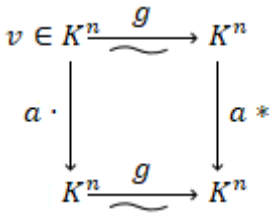
Задача 6b. Пусть K – несовершенное поле характеристики $p > 0$, $c \in K$ – элемент, не имеющий корня степени p в K, и $L = K[x]/K[x](x^p - c)$ – расширение поля K, полученное присоединением корня степени p из c. Будет ли алгебра $L \underset{K}{\otimes} L$ полупростой?

Решение.
Нет. Заметим, что $L \underset{K}{\otimes} L \simeq L[x]/L[x](x^p - c)$. Многочлен $x^p - c$ в $L[x]$ уже не является неприводимым: $x^p - c = (x - a)^p$, где a – корень степени p из c, который мы присоединили к исходному полю: $a \in L$, $a^p = c$. Понятно, что в алгебре $L[x]/L[x](x^p - c)$ есть нильпотентные элементы, например, смежный класс многочлена $(x - a)$ (несложно доказать, что $Rad\big(L[x]/L[x](x^p - c)\big) = (x - a)L[x]/(x - a)^p L[x]$). ■

Задача 3. Доказать, что все автоморфизмы алгебры $Mat_n(K)$ – внутренние, т.е. имеют вид $\varphi(x) = gxg^{-1}$ для некоторой матрицы $g \in GL_n(K)$. (*Указание*: рассмотреть φ как линейное представление алгебры $Mat_n(K)$ в пространстве K^n).

Доказательство.
Воспользуемся предложением 1 лекции 14 (конечномерная ассоциативная алгебра A полупроста ⇔ все ее конечномерные линейные представления вполне приводимы). Из него следует, что алгебра $Mat_n(K)$ имеет единственный (с точностью до изоморфизма) простой модуль K^n (со стандартным умножением $(a, v) \mapsto av$).

Рассмотрим φ как линейное представление алгебры $Mat_n(K)$ в пространстве K^n. Получаем другую структуру модуля над K^n: $*\colon (a, v) \mapsto \varphi(a)v$. Так как φ – автоморфизм, то этот модуль будет также простым, следовательно, изоморфным модулю K^n со стандартным умножением. Отсюда вытекает коммутативность следующей диаграммы:



т.е.

$$a * gv = g(av) \Leftrightarrow \varphi(a)gv = gav$$

Обозначим $w = gv$, тогда $v = g^{-1}w$, получим $\varphi(a)w = gag^{-1}w$, для любого $w \in K^n$, откуда следует, что $\varphi(a) = gag^{-1}$. ■

Задача 1. Пусть $f \in \mathbb{R}[x]$ – сепарабельный многочлен. Доказать, что число вещественных корней многочлена f равно $p - q$, где p и q – положительный и отрицательный индексы инерции стандартного скалярного умножения на алгебре $A = \mathbb{R}[x]/\mathbb{R}[x]f$. (*Указание*: разложить A в прямую сумму простых алгебр).

Доказательство.
На прошлом семинаре мы описали стандартное скалярное умножение на A в базисе из смежных классов $(1, x, x^2, \dots, x^{n-1})$: его матрица имеет вид

$$\begin{pmatrix} s_0 & s_1 & \cdots & \cdots & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & \cdots & \cdots & s_n \\ s_2 & s_3 & \ddots & \cdots & \cdots & s_{n+1} \\ \cdots & \cdots & \cdots & s_{i+j-2} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \ddots & \vdots \\ s_{n-1} & s_n & s_{n+1} & \cdots & \cdots & s_{2n-2} \end{pmatrix}$$

где $\lambda_1, \dots, \lambda_n$ – корни f в $\mathbb{C}$, $s_m(\lambda_1, \dots, \lambda_n) = \lambda_1^m + \cdots + \lambda_n^m$.

Пусть f имеет вещественные корни $\lambda_1, \dots, \lambda_r$, и комплексные корни $\lambda_{r+1}, \dots, \lambda_n$, тогда

$$f(x) = \prod_{i=1}^{r}(x - \lambda_i) \prod_{j=r+1}^{\frac{n-r}{2}} \left(x^2 - 2Re(\lambda_j) + |\lambda_j|^2\right)$$

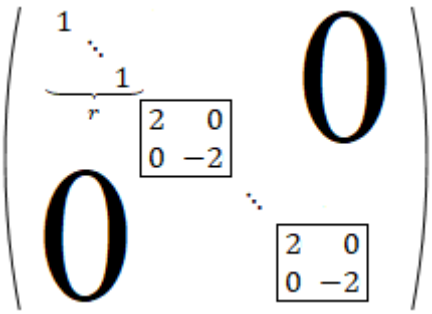
Воспользуемся разложением A в прямую сумму простых алгебр: из китайской теоремы об остатках следует, что

$$A = \mathbb{R}[x]/\mathbb{R}[x]f \simeq \left(\bigoplus_i \mathbb{R}[x]/\mathbb{R}[x](x - \lambda_i)\right) \oplus \left(\bigoplus_j \mathbb{R}[x]/\mathbb{R}[x]\left(x^2 - 2Re(\lambda_j) + |\lambda_j|^2\right)\right)$$

т.е.

$$A \simeq \mathbb{R}^r \oplus \mathbb{C}^{\frac{n-r}{2}}$$

Воспользуемся задачей 7 из прошлого семинара: матрица стандартного скалярного умножения на A в соответствующем базисе будет иметь вид



Имеем: $p = r + \frac{n-r}{2}$, $q = \frac{n-r}{2}$ и $p - q = r$, т.е. число вещественных корней многочлена f.

■

Центральные простые алгебры и алгебры с делением.

Продолжим обсуждение вопроса, начатого ранее (см. конец прошлого семинара) – перейдем к рассмотрению тензорного произведения алгебр с делением. Как было отмечено на прошлом семинаре, $D \underset{K}{\otimes} E$ полупроста, если $char\ K = 0$, но не обязательно проста. Если же $char\ K > 0$, то $D \underset{K}{\otimes} E$ не обязательно полупроста.

Однако, иногда можно гарантировать полупростоту и даже простоту тензорного произведения алгебр с делением – это справедливо для центральных алгебр.

Определение. Алгебра A с единицей над полем K называется *центральной*, если $Z(A) = K$, т.е. центр A совпадает с полем K.

Пример. $Mat_n(K)$ – центральная простая алгебра.

Задача 2. $Mat_n(D)$ центральна $\Leftrightarrow$ D – центральная алгебра с делением.

Утверждение 1. Пусть D, E – алгебры с делением, D центральна. Тогда $D \underset{K}{\otimes} E$ – простая алгебра, причем $Z\left(D \underset{K}{\otimes} E\right) = 1 \underset{K}{\otimes} Z(E) \simeq Z(E)$.

Доказательство.
Пусть $D \underset{K}{\otimes} E \rhd I \neq \{0\}$. Всякий ненулевой элемент $c \in I$ имеет вид:

$$c = \delta_1 \otimes \varepsilon_1 + \cdots + \delta_r \otimes \varepsilon_r$$

Пусть c – минимальный ненулевой элемент I. Тогда $\{\delta_1, \dots, \delta_r\}$ и $\{\varepsilon_1, \dots, \varepsilon_r\}$ линейно независимы над K (иначе получили бы более короткое разложение). Так как I – идеал, то можно заменить c на $c(\delta_1^{-1} \otimes 1) \in I$, т.е. без ограничения общности можно считать, что $\delta_1 = 1$.

Пусть $\delta \in D$. Рассмотрим $[c, \delta \otimes 1]$. Имеем:

$$[c, \delta \otimes 1] = c(\delta \otimes 1) - (\delta \otimes 1)c = [\delta_2, \delta] \otimes \varepsilon_2 + \cdots + [\delta_r, \delta] \otimes \varepsilon_r \in I,$$

откуда следует, что $[c, \delta \otimes 1] = 0$ (так как r – минимальный элемент I). Тогда $[\delta_2, \delta] = \cdots = [\delta_r, \delta] = 0$ (так как $\{\varepsilon_1, \dots, \varepsilon_r\}$ линейно независимы над K), следовательно, $\delta_1 = 1, \delta_2, \dots, \delta_r \in Z(D) = K$. Так как $\{\delta_1, \dots, \delta_r\}$ линейно независимы над K, то $r = 1$, т.е. $c = 1 \otimes \varepsilon_1$.

Так как I – идеал, то можно заменить c на $c(1 \otimes \varepsilon_1^{-1}) = 1 \otimes 1 = 1 \in I$, откуда следует, что $I = D \underset{K}{\otimes} E$, т.е. алгебра $D \underset{K}{\otimes} E$ проста.

Пусть $z \in Z\left(D \underset{K}{\otimes} E\right)$, $z = \delta_1 \otimes \varepsilon_1 + \cdots + \delta_r \otimes \varepsilon_r$ – кратчайшее разложение. Имеем:

$$[z, \delta \otimes 1] = z(\delta \otimes 1) - (\delta \otimes 1)z = [\delta_1, \delta] \otimes \varepsilon_1 + \cdots + [\delta_r, \delta] \otimes \varepsilon_r = 0$$

Так как $\{\varepsilon_1, \dots, \varepsilon_r\}$ линейно независимы над K, то $[\delta_1, \delta] = \cdots = [\delta_r, \delta] = 0$, следовательно, $\delta_1, \delta_2, \dots, \delta_r \in Z(D) = K$. Так как $\{\delta_1, \dots, \delta_r\}$ линейно независимы над K, то $r = 1$, т.е. $z = \delta_1 \otimes \varepsilon_1 = 1 \otimes \varepsilon$, откуда следует, что $\varepsilon \in Z(E)$. ■

Следствие. Если D, E – центральные алгебры с делением, то $D \underset{K}{\otimes} E$ – центральная простая алгебра.

Утверждение 2. Пусть D – центральная алгебра с делением, тогда и D^{op} – центральная алгебра с делением, причем $D \underset{K}{\otimes} D^{op} \simeq Mat_n(K)$.

Доказательство.
Так как умножение в D^{op} отличается от умножения в D лишь порядком сомножителей, то $Z(D) = Z(D^{op})$ и первая часть утверждения очевидна. Докажем, что $D \underset{K}{\otimes} D^{op} \simeq Mat_n(K)$.

Воспользуемся тем, что D является (D, D)-бимодулем, т.е. левым модулем над $D \underset{K}{\otimes} D^{op}$: получаем линейное представление $\mathcal{R}$: $D \underset{K}{\otimes} D^{op} \longrightarrow L(D)$. Так как $D \underset{K}{\otimes} D^{op}$ – простая алгебра, то $Ker\, \mathcal{R} = \{0\}$, либо $Ker\, \mathcal{R} = D \underset{K}{\otimes} D^{op}$, но так как $\mathcal{R}(1 \otimes 1) = \mathcal{E}$, остается только вариант $Ker\, \mathcal{R} = \{0\}$, т.е. $\mathcal{R}$ инъективен.

Пусть $\dim_K D = n$, тогда $\dim L(D) = n^2$, также $\dim D \underset{K}{\otimes} D^{op} = n^2$, откуда следует, что $\mathcal{R}$ – изоморфизм (из совпадения размерностей). ■

Пример. $\mathbb{H} \underset{\mathbb{R}}{\otimes} \mathbb{H} \simeq Mat_4(\mathbb{R})$. Это следует из того, что $\mathbb{H}^{op} \simeq \mathbb{H}$, изоморфизм осуществляется с помощью кватернионного сопряжения $q \mapsto \bar{q}$.

Группа Брауэра.

Пусть D, E – центральные простые конечномерные алгебры с делением над K. Тогда $D \underset{K}{\otimes} E \simeq Mat_m(F)$, где F – центральная алгебра с делением, и она однозначно определена по D, E. *Группа Брауэра* $Br(K)$ состоит из классов изоморфных центральных простых конечномерных алгебр с делением над K. Групповой закон: $[D][E] = [F]$.

- Ассоциативность умножения в группе Брауэра легко вытекает из определения и ранее доказанных фактов о тензорном произведении простых алгебр (доказательство оставляется читателю в качестве упражнения).

Задача 3. Доказать ассоциативность умножения в группе Брауэра.

- Нейтральный элемент: $[K]$.
- Обратный элемент: $[D]^{-1} = [D^{op}]$.

Таким образом, $Br(K)$ – абелева группа. Она является важным инвариантом поля K.

Примеры.

- $Br(\mathbb{C}) = \{1\}$
- $Br(K) = \{1\}$, если K алгебраически замкнуто
- $Br(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \simeq \mathbb{Z}_2$ (следует из теоремы Фробениуса)

Мы не будем описывать все алгебры с делением над данным полем, но укажем класс алгебр с делением, которые являются в некотором смысле простейшими (кроме самого поля) – это обобщенные алгебры кватернионов.

Обобщенные алгебры кватернионов.

Будем считать, что $char\, K \neq 2$. Рассмотрим алгебру $D(K, \alpha, \beta)$, $\alpha, \beta \in K^\times$ – это ассоциативная алгебра с 1 над K с базисом $\{1, i, j, k\}$ и операцией умножения

$$ij = k, \qquad ji = -k, \qquad i^2 = \alpha, \qquad j^2 = \beta$$

Отсюда вытекает, что $jk = -kj$, $ki = -ik$, $k^2 = -\alpha\beta$. Отметим, что $\mathbb{H} = D(\mathbb{R}, -1, -1)$.

Задача 4. Доказать, что $D(\alpha,\beta) \simeq D(\beta,\alpha) \simeq D(\alpha\lambda^2, \beta\mu^2)$, $\forall \lambda, \mu \in K$.

Доказательство.

- $D(\alpha,\beta) \simeq D(\beta,\alpha)$ следует из правил умножения в $D(\alpha,\beta)$.
- Рассмотрим замену базиса: $i \mapsto i\lambda = i'$, $j \mapsto j\mu = j'$, тогда $i'^2 = \alpha\lambda^2$, $j'^2 = \beta\mu^2$, откуда следует, что $D(\alpha,\beta) \simeq D(\alpha\lambda^2, \beta\mu^2)$. ■

Задача 5. Доказать, что $D(1,1) \simeq Mat_2(K)$.

Задача 6. Доказать, что $D(\alpha,\beta)$ – центральная простая алгебра (из соображений размерности отсюда вытекает, что $D(\alpha,\beta) \simeq Mat_2(K)$, либо $D(\alpha,\beta)$ – алгебра с делением).

Задача 7. Доказать, что $D(\alpha,1) \simeq Mat_2(K)$.

Задача 8. Доказать, что $[D(\alpha,\beta)]^2 = [K]$ в $Br(K)$.

Семинар 14. Свойства обобщённых кватернионных алгебр. Расширение скаляров, расщепление и степень центральной алгебры с делением. Групповые алгебры, их структура.

Разбор задач домашнего задания.

Задача 3. Обосновать ассоциативность умножения в $Br(K)$.

Решение.
Пусть $[A],[B],[C] \in Br(K)$ и $([A],[B],[C]) = [R] \Leftrightarrow (A \otimes B) \otimes C \simeq Mat_l(R)$. Докажем, что $([A][B])[C] = [R]$ (так как $(A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$, отсюда будет следовать, что и $[A]([B][C]) = [R]$).

Пусть $[A][B] = [F]$, т.е. $A \otimes B \simeq Mat_n(F)$. Имеем:

$$(A \otimes B) \otimes C \simeq Mat_n(F) \otimes C \simeq Mat_n(K) \otimes \underbrace{F \otimes C}_{Mat_m(Q)} \simeq$$

$$\simeq Mat_n(K) \otimes Mat_m(Q) \simeq Mat_{nm}(K \otimes Q) \simeq Mat_{nm}(Q)$$

Так как $(A \otimes B) \otimes C \simeq Mat_l(R)$, то $Mat_{nm}(Q) \simeq Mat_l(R)$ и $Q \simeq R$. Получаем

$$([A][B])[C] = [F][C] = [Q] = [R],$$

что и требовалось. ■

Задача 4. Пусть K – поле характеристики $\neq 2$. Доказать, что:

- (a) обобщенная алгебра кватернионов $D(K, \alpha, \beta)$ – центральная простая алгебра размерности 4 (а значит, либо алгебра с делением, либо изоморфна $Mat_2(K)$);
- (b) $[D(K, \alpha, \beta)]$ – элемент порядка 2 в группе Брауэра $Br(K)$;
- (c) $D(K, 1,1) \simeq Mat_2(K)$;
- (d) $D(K, \alpha, 1) \simeq Mat_2(K)$;
- (e) как выглядят кватернионное сопряжение и кватернионная норма в $Mat_2(K)$?

Доказательство.
(a) Пусть $D(K, \alpha, \beta) \rhd I$ – ненулевой идеал, $0 \neq q = a + bi + cj + dk \in I$. Имеем:

$$[q, i] = ai + bi^2 + cji + dki - ai - bi^2 - cij - dik = -2cij - 2dik = -2ck - 2da j \in I$$

Т.е. при коммутировании с i остаются только члены с j и k. Аналогично, при коммутировании с j остаются только члены с i и k, и т.д. – отсюда можно заключить, что

$bi, cj, dk \in I$, а значит, и $a \in I$. Так как $q \neq 0$, то хотя бы одно из чисел a, b, c, d не равно нулю. Если $a \neq 0$, то $1 \in I$, а значит, $I = D(K, \alpha, \beta)$. Если $b \neq 0$, то $bi^2 = \alpha b \in I$, и мы приходим к случаю $a \neq 0$ (рассуждения для $c \neq 0$ и $d \neq 0$ аналогичны). Следовательно, алгебра $D(K, \alpha, \beta)$ проста.

Пусть $z \in Z\big(D(K, \alpha, \beta)\big)$, $z = x_1 + x_2 i + x_3 j + x_4 k$. Имеем:

$$zi = x_1 i + x_2 \alpha - x_3 k - x_4 \alpha j$$
$$iz = x_1 i + x_2 \alpha + x_3 k + x_4 \alpha j$$

Из равенства $zi = iz$, следует, что $x_3 = 0$ и $x_4 = 0$. Аналогично, из равенства $zj = jz$ следует, что $x_2 = 0$ и $x_4 = 0$. Получаем $z = x_1 \in K$, т.е. алгебра $D(K, \alpha, \beta)$ центральна.

(b) Если $D(K, \alpha, \beta) \simeq Mat_2(K)$, то $[K]$ – нейтральный элемент в $Br(K)$. Если $D(K, \alpha, \beta)$ – алгебра с делением, то воспользуемся тем, что в группе Брауэра $[D]^{-1} = [D^{op}]$, т.е. докажем, что $D(K, \alpha, \beta)^{op} \simeq D(K, \alpha, \beta)$. В качестве изоморфизма рассмотрим кватернионное сопряжение: $q = a + bi + cj + dk \mapsto \bar{q} = a - bi - cj - dk$.

(c) Искомый изоморфизм строится, например, так:

$$1 \mapsto E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$i \mapsto I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$j \mapsto J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$k \mapsto K = IJ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

(d) Как и в пункте (c), можно явно построить искомый изоморфизм, но мы решим эту задачу другим способом. Из пункта (a) следует, что если в $D(K, \alpha, \beta)$ есть необратимый элемент, то $D(K, \alpha, \beta) \simeq Mat_2(K)$. Для обобщенных кватернионов (как и для обычных) для поиска кватерниона, обратного к данному $q = a + bi + cj + dk$, воспользуемся понятием кватернионной нормы: $N(q) = q\bar{q} = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2$ – квадратичная форма на $D(K, \alpha, \beta)$. Тогда

$$N(q) \neq 0 \Leftrightarrow q^{-1} = \frac{\bar{q}}{N(q)}$$

Таким образом, вопрос о том, является ли алгебра $D(K, \alpha, \beta)$ алгеброй с делением, сводится к вопросу о том, принимает ли квадратичная форма $N(q)$ нулевые значения на ненулевых кватернионах.

Для $D(K, \alpha, 1)$:

$$N(q) = a^2 - \alpha b^2 - c^2 + \alpha d^2$$

Несложно видеть, что $N(q) = 0$, например, при $a = c = 1, b = d = 0$, т.е. для $q = 1 + j$. ■

Расширение скаляров.

Пусть $K \subseteq L$ – расширение поля K, а D – центральная алгебра с делением над K. Тогда $D \underset{K}{\otimes} L$ – простая алгебра, центральная над L, а значит, $D \underset{K}{\otimes} L \simeq Mat_m(D')$, где D' – центральная алгебра с делением над L. При этом $\dim_K D = m^2 \dim_L D'$, т.е. за счет расширения скаляров мы можем от исходной алгебры перейти к алгебре матриц над алгеброй с делением меньшей размерности (в m^2 раз). Оказывается, таким путем можно добиться того, чтобы алгебра D' стала полем.

Утверждение 1. Существует конечное расширение $K \subseteq L$, такое что $D \underset{K}{\otimes} L \simeq Mat_n(L)$.

Доказательство.
Построим вначале расширение $K \subseteq L$, такое что $D \underset{K}{\otimes} L$ имеет делители нуля. Пусть $\delta \in D$, $\delta \notin K$ – так как минимальный аннулирующий многочлен $\mu = \mu_\delta \in K[x]$ неприводим, то в качестве L можно выбрать $L = K(\lambda \mid \mu(\lambda) = 0)$. Тогда $D \underset{K}{\otimes} L \supset D$, элементу $\delta \in D$ соответствует элемент $\delta \otimes 1 \in D \underset{K}{\otimes} L$, причем $\delta \otimes 1$ имеет тот же минимальный многочлен μ над L, т.е. $\mu(\delta) = 0$. С другой стороны, $\mu(x) = (x - \lambda) f(x)$, откуда $\mu(\delta) = (\delta - \lambda) f(\delta)$. Но $\delta - \lambda \neq 0$ и $f(\delta) \neq 0$ в силу минимальности μ, поэтому $\delta - \lambda$ и $f(\delta)$ – делители нуля.

Отсюда следует, что $D \underset{K}{\otimes} L \simeq Mat_m(D'), m > 1$, поэтому $\dim_L D' < \dim_K D$. Далее, строя расширение $L \subseteq M$, такое что $D' \underset{L}{\otimes} M \simeq Mat_p(M)$, получаем, что

$$D \underset{K}{\otimes} M = \left(D \underset{K}{\otimes} L\right) \underset{L}{\otimes} M = Mat_m(D') \underset{L}{\otimes} M = Mat_m\left(D' \underset{L}{\otimes} M\right) = Mat_{mp}(M)$$

И так далее – так как размерность на каждом шаге уменьшается, в итоге добьемся того, чтобы алгебра матриц над алгеброй с делением стала алгеброй матриц над полем. ■

Следствие. Размерность центральной алгебры с делением является полным квадратом: $\dim_K D = n^2$, число $n = \deg D$ называют степенью центральной алгебры с делением.

Определение. Поле L, такое что $D \underset{K}{\otimes} L \simeq Mat_n(L)$, называется *полем расщепления* для D.

Задача 1. Найти поле расщепления для $D(K, \alpha, \beta)$.

Задача 2. Доказать, что если L – поле расщепления для D над K, то $(L\colon K) \geq \deg D$.

Задача 3. Доказать, что если $\deg D = 2$, то $D \simeq D(K, \alpha, \beta)$ (при условии, что $char\ K \neq 2$).

Групповые алгебры.

Обсудим еще один класс полупростых алгебр – групповые алгебры конечных групп. Пусть $G = \{g_1, \dots, g_N\}$ – конечная группа, KG – ее групповая алгебра над K. Как известно, если $char\ K = 0$, или $char\ K$ не делит $|G| = N$, то KG полупроста. Докажем, что ослабить эти требования нельзя.

Утверждение 2. Если $char\ K = p$ и p делит N, то KG не полупроста.

Доказательство.
Для доказательства поищем в KG ненулевой нильпотентный идеал. Для начала, найдем нильпотентный элемент – рассмотрим $z = g_1 + \dots + g_N$. Имеем: $gz = z$ и $zg = z$ (так как домножение на любой элемент группы слева или справа лишь меняет порядок слагаемых $g_1, \dots, g_N$, но не меняет их сумму). Отсюда, в частности, следует, что $z \in Z(KG)$. Заметим, что $z^2 = 0$:

$$z^2 = (g_1 + \dots + g_N)z = g_1 z + \dots + g_N z = \underbrace{z + \dots + z}_{N \text{ слагаемых}} = Nz = 0$$

Так как $z \in Z(KG)$, то $I = (KG)z$ – нильпотентный двусторонний идеал (двусторонность следует из равенства $(az)b = a(zb) = abz$, а нильпотентность – из равенства $(az)^2 = a^2 z^2 = 0$ для любых $a, b \in KG$). Следовательно, KG не полупроста. ■

Далее считаем, что алгебра KG полупроста, поле K алгебраически замкнуто. В этом случае $KG \simeq A_1 \oplus \dots \oplus A_s$, где $A_i \lhd KG$, $A_i \simeq Mat_{n_i}(K)$, $n_1, \dots, n_s$ – размерности всех неприводимых представлений G. Отметим, что G коммутативна $\Leftrightarrow KG$ коммутативна $\Leftrightarrow n_1 = \dots = n_s = 1 \Leftrightarrow KG \simeq K^N$.

Также отметим, что KG проста только при $G = \{1\}$, так как иначе число классов сопряженности s будет больше 1.

Как было отмечено на лекциях, теория представлений групп эквивалента теории представлений их групповых алгебр. Возникает естественный вопрос – можно ли восстановить группу G по ее групповой алгебре KG ? Ответ отрицательный, так как групповые алгебры коммутативных групп G, H одного порядка N устроены одинаково: $KG \simeq KH \simeq K^N$.

Семинар 15. Разложение групповой алгебры в прямую сумму простых идеалов. Группа обратимых кватернионных матриц как вещественная группа Ли.

Разбор задач домашнего задания.

Разбор задачи 2 см. на следующем семинаре

Задача 4. Пусть $\varphi\colon G \longrightarrow H$ – гомоморфизм конечных групп, который по линейности однозначно продолжается до гомоморфизма групповых алгебр $\tilde{\varphi}\colon KG \longrightarrow KH$. Доказать, что $Ker\ \tilde{\varphi}$ – левый (или правый) идеал в KG, порожденный всеми элементами вида $g - 1$, где $g \in Ker\ \varphi$.

Решение.
Имеем:

$$Ker\ \tilde{\varphi} = \left\{ \sum_{g\in G} \lambda(g)g \ \middle|\ \sum_{g\in g_0 Ker\ \varphi} \lambda(g) = 0, \ \ \forall g_0 \in G \right\}$$

и

$$\left\{ \sum_{g\in g_0 Ker\ \varphi} \lambda(g)g \ \middle|\ \sum_{g\in g_0 Ker\ \varphi} \lambda(g) = 0 \right\} = \langle g_0 n - g_0 \mid n \in Ker\ \varphi \rangle_K$$

Так как $g_0 n - g_0 = g_0(n-1)$, получаем требуемое. Аналогично для правого идеала. ■

Задача 6. Пусть $KG = A_1 \oplus \cdots \oplus A_s$ – групповая алгебра конечной группы G над алгебраически замкнутым полем K характеристики, не делящей $|G|$ (возможно, нулевой), и $A_i \simeq Mat_{n_i}(K)$ – простые двусторонние идеалы в ней, соответствующие неприводимым представлениям группы G размерностей n_i $(i = 1, \dots, s)$. Каким элементом групповой алгебры порождается одномерный идеал A_i, отвечающий одномерному представлению $\rho_i\colon G \longrightarrow K^\times$?

Решение.
Если $A_i = Ka_i$, то $ga_i = \rho_i(g)a_i$. Пусть $a_i = \sum_{h\in G} \lambda(h)h$, тогда:

$$ga_i = \sum_{h\in G} \lambda(h)gh = \sum_{t\in G} \lambda(g^{-1}t)t$$

Получаем равенство

$$\sum_{t\in G} \lambda(g^{-1}t)t = \rho_i(g) \sum_{t\in G} \lambda(t)t,$$

из которого следует, что

$$\lambda(g^{-1}t) = \rho_i(g)\lambda(t)$$

Например, можно взять $\lambda(t) = \frac{1}{\rho_i(t)}$, тогда

$$a_i = \sum_{h\in G} \frac{1}{\rho_i(h)} h$$

■

Задача 7а. В обозначениях задачи 6 найти все простые двусторонние идеалы A_i в алгебре KG и минимальные левые идеалы в A_i, в которых реализуются неприводимые представления группы G для группы $G = S_3$.

Решение.
Простых двусторонних идеалов в алгебре KS_3 столько же, сколько классов сопряженности в S_3, т.е. 3:

$$KS_3 = A_1 \oplus A_2 \oplus A_3,$$

где $A_i \simeq Mat_{n_i}(K)$. Размерности n_i находим из равенства $n_1^2 + n_2^2 + n_3^2 = 6$ (см. теорию представлений групп, курс Алгебра-3), откуда $n_1 = n_2 = 1, n_3 = 2$. Таким образом,

$$KS_3 \simeq Ka_1 \oplus Ka_2 \oplus Mat_2(K)$$

Как известно, существует два неприводимых одномерных представления группы S_3 (см. курс Алгебра-3): тривиальное и задаваемое функцией sgn. Воспользуемся предыдущей задачей – соответствующие им порождающие элементы одномерных идеалов выглядят так:

$$a_1 = \sum_{g\in S_3} g$$

$$a_2 = \sum_{g\in S_3} sgn\, g \cdot g$$

Теперь найдем $A_3 \simeq Mat_2(K)$ – для этого воспользуемся тем, что A_3 полностью определяется равенствами $A_1A_3 = \{0\}$ и $A_2A_3 = \{0\}$, т.е. все элементы $a \in A_3$ (и только они) удовлетворяют условиям $a_1a = 0$ и $a_2a = 0$. Получаем:

$$a_1 a = \sum_{g\in S_3} g \sum_{h\in S_3} \lambda(h)h = \sum_{g,h\in S_3} \lambda(h)gh = \sum_{t\in S_3} \left(\sum_{g\in S_3} \lambda(g^{-1}t)\right) t = \sum_{t\in S_3} \left(\sum_{s\in S_3} \lambda(s)\right) t = 0,$$

(сделали замену $gh = t$), откуда следует, что

$$\sum_{s \in S_3} \lambda(s) = 0.$$

Аналогично

$$a_2 a = \sum_{g \in S_3} sgn\, g \cdot g \sum_{h \in S_3} \lambda(h) h = \sum_{g,h \in S_3} sgn\, g \cdot \lambda(h) gh = \sum_{t \in S_3} \left(\sum_{g \in S_3} sgn\, g \cdot \lambda(g^{-1}t) \right) t =$$

$$= \sum_{t \in S_3} \left(\sum_{s \in S_3} sgn\,(ts^{-1}) \cdot \lambda(s) \right) t = \sum_{t \in S_3} \left(\sum_{s \in S_3} sgn\, s \cdot \lambda(s) \right) t = 0,$$

откуда

$$\sum_{s \in S_3} sgn\, s \cdot \lambda(s) = 0.$$

Из полученных двух равенств следует, что

$$a \in A_3 \Leftrightarrow \sum_{\substack{\text{четные} \\ s \in S_3}} \lambda(s) = \sum_{\substack{\text{нечетные} \\ s \in S_3}} \lambda(s) = 0$$

Выбирая базисы для элементов идеала, соответствующих только четным или только нечетным перестановкам, получаем базис для A_3: $(123) - 1$, $(132) - 1$, $(12) - (23)$, $(13) - (23)$. ■

Группа обратимых кватернионных матриц как вещественная группа Ли.

Рассмотрим группу обратимых кватернионных $n \times n$ матриц $GL_n(\mathbb{H})$. Невырожденность матриц из $GL_n(\mathbb{H})$ понимается как невырожденность соответствующего линейного оператора. Эта группа естественно действует на пространстве $\mathbb{H}^n$, которое является правым векторным пространством над $\mathbb{H}$ (векторные пространства над телом определяются так же, как и над полем, за исключением одного нюанса: следует различать правые и левые векторные пространства. В правом (левом) векторном пространстве скалярный множитель пишется справа (слева) от вектора, и выполняется аксиома ассоциативности, в нашем случае $A(vq) = (Av)q$, где $A \in GL_n(\mathbb{H})$, $v \in \mathbb{H}^n$, $q \in \mathbb{H}$). Таким образом, понятие группы обратимых кватернионных матриц имеет смысл. Поймем, что это группа Ли.

Так как $\mathbb{H}^n \simeq \mathbb{R}^{4n}$, то можно пространство $Mat_n(\mathbb{H})$ интерпретировать как подпространство в $Mat_{4n}(\mathbb{R})$, а группу $GL_n(\mathbb{H})$ – как подгруппу в $GL_{4n}(\mathbb{R})$, при этом

можно указать явный способ ее задания. Пусть $A = \begin{pmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{n1} & \cdots & q_{nn} \end{pmatrix}$. Ее m-ый столбец $\begin{pmatrix} q_{1m} \\ \vdots \\ q_{lm} \\ \vdots \\ q_{nm} \end{pmatrix}$ – это образ базисного вектора $e_m = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$. Если мы рассматриваем $\mathbb{H}^n$ как $\mathbb{R}^{4n}$,

то базисному вектору e_m будут соответствовать базисные вектора $e_m,\ e_m i,\ e_m j,\ e_m k$.

Пусть $q_{lm} = a + bi + cj + dk$, тогда q_{lm} соответствует блок $\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$.

Отсюда следует, что $\dim Mat_n(\mathbb{H}) = 4n^2$.

Упражнение. Показать, что $GL_n(\mathbb{H})$ – открытое подмножество в $GL_{4n}(\mathbb{R})$.

Более подробно этот вопрос мы разберем в начале следующего семинара.

Семинар 16. Псевдоортогональная и симплектическая группы Ли. Связность групп Ли $GL_n(\mathbb{C})$ и $SO_n(\mathbb{C})$.

Начнем с разбора задачи 2 из домашнего задания предыдущего семинара.

Задача 2. Пусть D – центральная алгебра с делением над полем K, и L – поле расщепления для D. Доказать, что $(L:K) \geq \deg D$.

Доказательство.
Обозначим $(L:K) = m$, $\deg D = n$. Так как L – поле расщепления, то $D \underset{K}{\otimes} L \simeq Mat_n(L)$ (см. семинар 14). Эта алгебра действует в пространстве столбцов L^n. Так как имеет место вложение $D \simeq D \underset{K}{\otimes} 1 \subset D \underset{K}{\otimes} L$, то L^n можно рассматривать как левое векторное пространство над телом D, т.е. $L^n \simeq D^k$. Имеем: $\dim_K L^n = mn$, также $\dim_K D^k = n^2 k$, откуда следует, что $m = nk$, откуда следует утверждение задачи. ■

Группа обратимых кватернионных матриц как вещественная группа Ли.

Вернемся к вопросу, который мы рассматривали в конце предыдущего семинара (взгляд на кватернионную матричную группу $Mat_n(\mathbb{H})$ как вещественную матричную группу). Как отмечалось ранее, $\mathbb{H}^n$ можно рассматривать как правое векторное пространство над $\mathbb{H}$, а кватернионные матрицы – как матрицы линейных операторов на $\mathbb{H}^n$. Пусть $Q \in Mat_n(\mathbb{H})$,

$$Q = \begin{pmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{n1} & \cdots & q_{nn} \end{pmatrix}, \qquad Qe_m = \cdots + e_l q_{lm} + \cdots$$

Всякое n-мерное векторное пространство над $\mathbb{H}$ можно рассматривать как $2n$-мерное векторное пространство над $\mathbb{C}$ или $4n$-мерное векторное пространство над $\mathbb{R}$:

- $\mathbb{H}^n \simeq \mathbb{C}^{2n}$ (если $\cdots, e_m, \cdots$ – базис $\mathbb{H}^n$, то $\cdots, e_m, e_m j, \cdots$ – базис $\mathbb{C}^{2n}$).
- $\mathbb{H}^n \simeq \mathbb{R}^{4n}$ (если $\cdots, e_m, \cdots$ – базис $\mathbb{H}^n$, то $\cdots, e_m, e_m i, e_m j, -e_m k, \cdots$ – базис $\mathbb{R}^{4n}$).

Комплексный случай: пусть $q_{lm} = a + ib + jc - kd$. Сгруппируем слагаемые: $q_{lm} = (a + bi) + j(c + di) = z + jw$. Имеем:

$$Qe_m = \cdots + e_l q_{lm} + \cdots = \cdots + e_l z + e_l jw + \cdots =$$

Кватерниону q_{lm} соответствует матрица $\begin{pmatrix} z & -\overline{w} \\ w & \bar{z} \end{pmatrix}$ (по столбцам стоят коэффициенты в разложениях $e_l q_{lm} = e_l z + e_l jw$ и $e_l q_{lm} j = e_l zj + e_l jwj = e_l j\bar{z} - e_l \overline{w}$).

Действительный случай:

$$e_l q_{lm} = e_l z + e_l j w = e_l a + e_l i b + e_l j c - e_l k d$$

$$e_l q_{lm} i = e_l z i + e_l j w i = e_l i z + e_l j i w = e_l i a - e_l b - e_l k c - e_l j d$$

Аналогично можно расписать выражения $e_l q_{lm} j$ и $e_l q_{lm} j i$. Получаем, что кватерниону q_{lm} соответствует матрица

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

Таким образом, существует вложения $Mat_n(\mathbb{H}) \hookrightarrow Mat_{2n}(\mathbb{C}) \hookrightarrow Mat_{4n}(\mathbb{R})$, а значит, существует и вложения $GL_n(\mathbb{H}) \hookrightarrow GL_{2n}(\mathbb{C}) \hookrightarrow GL_{4n}(\mathbb{R})$. Отсюда следует, что $GL_n(\mathbb{H})$ – вещественная группа Ли (так как она задается линейными уравнениями на коэффициенты матриц из $Mat_{4n}(\mathbb{R})$).

Разбор задач домашнего задания.

Задача 2. Пусть на n-мерном векторном пространстве V над полем $\mathbb{R}$ задана невырожденная симметрическая билинейная форма сигнатуры (p, q). Линейный оператор на V, сохраняющий форму ω, называется *псевдоортогональным*. Псевдоортогональные операторы образуют подгруппу $O(V, \omega) \subset GL(V)$, называемую *псевдоортогональной группой*.

- (a) Задать псевдоортогональную группу матричным уравнением в ортонормированном базисе пространства V – соответствующая матричная группа обозначается $O_{p,q}(\mathbb{R})$.
- (b) Доказать, что $O_{p,q}(\mathbb{R})$ – группа Ли.
- (c) Найти размерность и касательную алгебру Ли группы $O_{p,q}(\mathbb{R})$.

Задача 3. Пусть на $2n$-мерном векторном пространстве V над полем $\mathbb{K}$ задана невырожденная кососимметрическая билинейная форма ω. Линейный оператор на V, сохраняющий форму ω, называется *симплектическим*. Симплектические операторы образуют подгруппу $Sp(V, \omega) \subset GL(V)$, называемую *симплектической группой*.

- (a) Задать симплектическую группу матричным уравнением в подходящем базисе пространства V – соответствующая матричная группа обозначается $Sp_{2n}(\mathbb{K})$.
- (b) Доказать, что $Sp_{2n}(\mathbb{K})$ – группа Ли.
- (c) Найти размерность и касательную алгебру Ли группы $Sp_{2n}(\mathbb{K})$.

Решение.

Пусть Ω – матрица формы ω. Имеем:

$$g^T \Omega g = \Omega$$

В самом деле, если линейный оператор сохраняет ω, то $\forall x, y \in V$ выполнено $\omega(gx, gy) = \omega(x, y)$, т.е.

$$x^T \Omega y = (gx)^T \Omega (gy) \Leftrightarrow x^T \Omega y = x^T g^T \Omega g y \Leftrightarrow \Omega = g^T \Omega g$$

- Симметрический случай:

Матричное уравнение $\Omega = g^T \Omega g$ задает $\frac{n(n+1)}{2}$ независимых функциональных уравнений на элементы матрицы g (так как $g^T \Omega g$ симметрична и нам достаточно найти элементы g на главной диагонали и выше главной диагонали).

- Кососимметрический случай:

Матричное уравнение $\Omega = g^T \Omega g$ задает $\frac{2n(2n-1)}{2} = n(2n-1)$ независимых функциональных уравнений на элементы матрицы g (так как $g^T \Omega g$ кососимметрична и нам достаточно найти элементы g выше главной диагонали).

Так как $O_{p,q}(\mathbb{R})$ и $Sp_{2n}(\mathbb{K})$ – подгруппы в $GL_n(\mathbb{K})$ и $GL_{2n}(\mathbb{K})$ соответственно, то для того, чтобы доказать, что они являются подгруппами Ли, достаточно проверить, что они являются подмногообразиями в окрестности e, а для этого нужно проверить, что матрица Якоби J соответствующей системы функциональных уравнений имеет в e максимально возможный ранг.

Вместо того, чтобы искать ранг матрицы J, будем интерпертировать ее строки как дифференциалы соответствующих функций, и найдем размерность пространства решений системы уравнений, которая задается этой матрицей:

$$d(g^T \Omega g - \Omega) = dg^T \Omega g + g^T \Omega dg \underset{\text{при } g=E}{=} dg^T \Omega + \Omega dg = 0$$

Обозначая $dg = X$, получаем уравнения:

- Симметрический случай:

$$\Omega X = -(\Omega X)^T,$$

Решением этого уравнения (относительно ΩX) являются все кососимметрические матрицы. Размерность пространства кососимметрических матриц $n \times n$ равна $\frac{n(n-1)}{2}$, значит, и размерность пространства решений системы уравнений равна $\frac{n(n-1)}{2}$. Тогда

$rk\, J = n^2 - \frac{n(n-1)}{2} = \frac{n(n+1)}{2}$ – ранг системы равен количеству уравнений, следовательно, $O_{p,q}(\mathbb{R})$ – подмногообразие, а значит, группа Ли.

- Кососимметрический случай:

$$\Omega X = (\Omega X)^T,$$

Решением этого уравнения (относительно ΩX) являются все симметрические матрицы. Размерность пространства симметрических матриц $2n \times 2n$ равна $\frac{2n(2n+1)}{2}$, значит, и размерность пространства решений системы уравнений равна $\frac{2n(2n+1)}{2}$. Тогда $rk\, J = (2n)^2 - \frac{2n(2n+1)}{2} = \frac{2n(2n-1)}{2} = n(2n-1)$ – ранг системы равен количеству уравнений, следовательно, $O_{p,q}(\mathbb{R})$ – подмногообразие, а значит, группа Ли.

Уравнения на $\mathfrak{g}$:

$$\Omega X = \mp (\Omega X)^T$$

Правильно выбрав базис, можно понять, как устроены матрицы $X \in \mathfrak{g}$. Выбор базиса:

- Симметрический случай:

$$\Omega = \left(\begin{array}{ccc|c} \overbrace{1 & \cdots & 0}^{p\times p} & & \\ \vdots & \ddots & \vdots & \mathbf{0} \\ 0 & \cdots & 1 & \\ \hline & \mathbf{0} & & \begin{matrix} -1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -1 \end{matrix} \\ & & & \underbrace{\qquad\qquad}_{q\times q} \end{array}\right)$$

Пусть

$$X = \left(\begin{array}{c|c} \begin{matrix} A \\ p \times p \end{matrix} & \begin{matrix} B \\ p \times q \end{matrix} \\ \hline \begin{matrix} C \\ q \times p \end{matrix} & \begin{matrix} D \\ q \times q \end{matrix} \end{array}\right),$$

тогда $\Omega X = \begin{pmatrix} A & B \\ -C & -D \end{pmatrix}$ – кососимметрическая матрица, что равносильно тому, что $A^T = -A$, $D^T = -D$, $B^T = C$. Таким образом, мы получили явное описание матриц из $\mathfrak{g}$: у них диагональные блоки $p \times p$ и $q \times q$ – кососимметрические, а соответствующие антидиагональные блоки симметричны друг другу.

- Кососимметрический случай:

$$\Omega = \left(\begin{array}{ccc|ccc} & \mathbf{0} & & 1 & \cdots & 0 \\ & & & \cdots & \ddots & \cdots \\ & & & 0 & \cdots & 1 \\ \hline -1 & \cdots & 0 & & \mathbf{0} & \\ \cdots & \ddots & \cdots & & & \\ 0 & \cdots & -1 & & & \end{array}\right)$$

Пусть

$$X = \left(\begin{array}{c|c} \begin{matrix} A \\ n \times n \end{matrix} & \begin{matrix} B \\ n \times n \end{matrix} \\ \hline \begin{matrix} C \\ n \times n \end{matrix} & \begin{matrix} D \\ n \times n \end{matrix} \end{array}\right)$$

тогда $\Omega X = \begin{pmatrix} C & D \\ -A & -B \end{pmatrix}$ – симметрическая матрица, что равносильно тому, что $B^T = B$, $C^T = C$, $A^T = D$. Таким образом, мы получили явное описание матриц из $\mathfrak{g}$: у них антидиагональные блоки $n \times n$ – симметрические, а диагональные $n \times n$ блоки антисимметричны друг другу.

Отметим, что если мы выберем базис таким образом, чтобы матрица Ω имела вид

$$\Omega = \left(\begin{array}{ccc|ccc} & \mathbf{0} & & 0 & \cdots & 1 \\ & & & \cdots & \iddots & \cdots \\ & & & 1 & \cdots & 0 \\ \hline 0 & \cdots & -1 & & \mathbf{0} & \\ \cdots & \iddots & \cdots & & & \\ -1 & \cdots & 0 & & & \end{array}\right),$$

то матрицы из $\mathfrak{g}$ описываются немного иначе: блоки B и C должны быть симметричны относительно побочной диагонали, а блоки A и D – антисимметричны друг другу относительно побочной диагонали:

$$X = \left(\begin{array}{cc|cc} & & + & + \\ & & & + \\ \hline + & & & \\ & + & & - \end{array}\right)$$

■

Задача 4. Доказать, что группа Ли $GL_n(\mathbb{C})$ связна.

Доказательство.
Можно использовать жорданову форму матрицы: любую жорданову клетку можно связать непрерывным путем с единичной матрицей соответствующего размера (здесь $\lambda(t)$ – кривая, не проходящая через 0, такая что $\lambda(0) = 1,\ \lambda(1) = \lambda$):

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \rightsquigarrow \begin{pmatrix} \lambda(t) & t & 0 & \cdots & 0 \\ 0 & \lambda(t) & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \lambda(t) & t \\ 0 & \cdots & \cdots & 0 & \lambda(t) \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Отсюда следует, что любую жорданову матрицу из $GL_n(\mathbb{C})$ можно соединить непрерывным путем с E, а значит, и любую матрицу из $GL_n(\mathbb{C})$ можно соединить непрерывным путем с E (путем сопряжения с матрицей перехода), а значит, любые две матрицы из $GL_n(\mathbb{C})$ можно соединить непрерывным путем.

Однако, этот способ основан на приведении матрицы к канонической форме, что можно осуществить не для всех матричных групп. Поэтому мы обсудим более общий способ доказательства.

Пусть $g \in GL_n(\mathbb{C})$ – методом Гаусса приведем ее к единичной матрице. Несложно понять, что это можно сделать элементарными преобразованиями только первого типа и третьего типа, что соответствует умножению слева на элементарные матрицы g_i:

$$g_N \cdots g_1 g = E,$$

откуда

$$g = g_1^{-1} \cdots g_N^{-1}$$

Тогда $g(t) = g_1(t) \cdots g_N(t)$ – гладкая кривая в $GL_n(\mathbb{C})$, соединяющая $g = g(1)$ с $E = g(0)$, где

$$g_i(t) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \lambda(t) & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \text{ или } \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \lambda(t) & \vdots \\ 0 & \ddots & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

(здесь $\lambda(t)$ – кривая, не проходящая через 0, такая что $\lambda(0) = 1,\ \lambda(1) = \lambda$). ■

Задача. Доказать, что группа Ли $SO_n(\mathbb{C})$ связна.

Доказательство.

Вначале рассмотрим частный случай ($n = 2$): матрицы из $SO_2(\mathbb{C})$ имеют вид $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, где $a^2 + b^2 = 1$. Заметим, что $a^2 + b^2 = cc^{-1}$, где $c = a + bi$, тогда $a = \frac{c+c^{-1}}{2}$, $b = \frac{c-c^{-1}}{2i}$, т.е. выбор c однозначно определяет числа a и b, а значит, и матрицу из $SO_2(\mathbb{C})$. Отсюда следует, что $SO_2(\mathbb{C}) \approx \mathbb{C}^\times$ (более того, несложно видеть, что $SO_2(\mathbb{C}) \simeq \mathbb{C}^\times$), поэтому $SO_2(\mathbb{C})$ связна.

Пусть $g \in SO_n(\mathbb{C})$. Попробуем действовать так же, как и в предыдущей задаче, т.е. привести g некоторыми стандартными преобразованиями (матрицы которых также принадлежат $SO_n(\mathbb{C})$) к единичной матрице. Для этого выберем матрицы, отличающиеся от E подматрицей $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $a^2 + b^2 = 1$, диагональные элементы которой расположены на главной диагонали (условимся обозначать такие матрицы $SO_2(\mathbb{C})_{i,j}$):

$$\begin{pmatrix} 1 & \cdots & \cdots & \cdots & 0 \\ \vdots & a & \ddots & -b & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & b & \ddots & a & \vdots \\ 0 & \cdots & \cdots & \cdots & 1 \end{pmatrix}$$

Так как с помощью умножения на матрицу $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $a^2 + b^2 = 1$, из произвольного ненулевого вектора $\begin{pmatrix} x \\ y \end{pmatrix}$ можно получить произвольный вектор $\begin{pmatrix} x' \\ y' \end{pmatrix} \in \mathbb{C}^2$ с тем же скалярным квадратом, то с помощью умножения g на матрицы $SO_2(\mathbb{C})_{i,j}$ можно из двух произвольных элементов x и y (таких что $x^2 + y^2 \neq 0$), расположенных в одном столбце матрицы g, получить элементы z и 0, где $z^2 = x^2 + y^2$:

$$\begin{pmatrix} 1 & \cdots & \cdots & \cdots & 0 \\ \vdots & a & \ddots & -b & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & b & \ddots & a & \vdots \\ 0 & \cdots & \cdots & \cdots & 1 \end{pmatrix} \begin{pmatrix} & \cdots & \cdots & \cdots & \\ \vdots & x & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & y & \ddots & \ddots & \vdots \\ & \cdots & \cdots & \cdots & \end{pmatrix} = \begin{pmatrix} & \cdots & \cdots & \cdots & \\ \vdots & z & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots \\ & \cdots & \cdots & \cdots & \end{pmatrix}$$

Действуя так, занулим все элементы первого столбца, кроме g_{11} (так как $g \in SO_n(\mathbb{C})$, то можно добиться того, чтобы $g_{11} = 1$), занулятся также и все элементы первой строки, кроме g_{11}, т.е. мы сведем дело к случаю матрицы из $SO_{n-1}(\mathbb{C})$, и проделаем с ней те же самые операции, и т.д. Получим

$$g = g_1 \cdots g_N, \qquad g_k \in SO_2(\mathbb{C})_{i,j},$$

а матрицы $SO_2(\mathbb{C})_{i,j}$ стягиваются в E так же, как и матрицы из $SO_2(\mathbb{C})$. Следовательно, группа $SO_n(\mathbb{C})$ связна. ■

Семинар 17. Присоединённая алгебра Ли и группа Ли обратимых элементов конечномерной ассоциативной алгебры с единицей. Структура группы Ли обратимых кватернионов.

Разбор задач домашнего задания.

Задача 5b. Доказать связность группы Ли $Sp_{2n}(\mathbb{K})$.

Доказательство.
Выберем базис, в котором матрица симплектической формы имеет канонический вид:

$$\Omega = \left(\begin{array}{ccc|ccc} & & & 0 & \cdots & 1 \\ & \mathbf{0} & & \cdots & \iddots & \cdots \\ & & & 1 & \cdots & 0 \\ \hline 0 & \cdots & -1 & & & \\ \cdots & \iddots & \cdots & & \mathbf{0} & \\ -1 & \cdots & 0 & & & \end{array}\right)$$

Попробуем действовать так же, как при доказательстве связности $SO_n(\mathbb{C})$ (см. предыдущий семинар), т.е. привести произвольную симплектическую матрицу $g \in Sp_{2n}(\mathbb{K})$ некоторыми стандартными преобразованиями (матрицы которых симплектичны) к единичной матрице. Для этого выберем матрицы, отличающиеся от матриц, соответствующих элементарным преобразованиям первого типа, наличием элемента $\mp c_k$, стоящего на месте, симметричном c_k относительно побочной диагонали:

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ c_k & & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & \mp c_k & & 1 \end{pmatrix}$$

Умножением g на такие матрицы добьемся того, что получим матрицу, первый столбец и последняя строка которой совпадает с первым столбцом и последней строкой единичной матрицы. Далее зануляем оставшиеся элементы в первой строке и последнем столбце, и приходим к случаю $Sp_{2n-2}(\mathbb{K})$, и т.д.

Далее действуем как в случае $GL_n(\mathbb{K})$. ■

Задача 6.

(а) Описать явно группу Ли $O_{1,1}(\mathbb{R})^0$.

(b) Доказать, что группа Ли $O_{p,q}(\mathbb{R})^0$ состоит из псевдоортогональных матриц, у которых определитель и левый верхний угловой минор порядка p положительны.
(c) Вычислить группу компонент связности $O_{p,q}(\mathbb{R})/O_{p,q}(\mathbb{R})^0$.

Решение.
(a) Будем считать, что псевдоскалярное умножение, сохраняемое группой $O_{1,1}(\mathbb{R})$, имеет стандартный вид $(x \mid y) = x_1y_1 - x_2y_2$. (т.е. эта группа сохраняет квадратичную форму $q(x_1, x_2) = x_1^2 - x_2^2$). Тогда группа $O_{1,1}(\mathbb{R})$ состоит из следующих матриц:

$$g = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{ или } \begin{pmatrix} a & -b \\ b & -a \end{pmatrix}$$

где $a^2 - b^2 = 1$, т.е. $b \in \mathbb{R}$, $a = \pm\sqrt{1 + b^2}$.

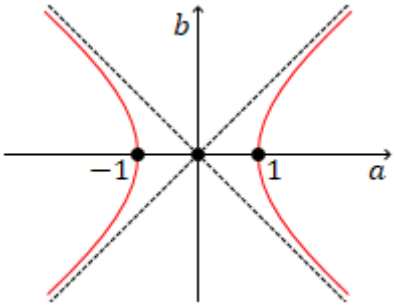


Рис. 17.1. Компоненты связности

Таким образом, каждому из двух видов матриц $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ и $\begin{pmatrix} a & -b \\ b & -a \end{pmatrix}$ соответствует две компоненты связности, т.е. всего имеется 4 компоненты связности.

Компоненту связности $O_{1,1}(\mathbb{R})^0$ зададим параметрически:

$$O_{1,1}(\mathbb{R})^0 = \left\{ g = \begin{pmatrix} ch\, t & sh\, t \\ sh\, t & ch\, t \end{pmatrix},\ t \in \mathbb{R} \right\}$$

- такие преобразования плоскости осуществляют движение по правой ветке гиперболы, нарисованной на рис. 17.1. Аналогично, остальные компоненты связности $O_{1,1}(\mathbb{R})$ задаются комбинациями знаков $(sgn(a), sgn(det))$. Несложно понять, что

$$\pi_0\left(O_{1,1}(\mathbb{R})\right) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

- в самом деле, представители компонент связности $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ образуют группу $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Будем считать, что псевдоскалярное умножение, сохраняемое группой $O_{p,q}(\mathbb{R})$, имеет матрицу

$$Q = \left(\begin{array}{c|c} \overbrace{\begin{matrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{matrix}}^{p\times p} & \begin{matrix} & 0 & \\ & & \end{matrix} \\ \hline \begin{matrix} & 0 & \end{matrix} & \underbrace{\begin{matrix} -1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -1 \end{matrix}}_{q\times q} \end{array}\right)$$

Пусть $g \in O_{p,q}(\mathbb{R})$. В пункте (a) мы выяснили, что комоненты связности различаются знаком определителя матрицы и знаком a, т.е. знаком левого верхнего углового минора. В общем случае ситуация аналогичная: разделим матрицу $g \in O_{p,q}(\mathbb{R})$ на 4 блока:

$$g = \left(\begin{array}{c|c} p \times p & p \times q \\ \hline q \times p & q \times q \end{array}\right)$$

Заметим, что левый верхний угловой минор Δ размера $p \times p$ отличен от нуля. В самом деле, в противном случае столбцы матрицы Δ были бы линейно зависимы, т.е. существовала бы их нетривиальная линейная комбинация, равная нулю, и линейная комбинация первых p столбцов матрицы g с теми же коффициентами принадлежала бы линейной оболочке последних q столбцов матрицы g – противоречие (так как псевдоскалярное умножение на первых p столбцах матрицы g определено положительно, а на последних q столбцах матрицы g определено отрицательно).

Теперь путем умножения на матрицы из $O_{p,q}(\mathbb{R})$, задающие повороты в координатных плоскостях (обычные или гиперболические) приведем g к следующему виду:

$$\left(\begin{array}{c|c} \overbrace{\begin{matrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \pm 1 \end{matrix}}^{p\times p} & \begin{matrix} & 0 & \\ & & \end{matrix} \\ \hline \begin{matrix} & 0 & \end{matrix} & \underbrace{\begin{matrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \pm 1 \end{matrix}}_{q\times q} \end{array}\right)$$

- снова получаем 4 компоненты связности, которые задаются знаком определителя и левого верхнего углового минора порядка p.

(c) Из вышеприведенных рассуждений вытекает, что $\pi_0\left(O_{p,q}(\mathbb{R})\right) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. ■

Упражнение. Проверить, что операция коммутирования на алгебре Ли удовлетворяет тождеству Якоби.

Решение.
Проверим, что $[X,[Y,Z]]+[Z,[X,Y]]+[Y,[Z,X]]=0$. Имеем:

$$[X,[Y,Z]]+[Z,[X,Y]]+[Y,[Z,X]] = [X,YZ-ZY]+[Z,XY-YX]+[Y,ZX-XZ] =$$

$$\begin{aligned} &= XYZ-XZY-YZX+ZYX+ \\ &+ZXY-ZYX-XYZ+YXZ+ \\ &+YZX-YXZ-ZXY+XZY=0 \end{aligned}$$

■

Данное упражнение показывает, что алгебру Ли можно “изготовить” из любой ассоциативной алгебры: если A – ассоциативная алгебра, то операция коммутирования $[a,b]=ab-ba$ превращает A в алгебру Ли, обозначаемую $A^{(-)}$.

Отметим, однако, что операция умножения в алгебре Ли не обязательно связана с некоторым ассоциативным умножением (например, в $\mathbb{R}^3$ операция векторного умножения не происходит из какого-либо ассоциативного умножения в $\mathbb{R}^3$). При этом любая конечномерная алгебра Ли связана с некоторой ассоциативной алгеброй, так как она вкладывается в алгебру матриц подходящего размера.

Упражнение. Пусть A – конечномерная ассоциативная алгебра с 1.

- (1) Доказать, что $G=A^{\times}$ - группа Ли.
- (2) $\mathfrak{g}$ = ?
- (3) $\exp$ = ?
- (4) Ad = ?

Решение.
(1) Вложим алгебру A в алгебру $L(A)$:

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

Мы хотим доказать, что $G=\mathcal{L}(A)\cap GL(A)$, т.е. $a\in A^{\times} \Leftrightarrow \mathcal{L}(a)\in GL(A)$.

$\Rightarrow$:
Если a обратим, то $\mathcal{L}(a) \in GL(A)$.
$\Leftarrow$:
Пусть $\mathcal{L}(a)^{-1}1 = b$, тогда $\mathcal{L}(A)b = ab = 1$, т.е. элемент a обратим справа. Для того, чтобы доказать, что a обратим слева, умножим равенство $ab = 1$ справа на a:

$$aba = 1 \cdot a = a \cdot 1$$

Получаем, что $a \cdot (ba) = a \cdot (1)$ – из этого равенства и из обратимости оператора $\mathcal{L}(A)$ следует, что $ba = 1$, т.е. a обратим слева.

Итак, $G = \mathcal{L}(A) \cap GL(A)$, откуда следует, что G – группа Ли (так как $\mathcal{L}(A)$ – подпространство, $GL(A)$ открыто).

(2) $\mathfrak{g} = A^{(-)}$. Такая структура алгебры Ли следует из вложения $A \hookrightarrow L(A)$: в самом деле, $\forall x, y \in \mathfrak{g}$ равенство $[x, y] = xy - yx$ следует из равенства $[\mathcal{L}(x), \mathcal{L}(y)] = \mathcal{L}([x, y])$.

(3) Имеем:

$$\exp \mathcal{L}(A) = E + \mathcal{L}(A) + \frac{\mathcal{L}(A)^2}{2} + \cdots$$
$$x \mapsto x + ax + \frac{a^2 x}{2} + \cdots$$

Получаем

$$\exp(a) = 1 + a + \frac{a^2}{2!} + \cdots + \frac{a^k}{k!} + \cdots$$

(4) Для $g \in G$ имеем:

$$Ad(g)\colon\ x \mapsto gxg^{-1}$$

По определению, Ad – дифференциал в E внутреннего автоморфизма:

$$i_g\colon\ G \mapsto G$$
$$h \mapsto ghg^{-1}$$

Его можно также рассматривать как внутренний автоморфизм алгебры A:

$$i_g\colon\ A \mapsto A$$
$$h \mapsto ghg^{-1}$$

- это линейное отображение, а значит, оно совпадает со своим дифференциалом. ■

Таким образом, для произвольной конечномерной ассоциативной алгебры с 1 выражения для $\mathfrak{g}$, exp, Ad, такие же, как и для алгебры матриц. В качестве примера, иллюстрирующего это, рассмотрим алгебру кватернионов.

Структура группы Ли обратимых кватернионов.

Рассмотрим алгебру кватернионов $A = \mathbb{H}$. Группа обратимых элементов: $\mathbb{H}^\times = \mathbb{H}\backslash\{0\}$. Разберемся со структурой группы $\mathbb{H}^\times$: алгебра кватернионов – это четырехмерное векторное пространство над $\mathbb{R}$:

$$A = \mathbb{H} = \langle 1, i, j, k\rangle_{\mathbb{R}}$$

Кватернионы, норма которых равна единице, т.е. $U_1(\mathbb{H}) = \{q \in \mathbb{H} \mid N(q) = q\bar{q} = 1\}$, образуют в этом пространстве трехмерную сферу: $U_1(\mathbb{H}) \approx S^3$, при этом

$$\mathbb{H}^\times = \mathbb{H}\backslash\{0\} = U_1(\mathbb{H}) \times \mathbb{R}_{>0}$$

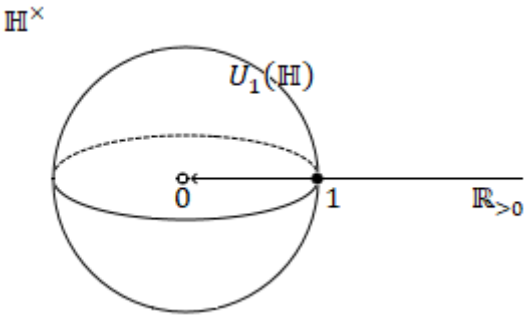


Рис. 17.2. $\mathbb{H}^\times = \mathbb{H}\backslash\{0\} = U_1(\mathbb{H}) \times \mathbb{R}_{>0}$

Найдем $Lie(\mathbb{H}^\times)$. Как было показано выше, $Lie(\mathbb{H}^\times) = \mathbb{H}^{(-)}$, а так как $\mathbb{H}^\times = U_1(\mathbb{H}) \times \mathbb{R}_{>0}$, то $Lie(\mathbb{H}^\times) = \mathbb{R} \oplus \mathbb{H}_{im}^{(-)}$, где $\mathbb{H}_{im} = \langle i, j, k\rangle_{\mathbb{R}}$ – пространство чисто мнимых кватернионов.

Задача. Доказать, что присоединенное действие группы Ли $U_1(\mathbb{H})$ на своей алгебре Ли $\mathfrak{u}_1(\mathbb{H}) = \mathbb{H}_{im}$ сохраняет скалярное умножение, соответствующее кватернионной норме $N(q) = q\bar{q}$ и тем самым задает гомоморфизм групп Ли $Ad\colon U_1(\mathbb{H}) \longrightarrow O(\mathbb{H}_{im}) \simeq O_3(\mathbb{R})$.

Семинар 18. Представления группы Ли $\mathbb{R}$. Стабилизатор вектора в линейном представлении группы Ли и группа автоморфизмов конечномерной алгебры — группы Ли, их касательные алгебры Ли.

Разбор задач домашнего задания.

Задача 5. Перечислить с точностью до изоморфизма все двумерные алгебры

- (a) над $\mathbb{C}$,
- (b) над $\mathbb{R}$,

и указать соответствующие группы Ли.

Решение.
Пусть $\mathfrak{g} = \langle e_1, e_2 \rangle$ и $[e_1, e_2] = \alpha e_1 + \beta e_2 = v$. Возможны два варианта:

- $v = 0$

Тогда $[\,\cdot\,,\,\cdot\,] = 0$, т.е. $\mathfrak{g}$ – абелева алгебра Ли. Соответствующая группа Ли – например,

$$G = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \mid \det \neq 0 \right\} \simeq \mathbb{K}^\times \times \mathbb{K}^\times$$

- $v \neq 0$

Можно считать, что $\alpha \neq 0$. Имеем: $[v, e_2] = \alpha v$, т.е. $\left[v, \frac{e_2}{\alpha}\right] = v$. Обозначим $\frac{e_2}{\alpha} = w$, тогда новый базис: v, w, и $[v, w] = v$. Соответствующая группа Ли:

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}, \quad b \neq 0 \right\},$$

алгебра Ли:

$$\mathfrak{g} = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \right\},$$

соответствующий базис:

$$v = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad w = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

■

Задача 7c. Доказать, что экспоненциальное отображение $\exp\colon \mathfrak{g} \longrightarrow G$ для группы $G = N_n(\mathbb{K})$ верхних унитреугольных матриц является диффеоморфизмом.

Доказательство.

Как известно, алгебра Ли группы верхних унитреугольных матриц – это алгебра нильтреугольных матриц:

$$\mathfrak{n}_n = \begin{pmatrix} 0 & * & \cdots & * \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

Если $X \in \mathfrak{n}_n$, то

$$\exp X = E + X + \frac{X^2}{2!} + \cdots + \frac{X^{n-1}}{(n-1)!}$$

(так как $\forall X \in \mathfrak{n}_n$ выполнено $X^n = 0$, то экспоненциальный ряд превращается в многочлен).

Если $g = E + Y \in N_n$, то

$$\ln g = \ln(E + Y) = Y - \frac{Y^2}{2} + \cdots + \frac{(-1)^n}{n-1} Y^{n-1}$$

(снова ряд превращается в многочлен, так как Y – нильпотентная матрица).

Докажем, что отображение ln обратно отображению exp – нужно проверить, что $\ln(\exp(X)) = X$ и $\exp(\ln(E + Y)) = E + Y$. Проверим эти равенства для формальных функциональных рядов

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{X^k}{k!} + \cdots$$

и

$$\ln(1 + y) = y - \frac{y^2}{2} + \cdots + \frac{(-1)^{k-1}}{k} y^k + \cdots$$

Так как $\exp(x)$ и $\ln(1 + y)$ – ряды Тейлора для аналитических функций, они сходятся абсолютно и равномерно внутри круга сходимости, а так как функции exp и ln обратны друг другу, то функциональные тождества $\ln(\exp(x)) = x$ и $\exp(\ln(1 + y)) = 1 + y$ справедливы и для их рядов Тейлора.

Подставляя вместо переменных x и y соответствующие нильпотентные матрицы, получаем требуемое. ■

Задача 6. *Группа Гейзенберга* $H_n(\mathbb{K})$ состоит из матриц вида

$$\begin{pmatrix} 1 & x_1 & \cdots & \cdots & x_n & z \\ 0 & 1 & 0 & \cdots & 0 & y_1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & y_n \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

над полем $\mathbb{K}$. Найти алгебру Ли $\mathfrak{h}_n(\mathbb{K})$ и вычислить exp: $\mathfrak{h}_n(\mathbb{K}) \longrightarrow H_n(\mathbb{K})$.

Решение.

$$\mathfrak{h}_n = \left\{ \begin{pmatrix} 0 & x_1 & \cdots & \cdots & x_n & z \\ 0 & 0 & 0 & \cdots & 0 & y_1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & y_n \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix} \right\}$$

Если $X \in \mathfrak{h}_n$, то

$$\exp X = E + X + \frac{X^2}{2!} + \cdots$$

Имеем:

$$X^2 = \begin{pmatrix} 0 & x_1 & \cdots & \cdots & x_n & z \\ 0 & 0 & 0 & \cdots & 0 & y_1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & y_n \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & x_1 & \cdots & \cdots & x_n & z \\ 0 & 0 & 0 & \cdots & 0 & y_1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & y_n \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & \sum_i x_i y_i \\ 0 & 0 & 0 & & & \\ \vdots & \ddots & \ddots & \cdots & 0 & 0 \\ & & & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & & 0 & \vdots \\ \vdots & \ddots & \ddots & & 0 & 0 \\ 0 & \cdots & \cdots & & 0 & 0 \end{pmatrix},$$

$$X^3 = 0$$

Получаем

$$\exp X = \begin{pmatrix} 1 & x_1 & \cdots & \cdots & x_n & z + \dfrac{\sum_i x_i y_i}{2} \\ 0 & 1 & 0 & \cdots & 0 & y_1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & y_n \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Несложно заметить, что отображение $\exp\colon \mathfrak{h}_n(\mathbb{K}) \longrightarrow H_n(\mathbb{K})$ является диффеоморфизмом (по X можно вычислить $\exp X$ и наоборот). ■

Линейное представление группы Ли $\mathbb{R}$.

На прошлой лекции (см. лекцию 19 курса лекций) мы упоминали о том, как устроены линейные представления простейшей группы Ли $\mathbb{R}$: они задаются произвольным линейным оператором A по формуле

$$\mathcal{R}(t) = \exp(tA)$$

Расмотрим кривую $g(t) \in GL(V)$. Поймем, задает ли она линейное представление группы Ли $\mathbb{R}$, и если да, то найдем A (т.н. *генератор* линейного представления). Пусть $g(t) = \begin{pmatrix} ch\, t & sh\, t \\ sh\, t & ch\, t \end{pmatrix}$. Имеем:

$$\frac{d}{dt}\Big|_{t=0} g(t) = \begin{pmatrix} sh\, t & ch\, t \\ ch\, t & sh\, t \end{pmatrix}\Big|_{t=0} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = A$$

Проверим, что $g(t) = \exp(tA)$:

$$\exp(tA) = E + tA + \frac{(tA)^2}{2!} + \cdots$$

Так как $A^2 = E,\ A^3 = A\,, \ldots, A^{2n} = E,\ A^{2n+1} = A, \ldots$, получаем

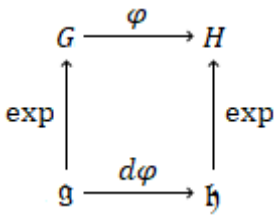
$$\exp(tA) = \left(\sum_{n=0}^{\infty} \frac{t^{2n}}{(2n)!}\right) E + \left(\sum_{n=0}^{\infty} \frac{t^{2n+1}}{(2n+1)!}\right) A = ch\, t \cdot E + sh\, t \cdot tA = \begin{pmatrix} ch\, t & sh\, t \\ sh\, t & ch\, t \end{pmatrix}$$

■

При гомоморфизме групп Ли прообраз подгруппы Ли – подгруппа Ли.

Пусть $\varphi\colon G \longrightarrow H$ – гомоморфизм групп Ли, $S \subset H$ – подгруппа. Ее прообраз $\varphi^{-1}(S)$ – подгруппа в G. Поймем, будет ли $\varphi^{-1}(S)$ подгруппой Ли – для этого проверим, будет ли $\varphi^{-1}(S)$ подмногообразием в окрестности E.

Как было доказано на лекциях (см. лекцию 18), $\varphi \circ \exp = \exp \circ\, d\varphi$. На языке коммутативных диаграмм:



В exp-координатах в окрестности E гомоморфизм φ отождествляется с $d\varphi$, т.е. становится линейным отображением.

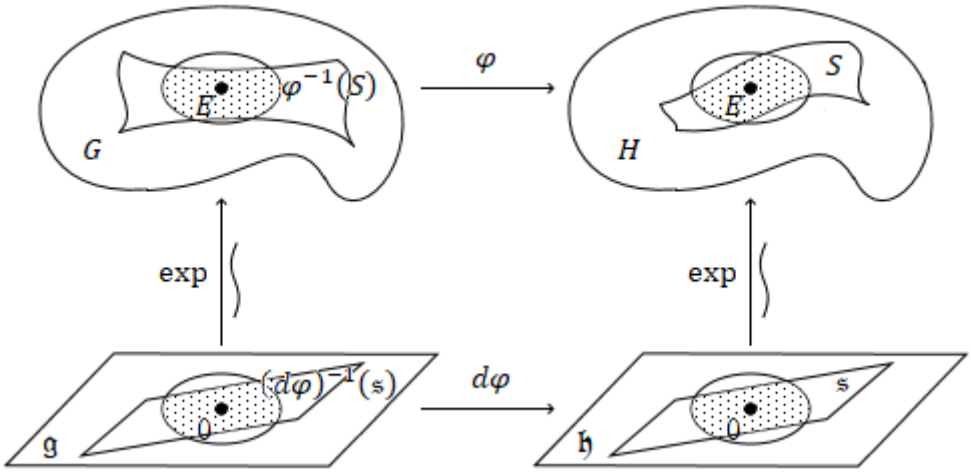


Рис. 18.1. При гомоморфизме групп прообраз подгруппы Ли – подгруппа Ли

Из рис. 18.1 нетрудно увидеть, что $\varphi^{-1}(S)$ – подпространство, а следовательно, и подмногообразие в окрестности E, откуда следует, что $\varphi^{-1}(S)$ – подгруппа Ли.

Отметим, что аналогичное утверждение для образов подгрупп при гомоморфизме групп Ли неверно: $Im\ \varphi$ не обязательно является подгруппой Ли в H.

Пример: рассмотрим отображение окружности в n-мерный тор:

$$\varphi\colon\ U_1(\mathbb{C}) \longrightarrow \underbrace{U_1(\mathbb{C}) \times \cdots \times U_1(\mathbb{C})}_{n \text{ сомножителей}}$$
$$\varphi\left(e^{it}\right) = \left(e^{i\alpha_1 t}, \dots, e^{i\alpha_n t}\right)$$

Доказать: $Im\ \varphi$ – подгруппа Ли $\Leftrightarrow \frac{\alpha_j}{\alpha_k} \in \mathbb{Q}, \forall\, j,k.$

Для наглядности проиллюстрируем двумерный случай: если $\frac{\alpha_1}{\alpha_2} \in \mathbb{Q}$, то кривая $\varphi\left(e^{it}\right) = \left(e^{i\alpha_1 t}, e^{i\alpha_2 t}\right)$ замкнется (т.е. при каком-то значении t перейдет в себя), а если

$\frac{\alpha_1}{\alpha_2} \notin \mathbb{Q}$, то кривая $\varphi\left(e^{it}\right)$ будет бесконечно наматываться на тор, а $Im\,\varphi$ не будет подмногообразием, а значит, и подгруппой Ли.

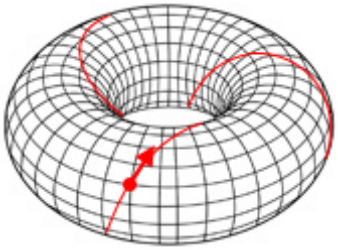


Рис. 18.2. Обмотка тора

Из сделанного нами наблюдения (при гомоморфизме групп прообраз подгруппы Ли является подгруппой Ли) выведем такие следствия:

- Рассмотрим линейное представление $\mathcal{R}\colon G \longrightarrow GL(V)$ и докажем, что стабилизатор $G_v = \{g \in G \mid \mathcal{R}(g)v = v\}$ – подгруппа Ли.

Рассмотрим подгруппу $GL(V) \supset S = \{\mathcal{A} \in GL(V) \mid \mathcal{A}v = v\}$, состоящую из всех невырожденных операторов, оставляющих v на месте. В базисе $e_1 = v, e_2, \dots, e_n$ имеем:

$$S = \left\{ \left(\begin{array}{c|ccc} 1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & \det \neq 0 & \\ 0 & & & \end{array} \right) \middle| \det \neq 0 \right\}$$

откуда следует, что S – подгруппа Ли, а значит, и G_v – подгруппа Ли (как полный прообраз S при гомоморфизме $\mathcal{R}$). Найдем ее касательную алгебру Ли $\mathfrak{g}_v$. В общем случае: $Lie\ \varphi^{-1}(S) = (d\varphi)^{-1}(\mathfrak{s})$, в нашем случае

$$\mathfrak{s} = \left\{ \left(\begin{array}{c|ccc} 0 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array} \right) \right\}$$

поэтому $\mathfrak{g}_v = \{X \in \mathfrak{g} \mid dR(X)v = 0\}$.

- Пусть A – конечномерная алгебра над $\mathbb{K}$. Рассмотрим ее группу автоморфизмов $G = Aut(A) \subseteq GL(A)$ и докажем, что G – группа Ли.

Имеем: $g \in G \Leftrightarrow g(xy) = g(x)g(y),\ \forall x, y \in A$. Операция умножения $\mu\colon A \times A \longrightarrow A$ – билинейное отображение. Рассмотрим пространство всех билинейных отображений на A – его можно отождествить с пространством

$$L(A \otimes A, A) \simeq (A \otimes A)^* \otimes A \simeq A^* \otimes A^* \otimes A$$

Линейное представление $GL(A)$ на $L(A \otimes A, A)$:

$$(g\mu)(x,y) = g\left(\mu\big(g^{-1}(x), g^{-1}(y)\big)\right),$$

т.е.

$$\underbrace{g\big(\mu(x,y)\big)}_{=g\left(g^{-1}(v),g^{-1}(w)\right)} = \underbrace{\mu\big(g(x),g(y)\big)}_{=\mu(v,w)}$$

Таким образом, $Aut(A) = GL(A)_\mu$, где μ – операция умножения в A.

Найдем $\mathfrak{g}$: найдем дифференциал представления $g\mu(x,y) = g\left(\mu\big(g^{-1}(x), g^{-1}(y)\big)\right)$ – для этого рассмотрим кривую $g = g(t)$, $g(0) = E$, $\dot{g}(0) = X$. Имеем:

$$X\mu(x,y) = \frac{d}{dt}\Big|_{t=0} g(t)\big(\mu(g(t)^{-1}x, g(t)^{-1}y)\big) = X\big(\mu(x,y)\big) + \mu(-Xx, y) + \mu(x, -Xy) = 0$$

$$\Leftrightarrow X(x,y) = Xx \cdot y + x \cdot Xy$$

– получили операторы дифференцирования, т.е. $\mathfrak{g} = Der\ A$ – алгебра дифференцирований.

Семинар 19. Линейные представления группы Ли SL_2 и алгебры Ли $\mathfrak{sl}_2$: структура неприводимых представлений, характеры, формула Клебша-Гордана.

Разбор задач домашнего задания.

Задача 7а. Пусть $\mathfrak{g}$ – 3-мерная алгебра Ли с базисом $\{e_1, e_2, e_3\}$ и коммутационными соотношениями $[e_1, e_2] = e_2$ (указаны только ненулевые коммутаторы базисных векторов, с точностью до перестановки аргументов). Найти группу $Aut(\mathfrak{g})$ и алгебру Ли $Der(\mathfrak{g})$.

Решение.
Пусть $\varphi\colon \mathfrak{g} \twoheadrightarrow \mathfrak{g}$ – автоморфизм. Заметим, что e_3 коммутирует со всеми векторами из $\mathfrak{g}$, $\mathfrak{z}(\mathfrak{g}) = \langle e_3 \rangle$ (т.е. центр $\mathfrak{g}$ порожден e_3), и $\mathfrak{z}(\mathfrak{g}) \twoheadrightarrow \mathfrak{z}(\mathfrak{g})$, $\varphi(e_3) = \alpha e_3$. Также $[\mathfrak{g}, \mathfrak{g}] = \langle e_2 \rangle$ (т.е. коммутант $\mathfrak{g}$ – это линейная оболочка e_2), и $\varphi\colon [\mathfrak{g}, \mathfrak{g}] \twoheadrightarrow [\mathfrak{g}, \mathfrak{g}]$ – изоморфизм, $\varphi(e_2) = \beta e_2$, т.е. в базисе $\{e_1, e_2, e_3\}$:

$$\varphi = \begin{pmatrix} \lambda & 0 & 0 \\ \mu & \beta & 0 \\ \nu & 0 & \alpha \end{pmatrix}, \qquad \varphi(e_1) = \lambda e_1 + \mu e_2 + \nu e_3.$$

Доджно быть выполнено: $[\varphi(e_1), \varphi(e_2)] = \varphi([e_1, e_2]) = e_2$. Так как $\varphi(e_2) = \beta e_2$, $[\varphi(e_1), \varphi(e_2)] = [\lambda e_1 + \mu e_2 + \nu e_3, \beta e_2] = \lambda\beta e_2$, получаем $\lambda = 1$. Окончательно получаем

$$Aut(\mathfrak{g}) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ \mu & \beta & 0 \\ \nu & 0 & \alpha \end{pmatrix} \middle| \, \alpha, \beta \neq 0 \right\}$$

Тогда

$$Der(\mathfrak{g}) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ \mu & \beta & 0 \\ \nu & 0 & \alpha \end{pmatrix} \right\}$$

Другими словами, если $X \in Der(\mathfrak{g})$, то X:

$$\begin{aligned} e_1 &\mapsto \langle e_2, e_3 \rangle \\ e_2 &\mapsto \langle e_2 \rangle \\ e_3 &\mapsto \langle e_3 \rangle \end{aligned}$$

■

Представления SL_2 и $\mathfrak{sl}_2$.

Как мы знаем (см. курс лекций, лекция 20), линейные представления группы Ли $SL_2(\mathbb{C})$ над $\mathbb{C}$ вполне приводимы, поэтому все сводится к изучению неприводимых

представлений $SL_2(\mathbb{C})$, которые устроены следующим образом (см. лекцию 20): $\forall n \geq 0$ существует единственное неприводимое комплексное линейное представление $\mathcal{R} = \mathcal{R}_n$ группы Ли $SL_2(\mathbb{C})$ размерности $n+1$. Оно реализуется в пространстве $\mathbb{C}[x,y]_n$ линейными заменами переменных, причем $d\mathcal{R}_n = \rho_n$, где ρ_n – представление алгебры Ли $\mathfrak{sl}_2(\mathbb{C})$ размерности $n+1$, которое реализуется в пространстве $V(n) = < v_0, v_1, \dots, v_n >$, где $\mathfrak{sl}_2(\mathbb{C})$ действует по правилам:

- $\mathcal{X} v_k = (n-k+1)k v_{k-1}$ (при $k > 0$) или 0 (при $k = 0$)
- $\mathcal{Y} v_k = v_{k-1}$ (при $k < n$) или 0 (при $k = n$)
- $\mathcal{Z} v_k = (n-2k)v_k$

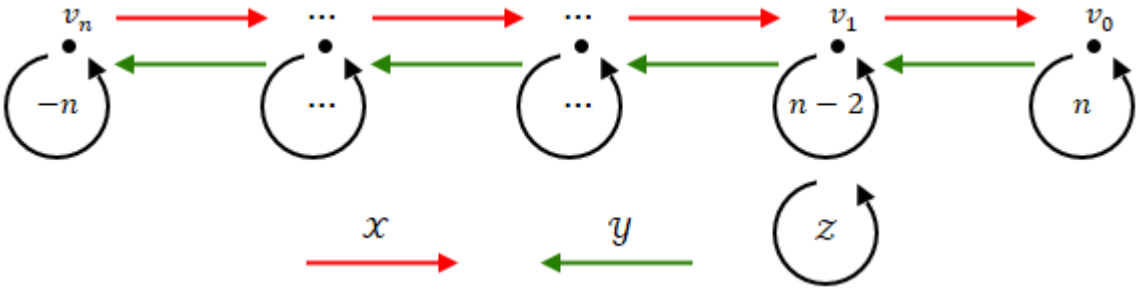


Рис. 19.1. Действие операторов $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$

Числа $n,\ n-2,\ n-4, \dots,\ -n$ называются *весами* представления ρ_n. Число n называется *старшим весом*. Здесь $\mathcal{X} = \rho(X),\ \mathcal{Y} = \rho(Y),\ \mathcal{Z} = \rho(Z)$, где

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- стандартный базис в $\mathfrak{sl}_2(\mathbb{C})$. Коммутационные соотношения:

$$[X,Y] = Z, \quad [Z,X] = 2X, \quad [Z,Y] = -2Y$$

Напоминание: пусть $\mathcal{R}$: $G \to GL(V)$ - линейное представление. Его характер:

$$\chi_{\mathcal{R}}(g) = tr\ \mathcal{R}(g) = tr\ R(g) = r_{11}(g) + \dots + r_{nn}(g)$$

- сумма диагональных матричных элементов представления $\mathcal{R}$ в некотором базисе.

Как мы знаем, характер однозначно определяет линейное представление конечной группы. Замечательно, что это верно и для группы $SL_2(\mathbb{C})$ (и для всех редуктивных групп). Матрицы с простым спектром (т.е. с различными собственными значениями) образуют в $SL_2(\mathbb{C})$ плотное открытое подмножество, поэтому достаточно знать значения характера на матрицах с простым спектром.

Если $g \in SL_2(\mathbb{C})$ – матрица с простым спектром, то $g = chc^{-1}$, где $h = \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$. Так как характер не меняется при сопряжении: $\chi_{\mathcal{R}}(g) = \chi_{\mathcal{R}}(h)$, то достаточно научиться вычислять характер на матрицах h. Здесь нам удобно будет перейти к алгберам Ли:

$$h = \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} = \exp(tZ),$$

где

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad z = e^t$$

Имеем:

$$d\mathcal{R}_n(Z) = \begin{pmatrix} n & 0 & \cdots & \cdots & 0 \\ 0 & n-2 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 2-n & 0 \\ 0 & \cdots & \cdots & 0 & -n \end{pmatrix},$$

$$\mathcal{R}_n(h) = \exp d\mathcal{R}_n(tZ) = \begin{pmatrix} e^{tn} & 0 & \cdots & \cdots & 0 \\ 0 & e^{t(n-2)} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & e^{t(2-n)} & 0 \\ 0 & \cdots & \cdots & 0 & e^{-tn} \end{pmatrix} =$$

$$= \begin{pmatrix} z^n & 0 & \cdots & \cdots & 0 \\ 0 & z^{n-2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & z^{2-n} & 0 \\ 0 & \cdots & \cdots & 0 & z^{-n} \end{pmatrix}$$

Получаем

$$\chi_{\mathcal{R}_n}(h) = z^n + z^{n-2} + \cdots + z^{2-n} + z^{-n} = z^{-n}\frac{z^{2n+2}-1}{z^2-1} = \frac{z^{n+1}-z^{-n-1}}{z-z^{-1}}$$

Теперь от неприводимых перейдем к произвольным представлениям.

Задача 1. Доказать, что $\chi_{\mathcal{R}\oplus\mathcal{S}} = \chi_{\mathcal{R}} + \chi_{\mathcal{S}}$.

Доказательство.
В согласованном базисе:

$$(\mathcal{R} \oplus \mathcal{S})(g) = \left(\begin{array}{c|c} \mathcal{R}(g) & 0 \\ \hline 0 & \mathcal{S}(g) \end{array}\right)$$

откуда следует, что $\chi_{\mathcal{R}\oplus\mathcal{S}} = tr\,\mathcal{R} \oplus \mathcal{S}(g) = tr\,\mathcal{R}(g) + tr\,\mathcal{S}(g) = \chi_{\mathcal{R}} + \chi_{\mathcal{S}}$. ■

Задача 2. Доказать, что любое линейное представление $\mathcal{R}$ группы $SL_2(\mathbb{C})$ однозначно восстанавливается по своему характеру.

Доказательство.
Разложим представление $\mathcal{R}$ в прямую сумму неприводимых:

$$\mathcal{R} = \mathcal{R}_{n_1} \oplus \cdots \oplus \mathcal{R}_{n_s},$$

тогда

$$\chi_{\mathcal{R}} = \chi_{\mathcal{R}_{n_1}} + \cdots + \chi_{\mathcal{R}_{n_s}} = \frac{z^{n_1+1} + \cdots + z^{n_s+1} - z^{-n_1-1} - \cdots - z^{-n_s-1}}{z - z^{-1}},$$

т.е.

$$\chi_{\mathcal{R}}(z)(z - z^{-1}) = \sum_{i=1}^{s} (z^{n_i+1} - z^{-n_i-1}),$$

- по $\chi_{\mathcal{R}}$ можно восстановить $\chi_{\mathcal{R}_{n_i}}$, а по ним можно восстановить $\mathcal{R}_{n_i}$, а значит, и $\mathcal{R}$. ■

Задача 3. Найти $\chi_{\mathcal{R}\otimes\mathcal{S}}$.

Решение.
Если $\mathcal{R}\colon\ SL_2 \to GL(V)$ и $\mathcal{S}\colon\ SL_2 \to GL(W)$, то

$$\mathcal{R} \otimes \mathcal{S}\colon\ SL_2 \to GL(V \otimes W)$$
$$(\mathcal{R} \otimes \mathcal{S})(g) = \mathcal{R}(g) \otimes \mathcal{S}(g)\colon\ v \otimes w \mapsto \mathcal{R}(g)v \otimes \mathcal{S}(g)w$$

и

$$\chi_{\mathcal{R}\otimes\mathcal{S}} = \chi_{\mathcal{R}}\chi_{\mathcal{S}}$$

В самом деле, пусть $h = \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$, тогда

$$\mathcal{R}(h) = \begin{pmatrix} * & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \lambda_i & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & * \end{pmatrix}, \qquad \mathcal{S}(h) = \begin{pmatrix} * & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \mu_j & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & * \end{pmatrix},$$

если (e_i) – базис V, а (f_j) – базис W, то $(e_i \otimes f_j)$ – базис $V \otimes W$ и

$$(\mathcal{R} \otimes \mathcal{S})(h)(e_i \otimes f_j) = \mathcal{R}(h)e_i \otimes \mathcal{S}(h)f_j = \lambda_i e_i \otimes \mu_j f_j = \lambda_i\mu_j(e_i \otimes f_j),$$

т.е.

$$(\mathcal{R}\otimes\mathcal{S})(h)=\begin{pmatrix}* & 0 & \cdots & \cdots & 0\\ 0 & \ddots & \ddots & \ddots & \vdots\\ \vdots & \ddots & \lambda_i\mu_j & \ddots & \vdots\\ \vdots & \ddots & \ddots & \ddots & 0\\ 0 & \cdots & \cdots & 0 & *\end{pmatrix}$$

■

Формула Клебша-Гордана.

Пусть $\mathcal{R}_n$ и $\mathcal{R}_m$ $(n\geq m)$ – неприводимые представления группы $SL_2(\mathbb{C})$. Поймем, как $\mathcal{R}_n\otimes\mathcal{R}_m$ разлагается на неприводимые слагаемые. Имеем: $\chi_{\mathcal{R}_n\otimes\mathcal{R}_m}=\chi_{\mathcal{R}_n}\chi_{\mathcal{R}_m}$,

$$\chi_{\mathcal{R}_n}(z)=\frac{z^{n+1}-z^{-n-1}}{z-z^{-1}},\qquad \chi_{\mathcal{R}_m}(z)=\frac{z^{m+1}-z^{-m-1}}{z-z^{-1}}=z^m+z^{m-2}+\cdots+z^{-m},$$

$$(z-z^{-1})\chi_{\mathcal{R}_n}(z)\chi_{\mathcal{R}_m}(z)=(z^{n+1}-z^{-n-1})(z^m+z^{m-2}+\cdots+z^{-m})=$$

$$=z^{n+m+1}+z^{n+m-1}+\cdots+z^{n-m+1}-(z^{n-m-1}+z^{n-m-3}+\cdots+z^{-n-m-1})$$

Тогда

$$\mathcal{R}_n\otimes\mathcal{R}_m\cong\mathcal{R}_{n+m}\oplus\mathcal{R}_{n+m-2}\oplus\mathcal{R}_{n+m-4}\oplus\cdots\oplus\mathcal{R}_{n-m}$$

Полученная формула называется *формулой Клебша-Гордана*.

Задача. Разложить на неприводимые слагаемые: $\mathcal{R}_1\otimes\mathcal{R}_2\otimes\mathcal{R}_3$.

Решение.

$$\mathcal{R}_1\otimes\mathcal{R}_2\otimes\mathcal{R}_3\cong(\mathcal{R}_3\oplus\mathcal{R}_1)\otimes\mathcal{R}_3\cong\mathcal{R}_3\otimes\mathcal{R}_3\oplus\mathcal{R}_1\otimes\mathcal{R}_3\cong$$

$$\cong\mathcal{R}_6\oplus\mathcal{R}_4\oplus\mathcal{R}_2\oplus\mathcal{R}_0\oplus\mathcal{R}_4\oplus\mathcal{R}_2\cong\mathcal{R}_6\oplus\mathcal{R}_4^{\oplus 2}\oplus\mathcal{R}_2^{\oplus 2}\oplus\mathcal{R}_0$$

■

Мы доказали формулу Клебша-Гордана, используя характеры. Поймем, что она означает с точки зрения теории представлений. Имеем:

$$V(n)\otimes V(m)\simeq V(n+m)\oplus V(n+m-2)\oplus\cdots\oplus V(n-m)$$

Попытаемся понять, какие подпространства в $V(n)\otimes V(m)$ отвечают неприводимым слагаемым в правой части разложения. Вспомним, что неприводимое представление однозначно определяется своим старшим вектором v_0. Пусть $v_0,v_1,\dots,v_n$ – базис $V(n)$,

$w_0, w_1, \dots, w_m$ – базис $V(m)$, тогда $v_i \otimes w_j$ – базис $V(n) \otimes V(m)$. Легко понять, что $v_0 \otimes w_0$ – старший вектор подпространства $V(n+m)$: это следует из общей формулы

$$\mathcal{X}(v_i \otimes w_j) = \mathcal{X}v_i \otimes w_j + v_i \otimes \mathcal{X}w_j,$$

при этом старший вес равен $n+m$: это следует из общей формулы

$$\mathcal{Z}(v_i \otimes w_j) = \mathcal{Z}v_i \otimes w_j + v_i \otimes \mathcal{Z}w_j = (n-2i)v_i + (m-2j)w_j =$$

$$= (n-2i+m-2j)(v_i \otimes w_j)$$

(продолжение см. в начале следующего семинара).

Семинар 20. Вычисление сферических функций Лапласа, многочлены Лежандра.

В конце прошлого семинара мы рассмотрели разложение $V(n) \otimes V(m)$ в прямую сумму:

$$V(n) \otimes V(m) \simeq V(n+m) \oplus V(n+m-2) \oplus \cdots \oplus V(n-m)$$

и установили, что $v_0 \otimes w_0$ – старший вектор подпространства $V(n+m)$ со старшим весом $n+m$. Теперь найдем старший вектор и его вес для подпространства $V(n+m-2)$. Должно быть выполнено:

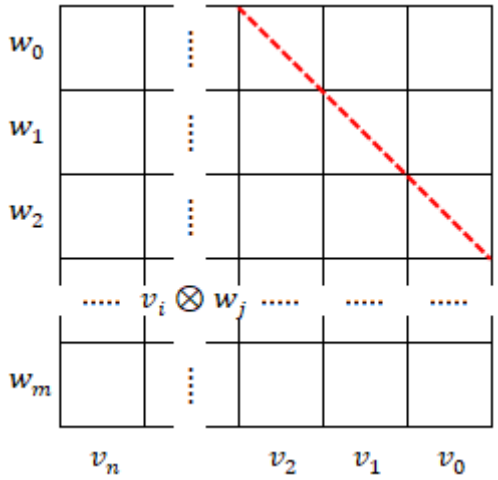
$$\mathcal{X}v = 0$$
$$\mathcal{Z}v = (n+m-2)v$$

Пусть $v = \sum_{i,j} c_{ij}\, v_i \otimes w_j$, тогда

$$\mathcal{Z}v = \sum_{i,j} c_{ij} \left(\mathcal{Z}v_i \otimes w_j + v_i \otimes \mathcal{Z}w_j\right) = \sum_{i,j} c_{ij} \Big((n-2i)v_i \otimes w_j + (m-2j)v_i \otimes w_j\Big) =$$

$$= \sum_{i,j} c_{ij}\,(n+m-2i-2j)\big(v_i \otimes w_j\big)$$

Заметим, что векторы одного веса расположены на одной диагонали в следующей таблице:



В частности, самый старший вес $(n+m)$ имеет отолько один вектор $v_0 \otimes w_0$. Вес $n+m-2$ имеют векторы $v_0 \otimes w_1$ и $v_1 \otimes w_0$, поэтому $v = av_0 \otimes w_1 + bv_1 \otimes w_0$. Найдем a и b (с точностью до пропорциональности) – для этого применим к v оператор $\mathcal{X}$:

$$\mathcal{X}v = av_0 \otimes \mathcal{X}w_1 + b\mathcal{X}v_1 \otimes w_0 = av_0 \otimes mw_0 + bnv_0 \otimes w_0 = (am + bn)v_0 \otimes w_0$$

Условие $\mathcal{X}v = 0$ будет выполнено, например, при $a = n$, $b = -m$, тогда

$$v = nv_0 \otimes w_1 - mv_1 \otimes w_0$$

Так можно найти старший вектор любого подпространства, встречающегося в разложении $V(n) \otimes V(m) \simeq V(n+m) \oplus V(n+m-2) \oplus \cdots \oplus V(n-m)$, а затем с помощью понижающих операторов получить базисы этих подпространств.

Вычисление сферических функций Лапласа.

На лекциях (см. курс лекций, лекции 20, 21) мы рассматривали гармонический анализ на сфере, и, в частности, ввели сферические функции Лапласа – они возникают как естественный базис в пространстве многочленов на сфере. Займемся их вычислением. Как было отмечено на лекциях,

$$A_n|_{S^2} = A_{n-2}|_{S^2} \oplus U_n$$

где A_n – инвариантное подпространство однородных многочленов степени n, $U_n = H_n|_{S^2} \simeq V(2n)$. Рассмотрим $\mathbb{C}[S^2]_{\leq n}$ – пространство многочленов на сфере степени не выше n. Имеет место разложение:

$$\mathbb{C}[S^2]_{\leq n} = \mathbb{C}[S^2]_{<n} \oplus U_n = \cdots = U_0 \oplus U_1 \oplus \cdots \oplus U_n$$

Сферические функции Лапласа $f_{n,0}, f_{n,1}, \ldots, f_{n,2n}$ образуют базис в $\mathbb{C}[S^2]_{\leq n}$, согласованный с этим разложением (например, $f_{n,n} \in U_n$ – сферическая функция веса 0, такие сферические функции принято называть зональными). Найдем $f_{n,n}$ – остальные сферические функции мы сможем найти, действуя повышающими и понижающими операторами. Имеем (пару вещественных координат x_2 и x_3 объединили в одну комплексную координату $z = x_2 + ix_3$):

$$f_{n,n} = \sum_{k+l+m=n} c_{klm}\, x_1^k z^l \bar{z}^m \Big|_{S^2}$$

Учитывая, что вес $f_{n,n}$ равен нулю, а вес элемента $x_1^k z^l \bar{z}^m$ равен $2(m-l)$, получаем

$$f_{n,n} = \sum_{k+2l=n} c_{kl}\, x_1^k z^l \bar{z}^l \Big|_{S^2}$$

На сфере: $z\bar{z} = x_2^2 + x_3^2 = 1 - x_1^2$, поэтому

$$f_{n,n} = \sum_{k+2l=n} c_{kl}\, x_1^k (1-x_1^2)^l \Big|_{S^2} = p_n(x_1)$$

Имеем: $\deg p_n \le n$, а так как функции $f_{n,n}$ ортогональны друг другу относительно инвариантного скалярного умножения на пространстве $A_n|_{S^2}$:

$$(f_1 \mid f_2) = \int_{S^2} \overline{f_1(x)}\, f_2(x) dx,$$

то они линейно независимы, следовательно, $\deg p_n = n$, и функции $p_0, p_1, \dots, p_n$ образуют базис пространства многочленов $\mathbb{C}[y]_{<n}$ (можно считать, что $p_n(y) = y^n + \cdots$).

Воспользуемся следующим фактом: если $f(x) = f(x_1)$, то перейдем к координатам (x_1, φ), где φ – угол в сечении сферы S^2 плоскостью, проходящей через точку с координатой $(x_1, 0,0)$ и параллельной плоскости Ox_2x_3:

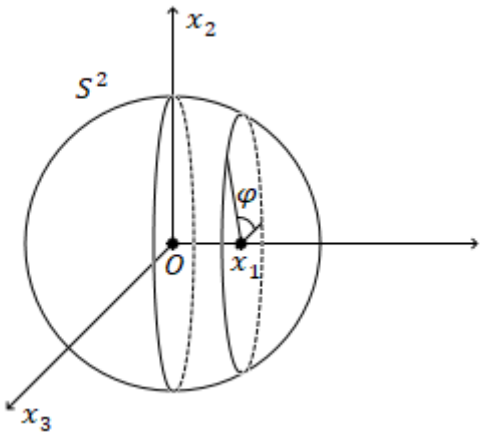


Рис. 20.1. Координаты (x_1, φ)

Если R – радиус сечения, то $R = \sqrt{1-x_1^2}$, замена координат:

$$\begin{aligned} x_1 &= x_1 \\ x_2 &= \sqrt{1-x_1^2}\sin\varphi \\ x_3 &= \sqrt{1-x_1^2}\cos\varphi \end{aligned}$$

тогда

$$r_{x_1} = \left(1, \frac{-x_1}{\sqrt{1-x_1^2}}\sin\varphi, \frac{-x_1}{\sqrt{1-x_1^2}}\cos\varphi\right), \qquad r_\varphi = \left(1, \sqrt{1-x_1^2}\cos\varphi, -\sqrt{1-x_1^2}\sin\varphi\right),$$

матрица Грама:

$$G = \begin{pmatrix} \dfrac{1}{1-x_1^2} & 0 \\ 0 & 1-x_1^2 \end{pmatrix}, \qquad \det G = 1,$$

поэтому

$$\int\limits_{S^2} f(x)\,dx = \int\limits_0^{2\pi} d\varphi \int\limits_{-1}^{1} dx_1\, f(x_1) = 2\pi \int\limits_{-1}^{1} f(x_1)dx_1$$

Получаем

$$(f_{n,n} \mid f_{m,m}) = 2\pi \int\limits_{-1}^{1} \overline{p_n(y)} p_m(y) dy$$

Так как $p_n(y) = y^n + \cdots$ и многочлены p_i ортогональны друг другу относительно этого скалярного умножения, то можно сказать, что последовательность $p_0, p_1, \ldots, p_n, \ldots$ получается из последовательности $1, y, \ldots, y^n, \ldots$ путем применения процесса ортогонализации Грама-Шмидта. Эти многочлены называются многочленами Лежандра.

Многочлены Лежандра.

Вычислим несколько первых многочленов Лежандра (при вычислении воспользуемся тем, что для k, l разной четности $(y^k \mid y^l) = 0$):

- $p_0(y) = 1$
- $p_1(y) = y - \dfrac{(y \mid p_0)}{(p_0 \mid p_0)} p_0 = y$
- $p_2(y) = y^2 - \dfrac{(y^2 \mid p_1)}{(p_1 \mid p_1)} p_1 - \dfrac{(y^2 \mid p_0)}{(p_0 \mid p_0)} p_0 = y^2 - \frac{1}{3}$
- $p_3(y) = y^3 - \dfrac{(y^3 \mid p_1)}{(p_1 \mid p_1)} p_1 = y^3 - \frac{3}{5} y$

Остальные сферические функции.

Сферические функции:

$$f_{n,2n}, f_{n,2n-1}, \ldots, \underbrace{f_{n,n}}_{\text{вес } 0}, \ldots, f_{n,1}, f_{n,0}$$

Функции справа от $f_{n,n}$ получаются с помощью применения к $f_{n,n}$ повышающих операторов $\mathcal{X}$, а функции слева – с помощью применения к $f_{n,n}$ понижающих операторов $\mathcal{Y}$. Осталось понять, как действуют эти операторы в пространстве многочленов на сфере. Имеем:

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad \exp(tX) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad \exp(tY) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

Рассмотрим присоединенное представление $Ad\colon SL_2(\mathbb{C}) \longrightarrow \mathfrak{sl}_2(\mathbb{C})$, (ранее мы уже обсуждали, что матрицы из $\mathfrak{sl}_2(\mathbb{C})$ имеют вид $\begin{pmatrix} ix_1 & z \\ -\bar{z} & -ix_1 \end{pmatrix}$, где $z = x_2 + ix_3$). Имеем:

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} ix_1 & z \\ -\bar{z} & -ix_1 \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} ix_1 - t\bar{z} & z - itx_1 \\ -\bar{z} & -ix_1 \end{pmatrix}\begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} ix_1 - t\bar{z} & -2itx_1 + t^2\bar{z} + z \\ -\bar{z} & t\bar{z} - ix_1 \end{pmatrix}$$

Т.е. точка $(x_1, x_2, x_3) = (x_1, z, \bar{z})$ под действием преобразования $g(t)^{-1}$, где $g(t) = \exp(tX)$ переходит в точку $(x_1 - it\bar{z}, z + 2itx_1 + t^2\bar{z}, \bar{z})$.

Поймем, как действует повышающий оператор $\mathcal{X}$ на произвольной функции:

$$(\mathcal{X}f)(x) = \frac{d}{dt}\Big|_{t=0} f(g(t)^{-1}x) = \frac{d}{dt}\Big|_{t=0} f(x_1 - it\bar{z}, z + 2itx_1 + t^2\bar{z}, \bar{z}) =$$

$$= -i\bar{z}\frac{\partial f}{\partial x_1} + 2ix_1\frac{\partial f}{\partial z}, \quad \text{т. е.} \quad \mathcal{X} = -i\bar{z}\frac{\partial}{\partial x_1} + 2ix_1\frac{\partial}{\partial z}$$

Аналогично

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}\begin{pmatrix} ix_1 & z \\ -\bar{z} & -ix_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}^{-1} = \begin{pmatrix} ix_1 & z \\ itx_1 - \bar{z} & tz - ix_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} ix_1 - tz & z \\ 2itx_1 - \bar{z} - t^2z & tz - ix_1 \end{pmatrix}$$

Т.е. точка $(x_1, x_2, x_3) = (x_1, z, \bar{z})$ под действием преобразования $g(t)^{-1}$, где $g(t) = \exp(tY)$ переходит в точку $(x_1 - it\bar{z}, z, 2itx_1 + \bar{z} + t^2z)$.

Поймем, как действует понижающий оператор $\mathcal{Y}$ на произвольной функции:

$$(\mathcal{Y}f)(x) = \frac{d}{dt}\Big|_{t=0} f(g(t)^{-1}x) = \frac{d}{dt}\Big|_{t=0} f(x_1 - it\bar{z}, z, 2itx_1 + \bar{z} + t^2z) =$$

$$= -iz\frac{\partial f}{\partial x_1} + 2ix_1\frac{\partial f}{\partial \bar{z}}, \quad \text{т. е.} \quad \mathcal{Y} = -iz\frac{\partial}{\partial x_1} + 2ix_1\frac{\partial}{\partial \bar{z}}$$

Итак,

$$f_{n,n}(x) = f_{n,n}(x, z, \bar{z}) = p_n(x_1)$$

$$f_{n,n-k} = \mathcal{X}^k\big(p_n(x_1)\big) = (-i)^k(\bar{z})^k p_n^{(k)}(x_1)$$

$$f_{n,n+k} = \mathcal{Y}^k\big(p_n(x_1)\big) = (-i)^k(z)^k p_n^{(k)}(x_1)$$

Семинар 21. Вычисления в алгебре Клиффорда. Алгебры Клиффорда размерностей 1 и 2. Отщепление двумерного подпространства.

Замечание. Уточним доказательство, приведенное на лекции (см. лекцию 23, предложение 2):

$$Ad(g)|_V = (-1)^l Ad(v_1 \cdots v_l)|_V$$

Если l нечетно, то $g^{-1}v_1 \cdots v_l \in Cl^-(V)$ и антикоммутирует с V – такое может быть выполнено, только если $g^{-1}v_1 \cdots v_l = \lambda e_1 \cdots e_n$ и n четно. Отсюда следует, что $\underbrace{g}_{\text{четный элемент}} = \frac{1}{\lambda}\underbrace{v_1 \cdots v_l e_n \cdots e_1}_{\text{нечетный элемент}}$ – противоречие.

Задача. Пусть $V = \langle e_1, e_2, e_3 \rangle$, скалярное умножение на V задано матрицей

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}.$$

Вычислить в $Cl(V)$:

$$(e_1 + e_2)(e_1 + e_3)(e_2 + e_3).$$

Решение.

$$(e_1 + e_2)(e_1 + e_3)(e_2 + e_3) = (e_1^2 + e_1e_3 + e_2e_1 + e_2e_3)(e_2 + e_3) =$$

$$= (e_1e_3 - e_1e_2 + e_2e_3)(e_2 + e_3) = e_1e_3e_2 - e_1e_2^2 + e_2e_3e_2 + e_1e_3^2 - e_1e_2e_3 + e_2e_3^2 =$$

$$= -e_1e_2e_3 - 2e_1 - e_1 - e_2^2e_3 - 2e_2 + e_1 - e_1e_2e_3 + e_2 = -2e_1 - e_2 - e_3 - 2e_1e_2e_3$$

■

Алгебры Клиффорда малых размерностей.

- $\dim V = 1$

$$Cl(V) = K[e]/(e^2 - \lambda)$$

- если $\nexists \sqrt{\lambda} \in K$, то $Cl(V) = K[e]/(e^2 - \lambda) \simeq K(\alpha)$, где α – корень многочлена $x^2 - \lambda$. Если же $\lambda = \mu^2$, то $Cl(V) = K[e]/(e - \mu)(e + \mu) \simeq K \oplus K$.

- $\dim V = 2$

Пусть $\{i, j\}$ – ортогональный базис пространства V, тогда $Cl(V) = \langle 1, i, j, ij = k \rangle$. Обозначим $(i \mid i) = \alpha$, $(j \mid j) = \beta$, тогда $i^2 = \alpha$, $j^2 = \beta$, $ij = -ji$, т.е. $Cl(V) = D(\alpha, \beta)$ – обобщенная алгебра кватернионов, задаваемая параметрами α и β.

Случай $K = \mathbb{R}$ или $\mathbb{C}$.

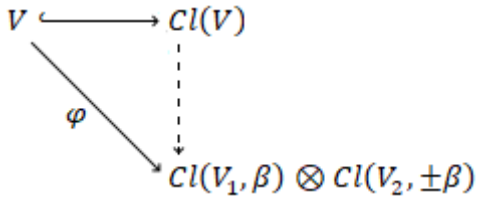
- Если $K = \mathbb{R}$, то с точностью до изоморфизма для каждого $n = \dim V$ алгебра Клиффорда имеет вид $Cl(V) = Cl_{p,q}$, где $n = p + q$, скалярное умножение имеет сигнатуру (p, q).
- Если $K = \mathbb{C}$, то с точностью до изоморфизма для каждого $n = \dim V$ алгебра Клиффорда имеет вид $Cl(V) = Cl_n$. При этом легко видеть, что в подходящих координатах любую комплексную алгебру Клиффорда можно записать как вещественную алгебру Клиффорда сигнатуры (p, q).

Задача. Пусть $V = V_1 \oplus V_2$, где $V_1 \perp V_2$ и $\dim V_1 = 2$. Тогда

$$Cl(V, \beta) \simeq Cl(V_1, \beta) \otimes Cl(V_2, \pm\beta),$$

где знак $\pm$ выбирается следующим образом: “+”, если $\beta|_{V_1}$ имеет сигнатуру $(1,1)$, и “−”, если $\beta|_{V_1}$ имеет сигнатуру $(2,0)$ или $(0,2)$.

Схема доказательства.
Воспользуемся вложением $V \hookrightarrow Cl(V)$ и универсальным свойством: построим отображение φ: $V \longrightarrow Cl(V_1, \beta) \otimes Cl(V_2, \pm\beta)$, которое даст нам изоморфизм $Cl(V) \longrightarrow Cl(V_1, \beta) \otimes Cl(V_2, \pm\beta)$:



Отображение φ строим так:

$$V_1 \ni v_1 \mapsto v_1 \otimes 1,$$
$$V_2 \ni v_2 \mapsto e_1 e_2 \otimes v_2,$$

где e_1, e_2 – ортонормированный базис пространства V_1. Легко видеть, что отображение φ обладает свойством $\varphi(v)^2 = (v \mid v)$. Тогда по универсальному свойству алгебры Клиффорда существует гомоморфизм $Cl(V) \longrightarrow Cl(V_1, \beta) \otimes Cl(V_2, \pm\beta)$. Это сюръективный гомоморфизм (так как в его образе лежат все порождающие элементы

тензорных сомножителей), также размерности $Cl(V)$ и $Cl(V_1, \beta) \otimes Cl(V_2, \pm\beta)$ совпадают (и равны 2^n), поэтому гомоморфизм $Cl(V) \longrightarrow Cl(V_1, \beta) \otimes Cl(V_2, \pm\beta)$ является изоморфизмом. ■

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ