ТЕОРИЯ ГАЛУА

М. Вербицкий

Данный текст представляет собой заново скомпилированную 28 февраля 2024 года третьим лицом версию оригинальных материалов курса 2013 года на факультете математики ВШЭ.

Краткое оглавление

Подробное оглавление

Нулевая глава

Предисловие

Данный текст представляет собой заново скомпилированную третьим лицом версию оригинальных материалов курса М. Вербицкого 2013 года на факультете математики ВШЭ, которые доступны по следующей ссылке: `http://verbit.ru/MATH/GALOIS-2013/` (дата обращения 23 февраля 2024 года).

Форматирование

В целом, стиль оформления старается быть похожим на стиль оригинала, однако цели сделать его 100% совпадающим не ставилось.

Номера страниц в оглавлениях кликабельны, как и ссылки на задачи, теоремы и тому подобное в листочках. Номера страниц в верхних колонтитулах кликабельны и ссылаются на краткое оглавление.

Глава 1

Текстовая лекция

Лекция 1: геометрический смысл теории Галуа

Версия 1.2, 25.01.2013.

В этой лекции я расскажу вкратце, в чем состоит предмет теории Галуа. За определениями и разъяснением основных понятий лучше обращаться в следующие лекции, здесь только обзор. Доказательства тоже там.

Предмет теории Галуа

Сейчас я дам определение основных понятий теории Галуа, и перечислю главные теоремы. Теория Галуа содержит много других теорем, но если вы хорошо понимаете доказательство главных утверждений, все остальное будет уже нетрудно. Результатом изучения теории Галуа должно быть тесное знакомство с этими утверждениями и их доказательствами.

Определение 1. Пусть k – поле. **Расширение** k есть поле K, содержащее k; отношение «K является расширением k» обозначается $[K : k]$. **Конечное расширение** есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k. Элемент

K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

Определение 2. Поле k называется **алгебраически замкнутым**, если любой многочлен $P(t) \in k[t]$ положительной степени имеет корень в k. Расширение $[\bar{k} : k]$ называется **алгебраическим замыканием** k, если $\bar{k}$ алгебраически замкнуто, а все элементы $\bar{k}$ алгебраичны над k.

Пример 1. Основная теорема алгебры утверждает, что поле $\mathbb{C}$ комплексных чисел алгебраически замкнуто.

Вопрос 1. Я знаю 4 доказательства этой теоремы: одно топологическое и использует свойства фундаментальной группы проколотого диска, другое, тоже топологическое, использует теорему Брауэра о неподвижной точке, третье, аналитическое, использует разложение полинома в ряд Тэйлора в окрестности минимума, и четвертое, алгебраическое, утверждает, что поле, где любой многочлен нечетной степени имеет корень, можно алгебраически замкнуть, если добавить корни всех квадратных полиномов. А сколько доказательств основной теоремы алгебры знаете вы?

Пример 2. Рассмотрим множество всех элементов $\mathbb{C}$, алгебраических над $\mathbb{Q}$. Это множество образует поле, которое обозначается $\bar{\mathbb{Q}}$, и называется **алгебраическим замыканием** $\mathbb{Q}$.

Теорема 1. Пусть k – поле. Тогда алгебраическое замыкание $[\bar{k} : k]$ существует, и единственно с точностью до изоморфизма. Более того, любой автоморфизм k продолжается до автоморфизма $\bar{k}$, сохраняющего k.

Определение 3. Пусть $[K : k]$ – расширение полей. **Автоморфизм** K есть биективное отображение, сохраняющее сложение и умножение. **Автоморфизм** K **над** k есть автоморфизм K, действующий тождественно на $k \subset K$.

Замечание 1. Группа автоморфизмов K над k обозначается $\mathrm{Aut}_k(K)$. Это одно из основных понятий теории Галуа.

Определение 4. Пусть группа G действует на множестве S. Множество точек, которые сохраняются G, обозначается S^G. Когда S – векторное пространство, это множество называется **пространство инвариантов действия** G.

Главным предметом теории Галуа являются расширения Галуа. Расширения Галуа можно определить множеством разных способов. Вот некоторые из них. Чтобы не усложнять формулировки, я потребую характеристики 0.

Теорема 2. Пусть $[K : k]$ – конечное расширение полей характеристики 0. Тогда следующие условия равносильны.

(i) Пусть $G = \mathrm{Aut}_k K$. Тогда $k = K^G$.

(ii) Пусть $P(t) \in k[t]$ – неприводимый полином над k, имеющий хотя бы один корень в K. Тогда $P(t)$ разложим над K: $P(t) = \prod_i (t-\alpha_i)$, где все α_i лежат в K.

(iii) Тензорное произведение $K \otimes_k K$ изоморфно прямой сумме нескольких копий K.

(iv) Порядок группы $\mathrm{Aut}_k K$ равен степени расширения $[K : k]$.

Определение 5. Если верно одно из этих условий, $[K : k]$ называется **расширением Галуа**. Группа $\mathrm{Aut}_k K$ в такой ситуации называется **группой Галуа**.

Теорема 3. (основная теорема теории Галуа)
Пусть $[K : k]$ – расширение Галуа. Тогда существует биекция между подгруппами в $\mathrm{Aut}_k K$ и расширениями $[K' : k]$, лежащими в K. Эта биекция задается $G \mapsto K^G$. При этом, $[K^G : k]$ является расширением Галуа тогда и только тогда, когда подгруппа $G \subset \mathrm{Aut}_k K$ нормальна.

Важное следствие основной теоремы теории Галуа - «теорема о примитивном элементе».

Определение 6. Пусть $[K : k]$ – конечное расширение. Элемент $x \in K$ называется **примитивным**, если он порождает поле K, то есть если минимальное подполе K, содержащее x, равно K.

Теорема 4. (теорема о примитивном элементе)
Пусть $[K : k]$ – расширение Галуа. Тогда в K существует примитивный элемент.

Доказывать эту теорему проще, если поле k бесконечно. Понятно, что $x \in K$ примитивен, если он не лежит в собственном подполе $K' \subsetneq K$. Но таких подполей – конечное число, потому что группа Галуа имеет конечное число подгрупп, и они все являются конечномерными подпространствами в K.

Значит, теорема о примитивном элементе (для бесконечного поля) – следствие следующего простого утверждения, которое я оставлю в качестве упражнения.

Упражнение 1. Пусть V – конечномерное векторное пространство над бесконечным полем, а $V_1, ..., V_n \subset V$ – конечный набор пространств положительной коразмерности. Тогда дополнение $V \setminus \bigcup V_i$ непусто.

Большинство утверждений теории Галуа выводятся (обыкновенно - весьма просто) из основной теоремы.

Вот несколько полезных теорем, которые хорошо освоить (желательно помнить их вместе с доказательством).

Теорема 5. Пусть $[K : k]$ – расширение Галуа с циклической группой Галуа порядка n. Предположим, что k содержит все корни степени n из 1, то есть что многочлен $x^n - 1$ разлагается в K на линейные множители. Тогда $K = k[\sqrt[n]{a}]$: K получается из k добавлением корня n-й степени из a.

Замечание 2. Такое расширение называется **расширением Куммера**.

Определение 7. Коммутатор группы G есть подгруппа $[G, G] \subset G$, порожденная элементами вида $xyx^{-1}y^{-1}$. **Производный ряд** группы G_0 есть ряд вида $G_0 \supset G_1 \supset ...$, где $G_i = [G_{i-1}, G_{i-1}]$. **Разрешимая группа** есть группа, производный ряд который заканчивается тривиальной группой $\{e\}$.

Определение 8. Поле разложения неприводимого многочлена $P(t) \in k[t]$ положительной степени есть минимальное расширение $[K : k]$ такое, что многочлен $P(t)$ разлагается в K на линейные множители.

Замечание 3. Существование такого расширения не сразу очевидно; тем не менее, оно существует, единственно с точностью до изоморфизма, и является расширением Галуа. Это еще одно утверждение, которое надо уметь доказывать.

Определение 9. Группа Галуа неприводимого многочлена $P(t) \in k[t]$ есть группа Галуа его поля разложения.

Определение 10. Полиномиальное уравнение $P(t) = 0$, $P(t) \in k[t]$, называется **разрешимым в радикалах над** k, если оно имеет решение в поле $[K : k]$, которое получено последовательными расширениями $[K = K_0 : K_1 : K_2 : ... : K_{N-1} : K_N = k]$, причем каждое $[K_i : K_{i+1}]$ есть поле разложения для многочлена $P(t) = t^n - a$.

Замечание 4. Иначе говоря, уравнение разрешимо в радикалах, если его решение можно выразить через алгебраические операции и операцию взятие корня.

Следующая теорема (доказанная Абелем) является одним из величайших достижений алгебры.

Теорема 6. Пусть $P(t)$ – неприводимый полином над полем k, а G – его группа Галуа. Уравнение $P(t) = 0$ разрешимо в радикалах тогда и только тогда, когда группа Галуа многочлена $P(t)$ разрешима.

Следствие 1. Существует полиномиальное уравнение степени 5 над $\mathbb{Q}$, которое не разрешимо в радикалах.

Действительно, можно без особенных усилий реализовать симметрическую группу S_5 в качестве группы Галуа некоторого уравнения степени 5; а эта группа не разрешима; доказательство этого чуть менее просто, но весьма элементарно.

Накрытия Галуа

Теория Галуа весьма мало отличается от теории накрытий, известной из топологии. Существует абстрактная (категорная) версия теории Галуа, в которой доказательство основной теоремы теории Галуа получается как следствие небольшого количества аксиоматических условий, которым удовлетворяют и расширения полей, и накрытия. Излагая

теорию Галуа в этом курсе, я буду рассказывать такие версии доказательств, которые легко сводятся к абстрактной версии. Таким образом, внимательный читатель сможет заодно изучить основы теории Галуа для накрытий.

Все топологические пространства в этом разделе предполагаются хаусдорфовыми, локально линейно связными и локально односвязными. Это условия, которые нужны для применения принципа накрывающей гомотопии. Также, я буду считать, что пространство M (которое служит базой накрытий) связно.

Определение 11. Пусть M, $\tilde{M}$ — топологические пространства, а $\pi : \tilde{M} \longrightarrow M$ непрерывное отображение. π называется **этальным**, если у каждой точки $\tilde{x} \in \tilde{M}$ есть окрестность $\tilde{U} \ni \tilde{x}$ такая, что

$$\pi|_{\tilde{U}} : \tilde{U} \longrightarrow \pi(\tilde{U})$$

это гомеоморфизм. Это отображение называется **накрытием**, если у каждой точки $x \in M$, есть окрестность $U \ni x$ такая, что $\pi^{-1}(U)$ гомеоморфно $U \times S$, где S — топологическое пространство с дискретной топологией, а отображение $\pi|_{\pi^{-1}(U)} : \pi^{-1}(U) \longrightarrow U$ при таком изоморфизме совпадает с проекцией $U \times S \longrightarrow U$. **Базой накрытия** называется M, а его **слоем** над точкой x — прообраз $\pi^{-1}(x)$. Накрытие $M_1 \longrightarrow M$ обозначается $[M_1 : M]$.

Замечание 5. Пусть $U \subset X$ — открытое подмножество, которое не является замкнутым. Отображение вложения $j : U \longrightarrow X$ этально, но не является накрытием (проверьте).

Пример 3. Отождествим окружность S^1 с одномерным тором $\mathbb{R}/2\pi\mathbb{Z}$. Естественная проекция $\mathbb{R} \longrightarrow S^1$ является накрытием (докажите). Проекция $\mathbb{R}^n$ на тор $T^n = \mathbb{R}^n/\mathbb{Z}^n$ также является накрытием (докажите это).

Определение 12. Пусть G — группа, действующая на топологическом пространстве M. Говорится, что действие G **вполне разрывно**, если у каждой точки $x \in M$ есть окрестность U такая, что $U \cap gU = \emptyset$ для любого $g \in G$ такого, что g действует не тождественно в окрестности U.

Пример 4. Пусть G — группа, вполне разрывно действующая на топологическом пространстве M. Тогда проекция $M \xrightarrow{\pi} M/G$ является накрытием.

Определение 13. Автоморфизм накрытия $[M_1 : M]$ есть гомеоморфизм, коммутирующий с проекцией на M.

На накрытиях определены две операции, которые коммутативны и ассоциативны: это произведение и несвязная сумма, которую также называют копроизведением.

Определение 14. Пусть $[M_1 : M]$, $[M_2 : M]$ – накрытия M. Рассмотрим расслоенное произведение $M_1 \times_M M_2 \subset M_1 \times M_2$, состоящее из всех $(x, y) \in M_1 \times M_2$, которые проектируются в одну и ту же точку M. Тогда $M_1 \times_M M_2$ называется **произведением накрытий**.

Замечание 6. Произведение $M_1 \times_M M_2$ является накрытием M.

Определение 15. Пусть $[M_1 : M]$, $[M_2 : M]$ – накрытия M. Несвязное объединение $M_1 \coprod M_2$ называется **несвязной суммой**, или же **копроизведением** накрытий.

Легко видеть, что несвязная сумма дистрибутивна относительно умножения накрытий.

Упражнение 2. Пусть $[M_1 : M]$ – связное накрытие. Докажите, что следующие условия равносильны.

(i) Группа автоморфизмов накрытия $[M_1 : M]$ действует транзитивно на слоях (то есть прообразах точек M).

(ii) Произведение $M_1 \times_M M_1$ изоморфно (как накрытие) несвязной сумме нескольких копий M_1.

Определение 16. Накрытие, удовлетворяющее какому-то из условий предыдущего упражнение, называется **накрытием Галуа**, а группа $\mathrm{Aut}[M_1 : M]$ – его группой Галуа, или группой монодромии (по-английски: «deck transformation group»).

Основная теорема теории Галуа для накрытий формулируется так.

Теорема 7. Пусть $[M_1 : M]$ – накрытие Галуа, а $G = \mathrm{Aut}[M_1 : M]$ – его группа Галуа. Тогда существует биекция между подгруппами G и накрытиями $[M_1 : M_2 : M]$. При этой биекции подгруппа $G' \subset G$ соответствует накрытию M_1/G'.

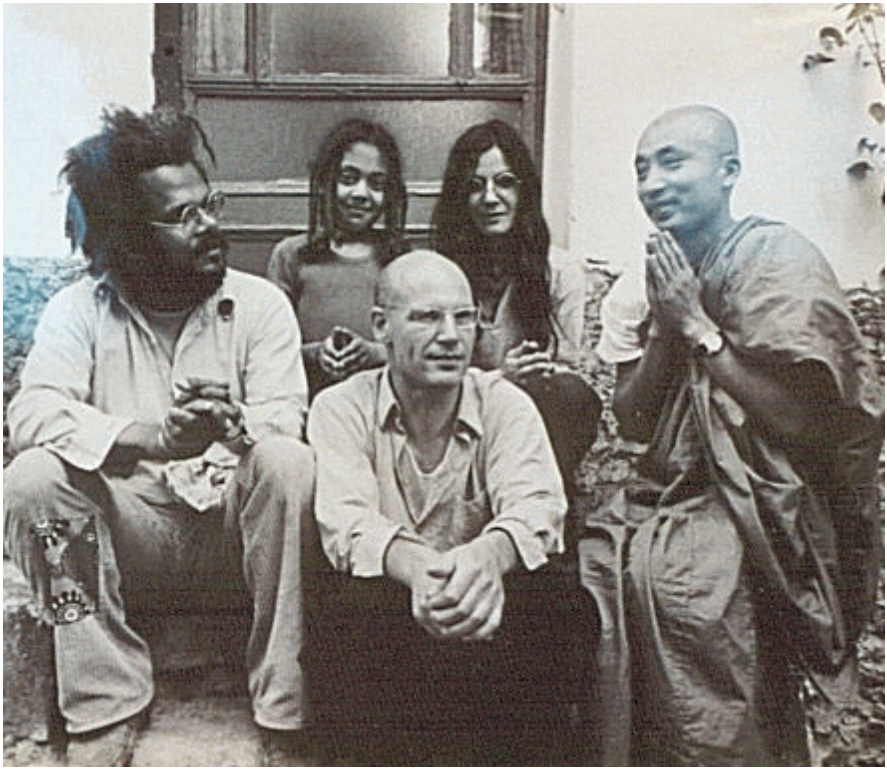
Теория Галуа в алгебре и геометрии: сравнительная табличка

Геометрия	**Алгебра**
Связное накрытие $[M_1 : M]$	Расширение полей $[K : k]$
Накрытие $[M_1 : M]$, которое не обязательно связно	Алгебра, изоморфная прямой сумме полей $[K_i : k]$
Несвязное объединение накрытий	Прямая сумма алгебр
Произведение накрытий	Тензорное произведение алгебр
Накрытие Галуа	Расширение Галуа
Универсальное накрытие	Алгебраическое замыкание
Накрытие Галуа есть такое накрытие $[M_1 : M]$, что $M' \times_M M' = \coprod^i M'$	Расширение Галуа есть такое расширение $[K : k]$, что $K \otimes_k K = \bigoplus^i K$
Взятие фактора M_1/G по подгруппе $G \subset \mathrm{Aut}[M_1 : M]$ группы автоморфизмов $[M_1 : M]$	Взятие пространства инвариантов K^G подгруппы $GH \subset \mathrm{Aut}[K : k]$ группы автоморфизмов $[K : k]$
Основная теорема теории Галуа	
$[M' : M]$ – накрытие Галуа. Тогда промежуточные накрытия $[M' : M'' : M]$ биективно соответствуют подгруппам в $\mathrm{Aut}[M' : M]$	$[K : k]$ – расширение Галуа. Тогда промежуточные расширения $[K : K' : k]$ биективно соответствуют подгруппам в $\mathrm{Aut}[K : k]$
подгруппа $G \subset \mathrm{Aut}[M' : M]$ соответствует фактору M'/G	подгруппа $G \subset \mathrm{Aut}[K : k]$ соответствует пространству инвариантов K^G.

Заключительные замечания

Аксиоматический подход к теории Галуа (включающей в себя обычную теорию Галуа и теорию Галуа накрытий) опубликован в SGA1 (Revêtements étales et groupe fondamental, Séminaire de Géométrie Algébrique

1),[1] за авторством Александра Гротендика и Мишель Рейно, которая была его студенткой.



Alexander Grothendieck
(род. 28 марта 1928)

Гротендик определяет специальный класс категорий, которые он называет «категории Галуа», и доказывает, что в рамках этой теории можно определить все конструкции, которые определяются в обычной теории Галуа или теории Галуа для накрытий, и доказать основную теорему теории Галуа. Также он доказывает, что категория Галуа есть категория множеств с действием группы; это позволяет явно выписать фундаментальную группу или группу $\mathrm{Aut}[\bar{k} : k]$, исходя из данных соответствующей категории Галуа.

В следующих томах SGA этот же подход применялся для определения гомотопического класса многообразия (в частности, его когомологий), пользуясь конструкциями из коммутативной алгебры; эта наука

[1] `http://arxiv.org/abs/math/0206203`

называется «этальные когомологии». С помощью «этальных когомологий» можно говорить о топологическом устройстве многообразия над полем конечной характеристики, или, например, кольца $\mathbb{Z}$.

Глава 2

Листки с задачами

Листок 1: алгебраические числа

Впервые выдано 18.01.2013. Версия 1.2, 25.01.2013.

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Алгебраические числа

Определение 1. Пусть $k \subset K$ – поле, содержащееся в поле K (в такой ситуации говорится, что k **подполе** в K, а K **расширение** k). Элемент $x \in K$ называется **алгебраическим над** k, если x – корень ненулевого многочлена с коэффициентами в k.

Довольно часто, когда говорят про алгебраические числа, подразумевают комплексные числа, алгебраические над $\mathbb{Q}$, т.е. корни многочленов с рациональными коэффициентами.

Задача 1. Пусть k – подполе в K, а x – элемент в K. Рассмотрим K как линейное пространство над k. Пусть $K_x \subset K$ – линейное подпространство K, порожденное степенями x. Докажите, что K_x конечномерно тогда и только тогда, когда x алгебраично.

Замечание 1. Если $k \subset K$ подполе K, а V, W - линейные пространства над K, мы можем рассмотреть V, W как линейные пространства V_k, W_k над k. В такой ситуации, линейное отображение $V_k \longrightarrow W_k$ называется **k-линейным отображением пространства V в W.** Линейные отображения векторных пространств над полем k часто называют **k-линейными**, чтобы обозначить зависимость от k.

Задача 2. Пусть $k \subset K$ - подполе K. Приведите пример отображения K-векторных пространств $V \longrightarrow W$, которое k-линейно, но не K-линейно.

Задача 3. Пусть k – подполе в K, x – алгебраический элемент в K, а $K_x \subset K$ – линейное подпространство, порожденное степенями x. Для ненулевого вектора $v \in K_x$, рассмотрим операцию m_v домножения на v в K. Докажите, что m_v – k-линейное отображение, которое сохраняет подпространство $K_x \subset K$.

Задача 4. В условиях предыдущей задачи, докажите, что ограничение гомоморфизма m_v на $K_x \subset K$ обратимо.

Задача 5 (!). Выведите из этого, что K_x – подполе в K.

Определение 2. Конечное расширение поля k – это поле $K \supset k$, которое конечномерно как векторное пространство над k.

Задача 6. Пусть $K_1 \supset K_2 \supset K_3$ поля, такие, что K_1 конечномерно над K_2, которое конечномерно над K_3. Докажите, что K_1 – конечное расширение K_3.

Задача 7 (!). Выведите из этого следующее: сумма, произведение, частное алгебраических над k элементов снова алгебраично над k.

Задача 8. Докажите, что любое конечное поле – конечное расширение поля остатков по модулю p для какого-то простого числа p. Выведите из этого, что конечное поле имеет p^n элементов (для каких-то чисел p, n, где p простое).

Задача 9 (*). Докажите, что существует неалгебраическое комплексное число.

Задача 10 (**). а. Докажите, что вещественное число $0,0100010000000000000000001...$ (число нулей после i-й единицы равно 2^{2^i}) неалгебраично.

б. Докажите, что вещественное число число $0,0100100001000...$ (число нулей после i-й единицы равно 2^i) неалгебраично.

Задача 11 (*). Пусть комплексное число x алгебраично. Докажите, что его комплексно-сопряженное $\bar{x}$ тоже алгебраично.

Указание. Воспользуйтесь тем, что комплексное сопряжение есть автоморфизм $\mathbb{C}$, сохраняющий $\mathbb{Q}$.

Задача 12 (*). Пусть комплексное число $x = a + b\sqrt{-1}$ алгебраично. Докажите, что вещественные числа a и b алгебраичны.

Задача 13 (*). Докажите, что $\alpha := \sin(\frac{n\pi}{m})$ алгебраично (над $\mathbb{Q}$) для всех целых n, m.

Алгоритм Евклида и его применения

Задача 14. Пусть $P(t), Q(t) \in k[t]$ – полиномы положительной степени над полем k, не имеющие общих делителей. Докажите, что 1 можно выразить как линейную комбинацию P и Q над $k[t]$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Указание. Воспользуйтесь алгоритмом Евклида для полиномов (делением в столбик с остатком и индукцией).

Задача 15. Пусть $P(t)$ – неприводимый полином (не раскладывается в произведение многочленов положительной степени с коэффициентами из k), а произведение $Q(t)Q_1(t)$ делится на $P(t)$, где $Q(t)$, $Q_1(t)$ – ненулевые полиномы. Докажите, что $Q(t)$ или $Q_1(t)$ делится на $P(t)$.

Указание. Пусть $Q(t)$ не делится на $P(t)$. Воспользуйтесь предыдущей задачей, чтобы выразить 1 как линейную комбинацию $Q(t)$ и $P(t)$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Тогда $1 \cdot Q_1(t) = Q(t)Q_1(t)A(t) + P(t)B(t)Q_1(t)$ очевидно делится на $P(t)$.

Задача 16. Пусть $P(t)$ – многочлен над k. Рассмотрим кольцо $k[t]$ полиномов от t и факторпространство $k[t]/Pk[t]$ всех полиномов по полиномам, которые делятся на P. Докажите, что $k[t]/Pk[t]$ есть кольцо (относительно естественных операций умножения и сложения).

Задача 17. Докажите, что умножение на полином $Q(t)$ действует на $k[t]/Pk[t]$ как эндоморфизм (эндоморфизм это гомоморфизм из пространства в себя).

Задача 18. Пусть умножение на полином $Q(t)$ действует на $k[t]/Pk[t]$ нулем. Докажите, что Q делится на P в кольце $k[t]$.

Задача 19. Пусть $P(t)$ неприводим. Предположим, что $Q(t)$ – полином, который не делится на $P(t)$. Докажите, что оператор умножения m_Q на $Q(t)$ на пространстве $k[t]/Pk[t]$ – мономорфизм.

Указание. Пусть v лежит в ядре m_Q, а $Q_1(t)$ – полином, представляющий v. Тогда QQ_1 делится на P в силу утверждения предыдущей задачи. Воспользуйтесь алгоритмом Евклида для полиномов, чтобы получить, что Q делится на P либо Q_1 делится на P.

Задача 20 (*). Пусть $A : V \longrightarrow V$ - линейный оператор на конечномерном векторном пространстве. Докажите, что есть такой полином $P(t) = t^n + a_n t^{n-1} + ...$, что $P(A) = 0$. Всегда ли можно найти неприводимый полином $P(t)$ такой, что $P(A) = 0$?

Задача 21 (!). Пусть $P(t)$ неприводим. Докажите, что $k[t]/Pk[t]$ – поле.

Указание. Воспользуйтесь предыдущей задачей, чтобы доказать, что если Q не делится на P, то умножение на $Q(t)$ задает на $k[t]/Pk[t]$ обратимый линейный оператор.

Определение 3. Пусть $P(t)$ – неприводимый полином. Говорится, что поле $k[t]/Pk[t]$ есть **расширение, полученное добавлением корня** $P(t)$.

Определение 4. Алгебраическое расширение поля k – это такое поле $K \supset k$, что все элементы K алгебраичны над k.

Задача 22. Докажите, что любое конечное расширение алгебраично.

Задача 23 (*). Докажите, что не любое алгебраическое расширение конечно.

Листок 2: идеалы и идемпотенты

Впервые выдано 25.01.2013. Версия 1.3, 25.01.2013.

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Идеалы в кольцах

Замечание 1. Все кольца в дальнейшем предполагаются коммутативные, с единицей, и $1 \neq 0$. Все гомоморфизмы сохраняют 1. Все идеалы в кольце R по умолчанию предполагаются **нетривиальными**, то есть не равными R. Кольцо, содержащее поле k, называется **коммутативной k-алгеброй**, или **кольцом над** k.

Определение 1. Максимальный идеал в кольце есть идеал, который не содержится ни в каком большем.

Задача 1. Докажите, что идеал $I \subset R$ максимален тогда и только тогда, когда R/I – поле.

Определение 2. Элемент $r \in R$ в алгебре (или кольце) R называется **нильпотентным**, или **нильпотентом**, если $r^k = 0$, для какого-то $k \in \mathbb{N}$.

Задача 2. Пусть – конечномерное векторное пространство, а r, r' – нильпотентные элементы в алгебре $\mathrm{End}(V)$. Всегда ли $r + r'$ нильпотентен?

Задача 3. Рассмотрим множество всех нильпотентных элементов в кольце R. Докажите, что это идеал.

Определение 3. Этот идеал называется **нильрадикалом** кольца R.

Задача 4 (!). Рассмотрим фактор кольца $R/\mathfrak{n}$ по его нильрадикалу. Докажите, что в $R/\mathfrak{n}$ нет ненулевых нильпотентов.

Определение 4. Простой идеал есть такой идеал, что в факторе по нему нет делителей нуля.

Задача 5 (*). Пусть A – кольцо без нильпотентов. Докажите, что пересечение всех простых идеалов A равно 0.

Конечномерные кольца над полем

Определение 5. Пусть дана коммутативная алгебра R с единицей над полем k. Говорят, что R **артиново кольцо над полем** k, если R конечномерна как векторное пространство.

Задача 6. Пусть дан линейный оператор $A \in \operatorname{End} V$, где V конечномерно. Рассмотрим подалгебру в $\operatorname{End} V$, порожденную k и A. Докажите, что это артиново кольцо над k.

Задача 7 (!). Пусть R – артиново кольцо без делителей нуля. Докажите, что это поле.

Указание. Воспользуйтесь тем, что любой инъективный эндоморфизм конечномерного пространства сюръективен.

Задача 8. Докажите, что любой простой идеал в артиновом кольце максимален.

Указание. Воспользуйтесь предыдущей задачей.

Определение 6. Артиново кольцо R называется **полупростым**, если в нем нет ненулевых нильпотентов.

Определение 7. Пусть $R_1, \ldots, R_n$ – алгебры над полем. Возьмем прямую сумму $\oplus R_i$, с естественным (почленным) умножением и сложением. Получившаяся алгебра называется **прямой суммой** R_i, обозначается $\oplus R_i$.

Задача 9. Докажите, что прямая сумма полупростых артиновых колец полупроста.

Задача 10. Пусть v – элемент конечномерной алгебры R над k. Рассмотрим подпространство R, порожденное $1, v, v^2, v^3, \dots$ (для всех степеней v). Пусть оно n-мерно. Докажите, что $P(v) = 0$ для некоторого полинома $P = t^n + a_{n-1}t^{n-1} + \dots$ с коэффициентами из k. Докажите, что такой полином единственный.

Определение 8. Этот полином называется **минимальным полиномом** элемента v.

Задача 11. Пусть $v \in R$ – элемент артинова кольца над k, а $P(t)$ – его минимальный полином. Рассмотрим подалгебру R_v, порожденную v и k. Докажите, что R_v изоморфно кольцу $k[t]/P$ остатков по модулю P.

Определение 9. Пусть I - идеал в кольце. Рассмотрим идеал, порожденный мономами степени q: $x_1^{n_1}x_2^{n_2}...x_i^{n_i}$, $\sum_i n_i = q$, где все x_i лежат в I. Этот идеал обозначается I^q.

Задача 12 (**). Пусть R – артиново кольцо с единственным максимальным идеалом $\mathfrak{m}$. Рассмотрим функцию $\mathbb{N} \xrightarrow{\varphi} \mathbb{N}$, переводящую i в $\dim(\mathfrak{m}^i/\mathfrak{m}^{i+1})$. Число $d \in \mathbb{N}$ называется **строгим локальным максимумом**, если $\varphi(d) > \varphi(d-1)$ и $\varphi(d) > \varphi(d+1)$. Сколько строгих локальных максимумов может быть у φ?

Идемпотенты

Определение 10. Пусть $v \in R$ – такой элемент алгебры R, что $v^2 = v$. Тогда v называется **идемпотентом**.

Задача 13. Пусть $e \in R$ – идемпотент в кольце. Докажите, что $1 - e$ тоже идемпотент. Докажите, что произведение идемпотентов – идемпотент.

Задача 14. Пусть $e \in R$ – идемпотент в кольце. Рассмотрим пространство $eR \subset R$ (образ умножения на e). Докажите, что eR – подалгебра в R, e – единичный элемент в eR, и $R = eR \oplus (1-e)R$.

Задача 15 (!). Пусть $R = k[t]/P$, где P – полином, который разлагается в произведение попарно взаимно простых полиномов, $P = P_1P_2 \dots P_n$. Докажите, что в R есть n идемпотентов $e_1, \dots, e_n \subset R$, причем $e_iR \cong k[t]/P_i$.

Задача 16. Пусть R – полупростое артиново кольцо без неединичных идемпотентов. Докажите, что это поле.

Указание. Пусть R – не поле. Рассмотрите подалгебру $k[x] \subset R$, порожденную необратимым элементом $x \in R$, и примените к ней утверждение предыдущей задачи.

Определение 11. Говорят, что два идемпотента $e_1, e_2 \in R$ в коммутативной алгебре R **ортогональны**, если $e_1 e_2 = 0$.

Задача 17. Пусть $e_2, e_3 \in R$ – идемпотенты, причем $e_1 = e_2 + e_3$, а e_2 и e_3 ортогональны. Докажите, что e_1 – тоже идемпотент, причем $e_2, e_3 \in e_1 R$ и $e_1 R = e_2 R \oplus e_3 R$.

Задача 18. Пусть $\operatorname{char} k \neq 2$. Предположим, что e_1, e_2, e_3 – идемпотенты в артиновом кольце R над k, и $e_1 = e_2 + e_3$. Докажите, что e_2 и e_3 ортогональны.

Определение 12. Пусть R – артиново кольцо над полем k. Идемпотент e в R называется **неразложимым**, если нельзя найти такие ненулевые ортогональные идемпотенты e_2, e_3, что $e = e_2 + e_3$.

Задача 19 (!). Пусть R полупростое артиново кольцо, а e – неразложимый идемпотент. Докажите, что eR – поле.

Задача 20 (!). Пусть R – полупростое артиново кольцо над полем k, $\operatorname{char} k \neq 2$. Докажите, что 1 разлагается в сумму неразложимых ортогональных идемпотентов: $1 = \sum e_i$. Докажите, что это разложение единственно.

Указание. Для существования, возьмите какой-нибудь идемпотент $e \in R$, разложите $R = eR \oplus (1 - e)R$, и воспользуйтесь индукцией. Для единственности, перемножьте два возможных разложения 1.

Задача 21 (!). Пусть R – полупростое артиново кольцо над полем k, $\operatorname{char} k \neq 2$. Докажите, что R изоморфно прямой сумме полей.

Указание. Воспользуйтесь предыдущей задачей.

Задача 22 (**). Верно ли это, когда $\operatorname{char} k = 2$?

Задача 23 (*). Пусть R – артиново кольцо над полем k, $\operatorname{char} k \neq 2$, а $1 = e_1 + \cdots + e_n$ – разложение 1 в сумму неразложимых ортогональных идемпотентов. Докажите, что у R есть ровно n простых идеалов.

Определение 13. Пусть $I \subset R$ – идеал в кольце, удовлетворяющий $I^2 = I$. Такой идеал называется **идемпотентным**.

Задача 24 (**). Пусть I – идемпотентный идеал. Докажите, что I главный, или найдите контрпример.

Листок 3: Тензорные произведения полей и композиты

`Впервые выдано 01.02.2013. Версия 1.1, 23.01.2013.`

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Инвариантные билинейные формы и форма следа

При сдаче задач (кроме тех, где это специально оговорено или подразумевается), можно предполагать, что $\operatorname{char} k = 0$.

Определение 1. След линейного оператора есть сумма всех диагональных членов в каком-то матричном представлении.

Задача 1. Докажите, что след не зависит от выбора базиса, который применяется для матричного представления оператора.

Определение 2. Характеристический полином линейного оператора A есть полином $P(t) := \det(t\mathrm{Id} - A)$.

Задача 2. Пусть $A \in \operatorname{End} V$ – нильпотентный оператор. Докажите, что $\operatorname{tr}(A) = \det(A) = 0$, а характеристический полином $\operatorname{chpoly}_A(t) = t^{\dim V}$.

Определение 3. Пусть R – алгебра над полем k, а g – симметричная билинейная форма на R. Форма g называется **инвариантной**, если $g(x, yz) = g(xy, z)$ для любых x, y, z.

Замечание 1. Если R содержит единицу, то для любой инвариантной формы g, имеем $g(x, y) = h(xy, 1)$, то есть g определяется линейным функционалом.

Задача 3. Пусть R – артиново кольцо, снабженное билинейной инвариантной формой g, а $\mathfrak{m}$ – идеал в R. Докажите, что его ортогональное дополнение $\mathfrak{m}^\perp$ – тоже идеал.

Задача 4 (*). Найдите артиново кольцо, не допускающее невырожденной инвариантной билинейной формы.

Определение 4. Пусть R – артиново кольцо над полем k. Рассмотрим билинейную форму $a, b \longrightarrow \operatorname{tr}(ab)$, где $\operatorname{tr}(ab)$ – след эндоморфизма $L_{ab} \in \operatorname{End}_k R$, $x \xrightarrow{L_{ab}} abx$. Эта форма называется **формой следа**, и обозначается $\operatorname{tr}_k(ab)$.

Задача 5. Пусть $[K : k]$ – расширение полей характеристики 0. Докажите, что форма следа всегда невырождена.

Замечание 2. Расширения с невырожденной формой следа называются **сепарабельными**.

Задача 6 (*). Приведите пример конечного расширения $[K : k]$, которое несепарабельно.

Определение 5. Напомню, что **полупростое артиново кольцо** есть прямая сумма полей.

Задача 7 (!). Пусть R – артиново кольцо над k. Докажите, что если форма следа невырождена, то R полупросто. Докажите, что если R полупросто, а $\operatorname{char} k = 0$, то эта форма невырождена.

Указание. В одну сторону, воспользуйтесь задачей 2. В другую сторону, рассмотрите сначала ситуацию когда R – поле.

Тензорные произведения полей

Задача 8. Пусть A и B – кольца над полем k.

а. Докажите, что существует мультипликативная операция $(A \otimes_k B) \times (A \otimes_k B) \longrightarrow A \otimes_k B$, переводящая $a \otimes b, a' \otimes b'$ в $aa' \otimes bb'$.

б. Докажите, что эта операция задает структуру кольца над $A \otimes_k B$.

Определение 6. Это кольцо называется **тензорным произведением колец A и B**, и обозначается $A \otimes_k B$.

Задача 9. Пусть $k[t_1, t_2, ..., t_p]$, $k[u_1, u_2, ..., u_q]$ – кольца полиномов. Докажите, что $k[t_1, t_2, ..., t_p] \otimes_k k[u_1, u_2, ..., u_q] \cong k[t_1, t_2, ..., t_p, u_1, u_2, ..., u_q]$.

Задача 10. Пусть R, R' – артиновы кольца над k. Обозначим естественные билинейные формы $a, b \longrightarrow \operatorname{tr}(ab)$ на них через g, g'. Рассмотрим тензорное произведение $R \otimes R'$ с естественной структурой артинова кольца и форму $g \otimes g'$ на $R \otimes R'$. Докажите, что $g \otimes g'$ равна форме $a, b \longrightarrow \operatorname{tr}(ab)$.

Задача 11 (!). Докажите, что тензорное произведение полупростых артиновых колец над полем k характеристики 0 полупросто.

Указание. Воспользуйтесь задачей 7.

Задача 12 (!). Пусть $[K_1 : k]$, $[K_2 : k]$ – сепарабельные расширения. Докажите, что алгебра $K_1 \otimes_k K_2$ полупроста.

Задача 13. Докажите, что алгебра $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ полупроста, и разложите ее в прямую сумму полей.

Задача 14. Докажите, что алгебра $\mathbb{Q}[\sqrt{-1}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{-1}]$ полупроста, и разложите ее в прямую сумму полей.

Задача 15 (!). Пусть $P(t)$ и $Q(t)$ – полиномы над полем k. Обозначим $K_1 = k[t]/P(t)$ и $K_2 = k[t]/Q(t)$. Докажите, что $K_1 \otimes K_2 \cong K_1[t]/Q(t) \cong K_2[t]/P(t)$.

Задача 16. Пусть $P(t) \in \mathbb{Q}[t]$ – многочлен, у которого есть ровно r вещественных корней и ровно $2s$ комплексных, но не вещественных, причем все корни разные. Докажите, что

$$(\mathbb{Q}[t]/P) \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_s \mathbb{C} \oplus \bigoplus_r \mathbb{R}.$$

Задача 17 (**). Найдите два нетривиальных конечных расширения K_1, K_2 над $\mathbb{Q}$ таких, что $K_1 \otimes_{\mathbb{Q}} K_2$ – тоже поле.

Задача 18 (**). Найдите два конечных расширения K_1 и K_2 поля k характеристики p, что $K_1 \otimes K_2$ не полупросто, или докажите, что таких расширений нет.

Композит расширений

Задача 19. Пусть K_1, K_2 – расширения поля k характеристики 0. Постройте инъективное отображение из K_i в $K_1 \otimes_k K_2$.

Задача 20. Пусть $\varphi : K \longrightarrow R = \bigoplus R_i$ гомоморфизм из поля в прямую сумму колец, а $\pi_i : R \longrightarrow R_i$ – проекция. Докажите, что $\varphi \circ \pi_i : K \longrightarrow R_i$ инъективно.

Указание. Убедитесь, что $\varphi \circ \pi_i$ переводит 1 в 1.

Задача 21. Пусть R – артиново кольцо над полем k, а $\mathfrak{n}$ – его нильрадикал.

а. Пусть $\operatorname{char} k \neq 2$. Докажите, что $R/\mathfrak{n}$ – прямая сумма полей.

б. (*) Верно ли это, когда $\operatorname{char} k = 2$?

Задача 22. Пусть K_1, K_2 – расширения k, $\operatorname{char} k \neq 2$, причем одно из них конечное. Обозначим за $\mathfrak{n}$ нильрадикал произведения $K_1 \otimes_k K_2$, и пусть $R = K_1 \otimes_k K_2/\mathfrak{n}$.

а. (!) Докажите, что R допускает разложение в конечную прямую сумму, $R = \bigoplus L_i$, где L_i – расширения k.

б. Докажите, что каждая из компонент L_i допускает k-линейные гомоморфизмы $K_1 \hookrightarrow L_i$, $K_2 \hookrightarrow L_i$.

Определение 7. Каждое из полей L_i, построенных в предыдущей задаче, называется **композитом** расширений K_1 и K_2.

Задача 23. Пусть L – поле, допускающее k-линейные вложения $K_1 \longrightarrow L$, $K_2 \longrightarrow L$.

а. Докажите, что существует нетривиальный гомоморфизм $K_1 \otimes_k K_2 \longrightarrow L$.

б. Докажите, что существует k-линейный гомоморфизм $L_i \longrightarrow L$, где L_i – какой-то из композитов K_1, K_2.

Задача 24 (!). (универсальное свойство композита) Пусть K_1, K_2 – расширения k, $\operatorname{char} k \neq 2$, причем одно из них конечное, а L – расширение k, снабженное k-линейными гомоморфизмами $K_1 \xrightarrow{\varphi} L$, $K_2 \xrightarrow{\psi} L$. Предположим, что L порождено образами φ и ψ. Докажите, что L это композит K_1 и K_2.

Замечание 3. В дальнейшем, можно пользоваться этим свойством в качестве определения композита.

Задача 25 (!). Пусть $K = k[t]/P(t)$ – расширение, полученное добавлением корня неприводимого многочлена $P(t)$, а $P(t) = P_1(t)P_2(t)...P_k(t)$ – неприводимое разложение $P(t)$ над полем $K' \supset k$. Докажите, что композиты K и K' суть все поля вида $K'[t]/P_i(t)$.

Задача 26 (*). Найдите поля K_1, K_2 и их композиты L, L', которые неизоморфны.

Листок 4: Алгебраическое замыкание

`Впервые выдано 08.02.2013. Версия 1.2, 26.01.2013.`

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

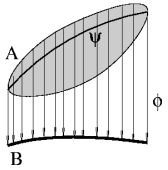
Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Вполне упорядоченные множества

При сдаче задач (кроме тех, где это специально оговорено или подразумевается), можно предполагать, что $\operatorname{char} k = 0$.

Определение 1. Пусть $\varphi : A \longrightarrow B$ сюръективное отображение множеств. **Сечением** отображения φ называется отображение $\psi : B \longrightarrow A$, такое, что $\psi \circ \varphi = \mathrm{Id}$.



Определение 2. Аксиома выбора утверждает, что каждое сюръективное отображение имеет сечение.

Определение 3. Пусть $(X, \prec)$ – линейно упорядоченное множество, а $Y \subset X$ – его подмножество. Элемент $y_0 \in Y$ называется **минимальным**, если для любого $y \in Y$, имеем $y_0 \preccurlyeq y$. Линейно упорядоченное множество называется **вполне упорядоченным** (well-ordered set), если любое его подмножество имеет минимальный элемент. Отношение порядка на таком множестве называется **отношение полного порядка**.

Определение 4. Начальным элементом вполне упорядоченного множества называется его минимальный элемент. **Отрезком** линейно упорядоченного множества $(X, \prec)$ называется подмножество $Y \subset X$ такое, что для любых $x, z \in Y$, и любого $y \in X$ такого, что $x \prec y \prec z$, имеем $y \in Y$. **Начальным отрезком** вполне упорядоченного множества называется отрезок, содержащий минимальный элемент.

Определение 5. Два вполне упорядоченных множества называются **изоморфными**, если между ними есть биекция, сохраняющая порядок. Классы изоморфизма вполне упорядоченных множеств называются **ординалами**, или же **ординальными числами**.

Задача 1 (!). Пусть X, Y – вполне упорядоченные множества. Докажите, что X изоморфно начальному отрезку Y, либо Y изоморфно начальному отрезку X.

Задача 2. Докажите, что такой изоморфизм определен однозначно.

Определение 6. Теорема Цермело утверждает, что любое множество может быть вполне упорядочено.

Задача 3. Выведите из теоремы Цермело аксиому выбора.

Указание. Возьмите минимальный элемент в $\psi^{-1}(b)$.

Определение 7. Пусть $(S, \prec)$ – частично упорядоченное множество. Элемент $x \in S$ называется **максимальным**, если не существует $y \in S$ с $x \prec y$. Для подмножества $S_1 \subset S$ и $x \in S$, мы пишем $S_1 \preccurlyeq x$, если для каждого $\xi \in S_1$ имеем $\xi \preccurlyeq x$. **Лемма Цорна** утверждает следующее. Пусть $(S, \prec)$ – частично упорядоченное множество, причем для любого вполне упорядоченного подмножества $S_1 \subset S$ найдется элемент $\xi \in S$ такой, что $S_1 \preccurlyeq \xi$. Тогда в S найдется максимальный элемент.

Задача 4. Выведите из леммы Цорна теорему Цермело.

Указание. Пусть A – множество, на котором мы хотим найти полный порядок. Рассмотрите в качестве S множество подмножеств A, снабженных полным порядком, а в качестве $\prec$ отношение "X есть начальный отрезок Y".

Задача 5 (**). Пусть – бесконечное множество. Докажите, что $X \times X$ равномощно X.

Задача 6 (!). Пусть α – ординал, а $N_1 > N_2 > N_3 > ...$ – последовательность строго убывающих элементов α. Докажите, что она конечна.

Замечание 1. В дальнейшем, при сдаче листков **вы можете пользоваться леммой Цорна и теоремой Цермело без доказательства.**

Задача 7. Пусть некоторое свойство P выполнено для некоторых элементов вполне упорядоченного множества X, причем P выполнено для $x \in X$, если оно выполнено для всех $y < x$. Докажите, что свойство P выполнено для всех $x \in X$

Замечание 2. Это утверждение есть форма принципа математической индукции, с той лишь разницей, что вместо индукции по множеству натуральных чисел, мы пользуемся индукцией по вполне упорядоченному множеству. Оно называется **принцип трансфинитной индукции**.

Направленные расширения

Напомню, что алгебраическое расширение $[K : k]$ есть расширение полей, такое, что все элементы K алгебраичны над k. Алгебраическое расширение не обязано быть конечным.

Задача 8. Пусть $[K_1 : k]$, $[K_2 : K_1]$ – расширения полей, $[K_1 : k]$ алгебраично, а $x \in K_2$ алгебраичен над K_1. Докажите, что x алгебраичен над k.

Указание. Докажите, что x является корнем многочлена с коэффициентами в K_1, и найдите конечное расширение $[K_1' : k]$, содержащее все эти коэффициенты.

Задача 9. Пусть α – ординал, а $K_0 \subset K_1 \subset K_2 \subset ...$ – возрастающая последовательность расширений, проиндексированных элементами α, такая, что $[K_i : \bigcup_{j<i} K_j]$ конечно.

а. Докажите, что все K_i алгебраичны над K_0.

б. Докажите, что $[\bigcup_{i\in\alpha} K_i : K_0]$ алгебраично.

Указание. Для (а), рассмотрим наименьший i, для которого K_i не алгебраично над K_0, и пусть $x \in K_i$. Поскольку x алгебраично над $\bigcup_{j<i} K_j$, является корнем многочлена с коэффициентами в $\bigcup_{j<i} K_j$, то есть в каком-то из полей K_{i_1} с $i_1 < i$; это поле уже алгебраично, по предположению индукции. Убедитесь, что в силу задачи 8, x алгебраичен над k.

Определение 8. В такой ситуации, расширение $[\bigcup_{i\in\alpha} K_i : K_0]$ называется **направленным алгебраическим расширением**, а выбор последовательности $K_0 \subset K_1 \subset K_2 \subset ...$, проиндексированной ординалом – **направленностью**. **Изоморфизм направленных алгебраических расширений** $[K : k]$ и $[K' : k]$ есть k-линейный изоморфизм $K \longrightarrow K'$, который переводит цепочку расширений, заданную для K, в аналогичную цепочку для K'.

Задача 10 (!). Пусть $[K : k]$ – алгебраическое расширение. Докажите, что K можно снабдить направленностью.

Указание. Пусть $\mathfrak{S}$ – множество промежуточных расширений $[K : K' : k]$, снабженных направленностью. Введем нас $\mathfrak{S}$ отношение частичного порядка таким образом: $K' \preccurlyeq K''$ если K' содержится в K'' в качестве элемента цепочки расширений, составляющих направленность, а направленность в K' является начальным сегментом направленности в K''. Примените лемму Цорна к $\mathfrak{S}$, и докажите, что максимальный элемент задает направленность на K.

Задача 11 (!). Пусть k – поле. Докажите, что классы изоморфизма всех расширений той же мощности, что и k, составляют множество.

Задача 12. Докажите, что классы изоморфизма направленных алгебраических расширений k составляют множество.

Задача 13. Рассмотрим на множестве $\mathfrak{R}$ классов изоморфизма направленных расширений $[K : k]$ следующее отношение частичного порядка: $K \prec K'$, если K изоморфно, как направленное алгебраическое расширение, сегменту в цепочке расширений, составляющих направленность для K'. Докажите, что существует максимальное направленное расширение.

Указание. Леммой Цорна воспользуйтесь же.

Определение 9. Алгебраически замкнутое поле есть такое поле K, что любой многочлен $P(t) \in K[t]$ положительной степени имеет корень в K. **Алгебраическое замыкание** поля k есть алгебраическое расширение $[\bar{k} : k]$, которое алгебраически замкнуто.

Задача 14 (!). Пусть поле K не допускает нетривиальных алгебраических расширений. Докажите, что оно алгебраически замкнуто.

Задача 15. Пусть $[K : k]$ – максимальное направленное алгебраически расширение поля k, построенное в задаче 13. Докажите, что K алгебраически замкнуто.

Указание. Воспользуйтесь предыдущей задачей.

Задача 16 (*). Пусть k – счетное поле. Докажите, что $\bar{k}$ можно получить как объединение возрастающей последовательности конечных расширений k.

Задача 17 (**). Пусть $[K : k]$ – расширение k, которое не обязательно алгебраично, а $P_1, ..., P_k \in k[t_1, ..., t_n]$ набор полиномов. Предположим, что уравнение $P_1(t_1, ..., t_n) = P_2(t_1, ..., t_n) = ... = P_n(t_1, ..., t_n)$ имеет решение в K. Докажите, что оно имеет решение в алгебраическом замыкании $\bar{k}$.

Единственность алгебраического замыкания

Здесь и в дальнейшем, $[\bar{k} : k]$ обозначает алгебраическое замыкание k.

Задача 18. Пусть $P(t) \in k[t]$ неприводимый многочлен над k, а $[K : k]$ расширение вида $K = k[t]/P$[1] Докажите, что тензорное произведение $\bar{k}$ и K есть прямая сумма нескольких копий $\bar{k}$: $\bar{k} \otimes_k K = \oplus\bar{k}$.

Задача 19 (!). Пусть $[K : k]$ – конечное расширение, $R := K \otimes_k \bar{k}$, а $\mathfrak{n}$ – нильрадикал R. Докажите, что $R/\mathfrak{n}$ есть прямая сумма нескольких копий $\bar{k}$.

Задача 20. а. Докажите, что любой k-линейный гомоморфизм $\bar{k} \to \bar{k}$ – изоморфизм.

б. Верно ли это без требования k-линейности?

Задача 21. Пусть R – прямая сумма нескольких копий $\bar{k}$, а $\bar{k} \longrightarrow R$ – k-линейный гомоморфизм. Докажите, что это композиция диагонального вложения и автоморфизма.

Указание. Воспользуйтесь тем, что гомоморфизм, по определению, переводит 1 в 1, и примените предыдущую задачу.

Задача 22. Пусть R – прямая сумма нескольких копий $\bar{k}$, а $R \longrightarrow K$ - k-линейный гомоморфизм на поле K. Докажите, это проекция на один из сомножителей.

Определение 10. Пусть R – кольцо, содержащее $\bar{k}$.[2] Кольцо R называется **поглощающим**, если каждый простой идеал $I \subset R$ максимален, и естественное отображение $\bar{k} \longrightarrow R/I$ – изоморфизм.

[1]Такое расширение называется **расширение, полученное добавлением корня многочлена** $P(t)$.

[2]В такой ситуации, также можно сказать «R – кольцо над $\bar{k}$».

Задача 23. Пусть R есть прямая сумма конечного числа копий $\bar{k}$. Докажите, что R – поглощающее.

Задача 24 (**). Пусть $R = \prod \bar{k}$ – произведение бесконечного числа копий k. Верно ли, что R – поглощающее?

Задача 25. Пусть $R_1 \subset R_2 \subset R_3 \subset ...$ набор вложенных друг в друга колец, а $I \subset R := \bigcup R_i$ – идеал. Докажите, что $R/I = \bigcup \left[R_i/I \cap R_i \right]$.

Задача 26 (!). Пусть $R_1 \subset R_2 \subset R_3 \subset ...$ – вполне упорядоченный набор вложенных друг в друга поглощающих колец. Докажите, что $R := \bigcup R_i$ тоже поглощающее.

Указание. Если $I \subset R$ – простой идеал, то $\bar{K} \longrightarrow R_i/(I \cap R_i)$ – изоморфизм для каждого i. Выведите из предыдущей задачи, что $R/I = \bigcup \left[R_i/I \cap R_i \right]$.

Задача 27. Пусть V – векторное пространство над полем k, $[K : k]$ – расширение, а $W \subset V \otimes_k K$ – подпространство. Докажите, что естественное отображение $[V/(W \cap V)] \otimes_k K \longrightarrow V \otimes_k K/W$ сюръективно.

Задача 28. Пусть $[\bar{k} : k]$ – алгебраическое замыкание, R – поглощающее кольцо над $\bar{k}$, а $[K : k]$ – конечное расширение. Докажите, что $R \otimes_k K$ – тоже поглощающее кольцо.

Указание. Пусть $I \subset R \otimes_k K$ – простой идеал. Воспользуйтесь предыдущей задачей, положив $W = I$, $V = R$, и примените задачу 19 и задачу 23.

Задача 29 (!). Пусть $[K : k]$ алгебраическое расширение (не обязательно конечное). Докажите, что кольцо $\bar{k} \otimes_k K$ – поглощающее.

Указание. Выберите направленность в K, и примените трансфинитную индукцию, воспользовавшись утверждением задачи 26 и задачи 28.

Задача 30 (!). Пусть $[\bar{k}_1 : k]$ и $[\bar{k}_2 : k]$ – алгебраические замыкания поля k. Постройте k-линейный изоморфизм между $\bar{k}_1$ и $\bar{k}_2$.

Указание. Воспользуйтесь предыдущей задачей.

Листок 5: Расширения Галуа

Впервые выдано 15.02.2013. Версия 1.4.1, 12.03.2013.

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Расширения Галуа

При сдаче задач (кроме тех, где это специально оговорено или подразумевается), можно предполагать, что $\operatorname{char} k = 0$.

Задача 1. Пусть задан полином $P(t) \in K[t]$ степени n с коэффициентами в поле K, у которого n попарно различных корней в K. Докажите, что кольцо $K[t]/P$ остатков по модулю P изоморфно прямой сумме n копий K.

Определение 1. Пусть $[K : k]$ – алгебраическое расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

Задача 2. Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в $K = k[t]/P$. Докажите, что $[K : k]$ – расширение Галуа.

Определение 2. Напомню, что конечное расширение $[K : k]$ **несепарабельно**, если форма следа $\operatorname{Tr}_k : K \longrightarrow k$ равна нулю.

Задача 3 (!). Пусть $[K : k]$ – конечное расширение полей. Докажите, что $[K : k]$ несепарабельно тогда и только тогда, когда $K \otimes_k K$ содержит нильпотенты.

Задача 4. Докажите, что $[\mathbb{Q}[\sqrt{-1}] : \mathbb{Q}]$ – расширение Галуа.

Задача 5. Пусть $[K : \mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). Докажите, что это расширение Галуа.

Задача 6 (!). Пусть p простое. Докажите, что для любого корня из единицы ζ степени p, $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ – расширение Галуа.

Задача 7 (*). Будет ли $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ расширением Галуа?

Задача 8 (**). Пусть $[K : \mathbb{Q}[\sqrt{-1}]]$ – расширение Галуа. Докажите, что $[K : \mathbb{Q}]$ – расширение Галуа, или найдите контрпример.

Задача 9 (*). Пусть F – поле характеристики p, а $k = F(z)$ – поле рациональных функций над F. Докажите, что полином $P(t) = t^p - z$ неприводим над k. Докажите, что $[k[t]/P : k]$ – не расширение Галуа.

Задача 10. Пусть $K_1 \supset K_2 \supset K_3$ – последовательность расширений полей. Докажите, что

$$K_2 \otimes_{K_3} K_1 \cong (K_2 \otimes_{K_3} K_2) \otimes_{K_2} K_1.$$

Задача 11. Рассмотрим расширение $[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}]$. Докажите, что это не расширение Галуа.

Задача 12 (*). Пусть $K_1 \supset K_2 \supset K_3$ - последовательность расширений полей, причем $[K_1 : K_2]$ и $[K_2 : K_3]$ - расширения Галуа. Докажите, что $[K_1 : K_3]$ – расширение Галуа, или найдите контрпример.

Указание. Воспользуйтесь предыдущей задачей.

Задача 13. Докажите, что $\mathbb{Q}[\sqrt[3]{2}, \frac{\sqrt{-3}-1}{2}]$ – расширение Галуа.

Задача 14. Пусть $K_1 \supset K_2 \supset K_3$ – последовательность расширений полей. Докажите, что естественное отображение

$$K_1 \otimes_{K_3} K_1 \longrightarrow K_1 \otimes_{K_2} K_1$$

– сюръективный гомоморфизм алгебр.

Задача 15 (!). Пусть $K_1 \supset K_2 \supset K_3$ – последовательность расширений полей, причем $[K_1 : K_3]$ – расширение Галуа. Докажите, что $[K_1 : K_2]$ – тоже расширение Галуа.

Поля разложения

Задача 16. Пусть $P \in k[t]$ – полином степени n над полем k. Положим $K_1 = k$, и рассмотрим последовательность расширений, $K_l \supset K_{l-1} \supset \cdots \supset K_1$, полученных индуктивно следующим образом. Пусть K_j построено. Разложим P на неприводимые сомножители $P = \prod P_i$ в K_j. Если все P_i линейны, мы закончили. В противном случае, пусть P_0 – неприводимый сомножитель P степени > 1. Возьмем $K_{j+1} = K_j[t]/P_0$. Докажите, что этот процесс закончится через конечное число шагов и даст некоторое поле $K \supset k$.

Определение 3. Это поле называется **полем разложения** (splitting field) многочлена P.

Задача 17. Пусть K – поле разложения для многочлена $P(t) \in k[t]$. Докажите, что K изоморфно подполю в алгебраическом замыкании $\bar{k}$, порожденному всеми корнями P.

Задача 18 (!). Пусть все корни $P(t)$ разные. Докажите, что поле разложения $P(t)$ есть минимальное расширение Галуа, содержащее $k[t]/(P)$.

Задача 19. Докажите, что поле разложения любого полинома единственно, с точностью до изоморфизма.

Указание. Воспользуйтесь предыдущей задачей.

Задача 20. Пусть $P(t)$ – многочлен степени n. Докажите, что степень его поля разложения не больше $n!$

Задача 21. Пусть $P \in k[t]$ – многочлен степени n, имеющий n попарно различных корней в алгебраическом замыкании k, и пусть $[K : k]$ – его поле разложения, а $K_l \supset K_{l-1} \supset \cdots \supset K_1$ соответствующая цепочка расширений. Докажите, что $K \otimes_{K_{i-1}} K_i$ изоморфно прямой сумме нескольких копий K.

Указание. Это сразу следует из Задачи 1.

Задача 22. Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в алгебраическом замыкании k (такой полином называется **не имеющим кратных корней**), а K – его поле разложения. Докажите, что $[K : k]$ – расширение Галуа.

Указание. Воспользуйтесь предыдущей задачей.

Задача 23. Пусть $P(t) \in k[t]$ – неприводимый многочлен над полем k характеристики 0. Докажите, что у P нет кратных корней.

Указание. Докажите, что у $P(t) = t^n + a_{n-1}t^{n-1} + \dots$ нет кратных корней тогда и только тогда, когда P не имеет общих множителей с многочленом

$$P'(t) = nt^{n-1} + (n-1)a_{n-1}t^{n-2} + \dots + 2a_2t + a_1.$$

Для этого докажите, что $(PQ)' = PQ' + Q'P$, и вычислите $P'(t)$ для $P = (t - b_1)\dots(t - b_n)$.

Замечание 1. Из предыдущей задачи следует, что над полем характеристики 0, поле разложения любого многочлена является расширением Галуа.

Задача 24. Пусть $a_1, ..., a_n$ – целые числа. Докажите, что $\mathbb{Q}[\sqrt{a_1}, ..., \sqrt{a_n}]$ – расширение Галуа (или прямая сумма расширений Галуа).

Задача 25 (**). Пусть $\operatorname{char} k = p$, а $f(x) = x^p - x + c$ – неприводимый многочлен над k. Докажите, что $k[t]/(f)$ есть расширение Галуа.

Задача 26 (*). Пусть $[K : \mathbb{Q}]$ – поле разложения многочлена $x^3 - 2$. Рассмотрим K как подполе в $\mathbb{C}$. Найдите комплексное число, которое порождает K над $\mathbb{Q}$.

Задача 27 (*). Пусть p простое, а $[K : \mathbb{Q}]$ – поле разложения многочлена $x^p - 2$. Докажите, что степень $[K : \mathbb{Q}]$ (то есть размерность K как $\mathbb{Q}$-линейного пространства) равна $p(p-1)$.

Листок 6: Группы Галуа

`Впервые выдано 22.02.2013. Версия 1.2, 12.02.2013.`

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Основная теорема теории Галуа

Определение 1. Пусть $[K : k]$ – расширение Галуа. **Группой Галуа** $[K : k]$ называется группа k-линейных автоморфизмов поля K. Мы обозначаем группу Галуа через $\mathrm{Gal}([K : k])$ или через $\mathrm{Aut}_k(K)$.

В дальнейшем мы будем рассматривать $K \otimes_k K$ как K-алгебру, с действием K^*, заданным формулой $a(v_1 \otimes v_2) = av_1 \otimes v_2$. Такое действие K^* называется **левым**. Оно отличается от "правого действия", заданного формулой $a(v_1 \otimes v_2) = v_1 \otimes av_2$.

Задача 1 (!). Пусть $[K : k]$ – расширение Галуа. Постройте биекцию между множеством K-линейных гомоморфизмов $K \otimes_k K \longrightarrow K$ и множеством неразложимых идемпотентов в $K \otimes_k K$.

Задача 2. Пусть $\mu : K \otimes_k K \longrightarrow K$ – ненулевой K-линейный гомоморфизм, а $k \otimes_k K \subset K \otimes_k K$ – k-подалгебра, естественно изоморфная K. Докажите, что $\mu \mid_{k\otimes_k K}$ задает k-линейный автоморфизм $K \longrightarrow K$.

Задача 3. Докажите, что всякий k-линейный автоморфизм K получается таким образом.

Указание. Пусть $\nu \in \mathrm{Gal}([K : k])$. Определим гомоморфизм $K \otimes_k K \longrightarrow K$ по формуле $v_1 \otimes v_2 \longrightarrow v_1\nu(v_2)$.

Задача 4 (!). Пусть $[K : k]$ – расширение Галуа. Постройте естественную биекцию между $\mathrm{Gal}([K : k])$ и множеством неразложимых идемпотентов в $K \otimes_k K$. Докажите, что порядок группы Галуа равен размерности K как векторного пространства над k.

Задача 5. Пусть $[K : k]$ – расширение Галуа, $\nu \in \mathrm{Gal}([K : k])$ – элемент группы Галуа, а e_ν – соответствующий идемпотент в $K \otimes_k K$. Обозначим через μ_l стандартное (левое) действие K^* на $K \otimes_k K$, а за μ_r правое действие. Докажите, что $\mu_l(a)e_\nu = \mu_r(\nu(a))e_\nu$.

Задача 6. Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Gal}([K : k])$. Докажите, что $a \otimes 1 = 1 \otimes a$ в $K \otimes_k K$.

Указание. Воспользуйтесь задачей 5.

Задача 7 (!). Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Gal}([K : k])$. Докажите, что $a \in k$.

Задача 8. Пусть $[K : k]$ – расширение Галуа, а K' – промежуточное поле, $K \supset K' \supset k$. Докажите, что $K' = K^{G'}$, где $G' \subset \mathrm{Gal}([K : k])$ – группа K'-линейных автоморфизмов K, а $K^{G'}$ обозначает множество G'-инвариантов.

Указание. Докажите, что $[K : K']$ – расширение Галуа, и воспользуйтесь предыдущей задачей.

Задача 9 (!). Докажите **основную теорему теории Галуа:** пусть $[K : k]$ – расширение Галуа. Тогда $G' \longrightarrow K^{G'}$ устанавливает биекцию между множеством подгрупп $G' \subset \mathrm{Gal}([K : k])$ и множеством промежуточных подполей $K \supset K' \supset k$.

Задача 10 (!). Пусть $[K : k]$ расширение степени n.

а. Докажите, что $\mathrm{Aut}_k K \leqslant n$.

б. Докажите, что K – расширение Галуа тогда и только тогда, когда $|\mathrm{Aut}_k K| = n$.

Группы Галуа и корни многочленов

Задача 11. Найдите группу Галуа $[\mathbb{Q}[\sqrt{a}] : \mathbb{Q}]$.

Задача 12. Пусть $[K : k]$ – расширение Галуа, а $V \subset K$ – объединение всех промежуточных полей $k \subset K' \subset K$, которые строго меньше K. Пусть k бесконечно. Докажите, что $V \neq K$.

Указание. V есть объединение конечного числа k-подпространств в K, которые имеют (над k) размерность меньше, чем размерность K как линейного пространства над k. Докажите, что в такой ситуации $V \neq K$.

Замечание 1. Из этого следует, что в любом расширении Галуа $[K : k]$ бесконечного поля k есть примитивный элемент.

Задача 13. Пусть $[K : k]$ – расширение Галуа. Докажите, что для любого $a \in K$ произведение $P(t) = \prod_{\nu_i \in \mathrm{Gal}([K:k])}(t - \nu_i(a))$ – многочлен с коэффициентами в k.

Задача 14 (!). Пусть $[K : k]$ – расширение Галуа. Докажите, что для любого $a \in K$ существует многочлен $P(t) \in k[t]$, $P(a) = 0$, все корни которого лежат в K.

Указание. Воспользуйтесь предыдущей задачей.

Задача 15 (!). Пусть $[K : k]$ – конечное расширение, $\mathrm{char}\, k = 0$. Докажите, что это расширение Галуа тогда и только тогда, когда для любого $a \in K$ существует многочлен $P(t) \in k[t]$, $P(a) = 0$, все корни которого лежат в K.

Задача 16 (*). Докажите утверждение предыдущей задачи для любого сепарабельного расширения $[K : k]$ (без условия $\mathrm{char}\, k = 0$).

Задача 17. Напомним, что корень n-й степени из единицы называется **примитивным**, если он порождает группу корней n-й степени из единицы. Пусть $\xi \in \mathbb{C}$ – примитивный корень степени n. Докажите, что группа $\mathrm{Gal}([\mathbb{Q}[\xi] : \mathbb{Q}])$ изоморфна группе $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ автоморфизмов группы $\mathbb{Z}/n\mathbb{Z}$. Найдите ее порядок.

Задача 18 (**). Зафиксируем целое число n. Пусть $P(t) = \prod(t - \xi_i)$, где ξ_i пробегает все примитивные корни степени n из единицы. Докажите, что $P(t)$ имеет рациональные коэффициенты и неприводим над $\mathbb{Q}$.

Замечание 2. Этот многочлен называется **круговым многочленом** (cyclotomic polynomial).

Задача 19. Пусть $a_1, \ldots, a_n \in \mathbb{Z}$ – взаимно простые числа, не являющиеся квадратами. Докажите, что $[\mathbb{Q}[\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}] : \mathbb{Q}]$ – расширение Галуа.

Задача 20. Найдите группу Галуа этого расширения.

Задача 21 (!). В условиях предыдущей задачи, докажите, что $\sqrt{a_1}$, $\sqrt{a_2}$, $\ldots$, $\sqrt{a_n}$ линейно независимы над $\mathbb{Q}$.

Задача 22. Докажите, что $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = \{1\}$.

Задача 23 (*). Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в $K = k[t]/P$. Докажите, что его группа Галуа абелева, или найдите контрпример.

Задача 24. Пусть $P(t) = x^3 - 2$.

а. Докажите, что поле разложения P над $\mathbb{Q}$ имеет степень 6.

б. (!) Найдите его группу Галуа.

Задача 25 (**). Докажите, что $\mathbb{Q}[\sqrt[4]{2}, \sqrt{-1}]$ – расширение Галуа $\mathbb{Q}$, а его группа Галуа – диэдральная порядка 8.

Задача 26 (**). Найдите пример расширения $[K : k]$ степени 4 такого, что не существует промежуточных полей $K \supsetneq K' \supsetneq k$, или докажите, что такого не бывет.

Задача 27 (*). Пусть $P(t) \in \mathbb{Q}[t]$ – неприводимый полином, у которого есть вещественные и комплексные корни. Докажите, что группа Галуа поля разложения $P(t)$ неабелева.

Листок 7: Конечные поля и абелевы расширения

`Впервые выдано 01.03.2013. Версия 1.2, 28.02.2013.`

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Конечные поля

Из курса алгебры нам известны следующие вещи про конечные поля. Порядок конечного поля равен p^n, где p – его характеристика. На любом поле k характеристики p задан **гомоморфизм Фробениуса**, $Fr : k \longrightarrow k$, $x \longrightarrow x^p$. В любое поле характеристики p естественно вложено конечное поле $\mathbb{F}_p$ из p элементов.

Мы обозначаем поле порядка p^n через $\mathbb{F}_{p^n}$.

Задача 1. Пусть $x \in \mathbb{F}_{p^n}$, $x \neq 0$. Докажите, что $x^{p^n-1} = 1$.

Указание. Воспользуйтесь теоремой Лагранжа (порядок элемента делит число элементов в группе).

Замечание 1. Из этого следует, что многочлен $P(t) = t^{p^n-1} - 1$ имеет ровно $p^n - 1$ корней в $\mathbb{F}_{p^n}$.

Задача 2 (!). Пусть $\mathbb{F}^*_{p^n}$ – мультипликативная группа ненулевых элементов конечного поля. Докажите, что она циклическая.

Указание. Воспользуйтесь теоремой Безу (число корней многочлена степени n над полем не больше n), чтобы найти элемент порядка $p^n - 1$ в $\mathbb{F}^*_{p^n}$.

Задача 3. Докажите, что $\prod_{\xi \in \mathbb{F}^*_{p^n}} (t - \xi) = t^{p^n-1} - 1$.

Задача 4 (!). Докажите, что $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ – расширение Галуа.

Задача 5. Докажите, что $Fr, Fr^2, \ldots, Fr^{n-1}$ – попарно различные автоморфизмы $\mathbb{F}_{p^n}$.

Указание. Воспользуйтесь теоремой Безу.

Задача 6 (!). Докажите, что $\mathrm{Gal}([\mathbb{F}_{p^n} : \mathbb{F}_p])$ – циклическая группа порядка n.

Задача 7 (!). Докажите, что поле разложения многочлена $t^{p^n-1} - 1$ над $\mathbb{F}_p$ имеет порядок p^n.

Задача 8 (!). Докажите, что поле порядка p^n единственно с точностью до изоморфизма.

Задача 9. Перечислите все подполя в $\mathbb{F}_{p^n}$.

Задача 10 (!). Пусть $[K : k]$ – расширение Галуа. Докажите, что в K есть примитивный элемент.

Указание. Отдельно разберите случай конечных и бесконечных полей.

Задача 11 (!). Докажите, что каждое конечное расширение $[K : k]$ в характеристике 0 порождено примитивным элементом.

Указание. Воспользуйтесь основной теоремой теории Галуа.

Задача 12 (*). Докажите то же самое для любого сепарабельного расширения. «Сепарабельное расширение» есть расширение $[K : k]$, для которого функция следа $\mathrm{Tr}_k K$ не равна нулю.

Задача 13 (*). Найдите конечное (несепарабельное) расширение, которое не может быть порождено примитивным элементом.

Задача 14 (**). Пусть $P(t) \in \mathbb{F}_p[t]$ – неприводимый многочлен степени n. Докажите, что его поле разложения изоморфно $\mathbb{F}_{p^n}$.

Задача 15. Разложите $x^8 - x$ в произведение неприводимых полиномов над $\mathbb{F}_2$.

Задача 16. Докажите, что каждый элемент конечного поля представляется в виде суммы квадратов.

Циклические расширения

Определение 1. Расширение Галуа $[K : k]$ называется **циклическим**, если его группа Галуа циклическая.

Задача 17. Пусть поле k содержит все корни из единицы порядка n, а $[K : k]$ – поле разложения многочлена $t^n - a$, не имеющего корней над k. Докажите, что это расширение циклическое.

Указание. Пусть α – какой-то корень многочлена $t^n - a$. Тогда все корни $t^n - a$ имеют вид $\alpha, \alpha\xi, \alpha\xi^2, \ldots, \alpha\xi^{p-1}$, где ξ – корень из единицы. Докажите, что автоморфизм, переводящий α в $\alpha\xi^i$, переводит $\alpha\xi^q$ в $\alpha\xi^{q+i}$.

Задача 18. Зафиксируем $n \in \mathbb{N}$ и $a \in \mathbb{Q}$. Пусть для любого $k > 1$, $|a|$ не равен k-й степени никакого рационального числа, а $[K : \mathbb{Q}]$ – поле разложения многочлена $t^n - a$.

а. Докажите, что K содержит все корни n-й степени из единицы.

б. (*) Постройте вложение из $\mathrm{Gal}([K : \mathbb{Q}])$ в полупрямое произведение $\mathbb{Z}/n\mathbb{Z} \rtimes \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

в. (**) Найдите пример n и a, для которого это не изоморфизм.

Задача 19. Пусть $[K : k]$ – циклическое расширение порядка n, ν – образующая группы $\mathrm{Gal}[K : k]$, $\xi \in k$ – примитивный корень из единицы степени n, а $a \in K$ – примитивный элемент. Напишем **резольвенту Лагранжа**

$$L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \cdots + \xi^{-n+1}\nu^{n-1}(a)$$

Докажите, что $\nu(L) = \xi L$. Докажите, что $L \neq 0$, для какого-то примитивного a, если поле k бесконечно.

Задача 20. В условиях предыдущей задачи, докажите, что $\prod_{i=0}^{n-1}(t - \nu^i(L)) = t^n - L^n$. Докажите, что L порождает K над k, и что $L^n \in k$.

Указание. Чтобы убедиться в том, что L порождает K над k, воспользуйтесь тем, что $\mathrm{Gal}[k[\sqrt[n]{L^n}], k] = \mathbb{Z}/n\mathbb{Z}$, а следовательно, размерность $k[L]$ над k такая же, как размерность K над k.

Задача 21 (!). Пусть $[K : k]$ – расширение Галуа порядка n, причем k содержит все корни n-й степени из единицы. Докажите, что $[K : k]$ циклическое тогда и только тогда, когда его можно получить добавлением корня n-й степени из $a \in k$.

Задача 22 (*). Пусть p – простое число вида $2^{2^n} + 1$ (простое число Ферма, Fermat's prime), а $P(t) := \sum_{i=0}^{p-1} t^i$. Докажите, что $P(t)$ неприводимо, а поле K_0 разложения $P(t)$ имеет вид $[K_0 : K_1 : K_2 : ...K_n = k]$, где все расширения $[K_i : K_{i+1}]$ квадратичны, то есть степени 2.

Задача 23 (**). Пусть p – простое число вида $2^k + 1$. Докажите, что k есть степень 2.

Задача 24 (*). Докажите, что группа Галуа поля разложения $P(t) = t^5 - 2$ имеет порядок 20.

Определение 2. Циклотомическое расширение $[K : \mathbb{Q}]$ есть поле разложения для одного из неприводимых сомножителей многочлена $P(t) := \sum_{i=0}^{n-1} t^i$.

Задача 25 (**). Докажите, что каждое число вида $\sqrt{d}$, $d \in \mathbb{N}$, лежит в каком-то циклотомическом расширении.

Листок 8: Теорема Абеля

`Впервые выдано 15.03.2013. Версия 1.3, 31.03.2013.`

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

Разрешимые группы

Задача 1. Пусть задан гомоморфизм $G_2 \xrightarrow{\varphi} \mathrm{Aut}(G_1)$. Определим на множестве пар $(g_1, g_2) \in G_1 \times G_2$ следующую операцию:

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 \varphi(g_2) h_1, g_2 h_2).$$

Докажите, что получится группа.

Определение 1. Эта группа называется **полупрямым**, или **скрученным** произведением G_1 и G_2 и обозначается $G_1 \rtimes G_2$.

Задача 2. В условиях предыдущей задачи докажите, что $(G_1, 1)$ задает нормальную подгруппу в G, а фактор по этой подгруппе изоморфен G_2.

Задача 3. Опишите группу S_3 как скрученное произведение двух абелевых групп.

Задача 4. Опишите диэдральную группу (группу симметрий правильного многоугольника на плоскости) как скрученное произведение двух абелевых групп.

Задача 5 (*). Группой Клейна называется группа кватернионов вида $\pm 1, \pm I, \pm J, \pm K$, с естественной операцией умножения. Можно ли получить группу Клейна как скрученное произведение двух абелевых групп?

Задача 6 (!). Пусть $1 \longrightarrow G_1 \longrightarrow G \xrightarrow{\varphi} G_2 \longrightarrow 1$ – расширение групп. Предположим, что задан гомоморфизм $G \xrightarrow{\psi} G_2$, такой, что $\psi \circ \varphi$ – тождественный автоморфизм G_2 (в такой ситуации говорится, что φ **допускает сечение**). Докажите, что G можно получить как скрученное произведение $G_1 \rtimes G_2$.

Определение 2. Группа G называется **разрешимой**, если существует последовательность $1 = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$ нормальных подгрупп, причем все G_i/G_{i-1} абелевы.

Задача 7. Докажите, что подгруппа разрешимой группы разрешима.

Задача 8. Докажите, что симметрическая группа S_3 разрешима.

Задача 9. Докажите, что симметрическая группа S_4 разрешима.

Задача 10. Докажите, что группа Клейна $\{\pm 1, \pm I, \pm J, \pm K\}$ разрешима.

Задача 11. Пусть G_0 – группа, G_1 – ее коммутант, $G_2 = [G_1, G_1]$ – коммутант коммутанта, и так далее, $G_i = [G_{i-1}, G_{i-1}]$. Докажите, что G_0 разрешима тогда и только тогда, когда на каком-то шаге мы получим $G_n = 1$.

Определение 3. Пусть G – группа, LG_1 – ее коммутант, $LG_2 = [G, LG_1]$, $LG_3 = [G, LG_2]$, и так далее. Эта последовательность подгрупп называется **нижним центральным рядом**. Группа, у которой нижний центральный ряд заканчивается группой $LG_n = \{1\}$, называется **нильпотентной**.

Задача 12. Докажите, что любая нильпотентная группа разрешима. Приведите пример разрешимой группы, которая не нильпотентна.

Определение 4. Обозначим за $Z(G)$ центр группы G. Если $H \subset G$ нормальная подгруппа, обозначим за $Z_H(G)$ все элементы G, которые переходят в $Z(G/H)$ при естественном гомоморфизме $G \longrightarrow G/H$. **Верхний центральный ряд** группы G есть $UG_0 = Z(G)$, $UG_1 = Z_{UG_0}(G)$, $UG_2 = Z_{UG_1}(G)$, и так далее.

Задача 13 (**). Докажите, что нижний центральный ряд нильпотентной группы имеет такую же длину, как и ее верхний центральный ряд.

Определение 5. Пусть $t, x \in G$ – элементы группы. Элемент вида xtx^{-1} обозначается t^x. Соответствующая операция называется **сопряжением**, **скруткой**, или **подкруткой на** x. Отображение $x \longrightarrow t^x$ есть (очевидно) автоморфизм группы. Такой автоморфизм называется **внутренним**.

Задача 14. Пусть $g_1, g_2 \in S_n$ элементы группы перестановок, разложение которых на циклы имеет одинаковую длину. Докажите, что g_1 можно перевести в g_2 внутренним автоморфизмом.

Задача 15 (!). Пусть $g_1, g_2 \in A_n$ элементы группы четных перестановок, разложение которых на непересекающиеся циклы имеет одинаковую длину. Всегда ли g_1 можно перевести в g_2 внутренним автоморфизмом?

Задача 16. Пусть t – элемент группы G. такой, что множество

$$\{x \in G \mid \exists g \in G \text{ такой, что } x = t^g t^{-1}\}$$

порождает G. Докажите, что G не разрешима.

Задача 17 (!). Докажите, что группа четных подстановок A_n, $n \geqslant 5$ неразрешима.

Указание. Воспользуйтесь предыдущей задачей, взяв $t = (123)$.

Задача 18. Докажите, что группа движений $\mathbb{R}^3$ неразрешима.

Указание. Постройте изоморфизм между A_5 и группой поворотов икосаэдра, и воспользуйтесь предыдущей задачей.

Задача 19. Пусть G – группа порядка p^n. Докажите, что центр G содержит больше одного элемента.

Указание. Рассмотрим действие G на себе автоморфизмами. Порядок G равен сумме мощностей классов вида x^G, где x^G есть совокупность всех элементов вида x^y, $y \in G$. Докажите сначала, что если x не лежит в центре, то порядок x^G делится на p. Выведите $|G| = 1 + \sum |y_i^G|$, причем если у G нет центра, все $|y_i^G|$ делятся на p.

Задача 20 (!). Пусть G – группа порядка p^n. Докажите, что G нильпотентна.

Замечание 1. Если вы хотите применить теорему Силова, пожалуйста, изучите и запомните ее доказательство.

Задача 21. Пусть G – группа порядка p^2, p простое. Докажите, что G абелева.

Задача 22. Приведите пример неабелевой группы порядка p^3, p – любое простое число.

Задача 23. Рассмотрим множество S верхнетреугольных матриц $n \times n$ с единицей на диагонали над полем k. Докажите, что такие матрицы образуют подгруппу в $GL(n, k)$. Докажите, что эта группа разрешима. Найдите ее порядок для $k = \mathbb{Z}/p\mathbb{Z}$.

Теорема Абеля

Теорема Абеля утверждает, что общий многочлен пятой степени неразрешим в радикалах; иначе говоря, решение общего уравнения пятой степени нельзя выразить посредством алгебраических операций (умножения, сложения, деления) и операции извлечения корня n-й степени. В этом разделе я приведу пример уравнения, неразрешимого в радикалах.

Задача 24. Пусть $[K : k]$ – расширение Галуа. Докажите, что подгруппа $G' \subset \mathrm{Gal}([K : k])$ нормальна тогда и только тогда, когда $[K^{G'} : k]$ – расширение Галуа.

Указание. Из основной теоремы теории Галуа сразу следует это.

Задача 25. Пусть $G' \subset \mathrm{Gal}([K:k])$ – нормальная подгруппа. Докажите, что группа $\mathrm{Gal}([K^{G'}:k])$ изоморфна фактору $\mathrm{Gal}([K:k])/G'$.

Задача 26 (!). Пусть k – поле характеристики 0, а $[K:k]$ – поле разложения многочлена $t^n - a$. Докажите, что группа Галуа $\mathrm{Gal}([K:k])$ разрешима.

Указание. Если k содержит корни n-й степени из 1, мы все доказали. Если нет, докажите, что K их содержит. Рассмотрите промежуточное расширение K', полученное добавлением этих корней к k, и докажите, что $[K:K']$ и $[K':k]$ – расширения Галуа с абелевыми группами Галуа.

Задача 27 (!). Пусть группа Галуа $[K:k]$ разрешима, а k содержит все корни из единицы. Докажите, что $[K:k]$ можно представить в виде последовательности расширений Галуа $k = K_0 \subset K_1 \subset ... \subset K_n = K$, таким образом, что для каждого i, $\mathrm{Gal}([K_i:K_{i-1}])$ - циклическая группа.

Задача 28 (!). (теорема Галуа) Докажите, что расширение Галуа $[K:k]$ порождается последовательным добавлением решений уравнения $t^n - a = 0$ тогда и только тогда, когда группа $\mathrm{Gal}[K:k]$ разрешима.

Замечание 2. Пусть $P(t) \in k[t]$ – многочлен. **Группой Галуа** P называется группа Галуа его поля разложения. Теорема Галуа утверждает, что уравнение $P(t) = 0$ разрешимо в радикалах тогда и только тогда, когда группа Галуа $P(t)$ разрешима.

Определение 6. Пусть группа G действует на множестве Σ. Действие называется **транзитивным**, если любой $x \in \Sigma$ можно перевести в любой $y \in \Sigma$ применением подходящего $g \in G$.

Задача 29. Пусть $G \subset S_n$, – подгруппа, содержащая транспозицию и действующая транзитивно на $\{1, 2, 3, \dots, n\}$.

а. (!) Докажите, что $G = S_n$ для $n = 5$.

б. (*) Докажите, что $G = S_n$ для любого простого n.

Задача 30. Пусть $P \in k[t]$ – неприводимый многочлен, $\xi_1, \dots, \xi_n$ – его корни, и пусть все эти корни различны. Докажите, что группа Галуа P действует на $\{\xi_1, \dots, \xi_n\}$ транзитивно.

Указание. Разобьем $\{\xi_1, \dots, \xi_n\}$ на смежные классы по действию $\mathrm{Gal}(P)$. Пусть S такой класс. Докажите, что полином $\prod_{\xi_i \in S}(t - \xi_i)$ имеет коэффициенты в k, и делит P.

Задача 31 (!). Пусть $P \in \mathbb{Q}[t]$ – неприводимый многочлен степени n, у которого ровно $n-2$ вещественных корня. Докажите, что его группа Галуа равна S_n.

Указание. Докажите, что $\mathrm{Gal}(P)$ транзитивно действует на корнях P, а комплексное сопряжение сохраняет поле разложения P и действует на множестве корней как транспозиция.

Задача 32. (теорема Эйзенштейна) Пусть $Q = t^n + t^{n-1}a_{n-1} + t^{n-2}a_{n-2} + \dots + a_0$ – такой многочлен с целыми коэффициентами, что все a_i делят заданное простое число p, а $a_0 \not\vdots p^2$. Докажите, что Q неприводим над $\mathbb{Q}$.

Задача 33. Докажите, что $Q(t) = x^5 - 10x + 5$ – неприводимый (над $\mathbb{Q}$) многочлен, у которого ровно 3 вещественных корня. Выведите из этого, что его группа Галуа это S_5.

Задача 34 (!). Докажите, что уравнение $x^5 - 10x + 5 = 0$ неразрешимо в радикалах.

Задача 35 (*). Постройте расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа $(\mathbb{Z}/5\mathbb{Z})^2$.

Задача 36 (**). Пусть n – число вершин правильного n-угольника в $\mathbb{R}^2$, который можно построить циркулем и линейкой. Докажите, что каждый простой делитель n имеет вид $2^k + 1$.

Задача 37 (*). Докажите, что для любого n существует расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа S_n (симметрической группой).

Задача 38 (*). Пусть G – конечная группа. Постройте конечное расширение $[K : k]$ с группой Галуа G.

Задача 39 (*). Пусть $[K : \mathbb{Q}]$ – расширение Галуа с группой Галуа $(\mathbb{Z}/2\mathbb{Z})^2$. Докажите, что $K = \mathbb{Q}[\alpha, \beta]$, где $\alpha = \sqrt{x}$, $\beta = \sqrt{y}$, а x, y – взаимно простые целые числа, или найдите контрпример.

Задача 40 (**). Пусть $[K : \mathbb{Q}]$ – конечное расширение, а Z – множество всех корней из единицы, лежащих в K. Докажите, что Z конечно.

Глава 3

Слайдовые лекции

Лекция 2: расширения полей

Расширения полей

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k. Отношение «быть расширением» обозначается $[K : k]$.

ОПРЕДЕЛЕНИЕ: Конечное расширение есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

Утверждение 1: Если $[K : K_1]$ **и** $[K_1 : k]$ **– конечные расширения, то** $[K : k]$ **тоже конечно.**

ДОКАЗАТЕЛЬСТВО: Возьмем базис $a_1, ..., a_n$ в K_1 над k, и $b_1, ..., b_m$ в K над K_1. Тогда $k\langle a_1, ..., a_n\rangle = K_1$, что дает

$$K = \bigoplus_{i=1}^{m} K_1 \cdot b_i = \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} k \cdot a_j b_i$$

то есть конечномерно. ■

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

Конечные расширения

ОПРЕДЕЛЕНИЕ: **Делители нуля** в кольце суть такие x, y, что $xy = 0$.

ОПРЕДЕЛЕНИЕ: Если $k \subset K$ – подполе K, а V, W – линейные пространства над K, мы можем рассмотреть V, W как линейные пространства V_k, W_k над k. В такой ситуации, линейное отображение $V_k \to W_k$ называется **k-линейным отображением пространства V в W.**

УТВЕРЖДЕНИЕ: Пусть K – конечномерное пространство над k, снабженное структурой кольца. **Если K не имеет делителей нуля, то это поле.**

Доказательство. Шаг 1: Для любого конечного расширения $[K : k]$, рассмотрим умножение на $x \in K$ как k-линейный эндоморфизм $A_x : K \to K$. Ядра у него нет, потому что K без делителей нуля. **Поскольку размерность ядра равна размерности коядра, A_x сюръективен.**

Шаг 2: Значит, найдется $y \in A$ такой, что $xy = 1$. ■

СЛЕДСТВИЕ: Пусть $x \in K$ – элемент расширения $[K : k]$, алгебраичный над k. **Тогда кольцо $k[x]$, порожденное x, это поле.**

Корни многочленов

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in K[t]$ – многочлен степени > 0. **Корень** P есть $\alpha \in K$ такое, что $P(\alpha) = 0$.

ТЕОРЕМА: Пусть $[K : k]$ расширение, а $x \in K$. Тогда следующие условия равносильны.
(i) **x – корень многочлена $P(x) = 0$ над k.**
(ii) **алгебраичен.**

ДОКАЗАТЕЛЬСТВО: , Если x алгебраичен, то $k[x]$ конечномерно над k, то есть x^d выражается как линейная комбинация x^{d-1}, x^{d-2}, ... x, 1 с коэффициентами из k. **Значит, x корень полинома.**

Наоборот, если x – корень многочлена, то x^d выражается как линейная комбинация x^{d-1}, x^{d-2}, ... x, 1, значит **$k[x]$ конечномерно над k;** в силу доказанного выше утверждения, **$k[x]$ конечномерное кольцо без делителей нуля, то есть поле.** ■

Алгебраические числа

ЗАМЕЧАНИЕ: Пусть $[K_1 = k[x] : k]$ конечное расширение, а $[K_2 = K_1[y] : K_1$ – тоже конечное расширение. Значит, **кольцо $k[x, y]$, порожденное x и y, конечномерно.**

СЛЕДСТВИЕ: Пусть $[K : k]$ – конечное расширение, $x_1, ..., x_n \in K$ – алгебраические элементы. Тогда **кольцо $R := k[x_1, x_2, ..., x_n]$, порожденное $x_1, ..., x_n$, является полем,** и расширение $[R : k]$ конечно. ■

СЛЕДСТВИЕ: Сумма, произведение, частное алгебраических над k элементов алгебраично над k. ■

ОПРЕДЕЛЕНИЕ: Поле $\bar{\mathbb{Q}}$ алгебраических чисел есть множество всех элементов $\mathbb{C}$, алгебраичных над $\mathbb{Q}$.

ОПРЕДЕЛЕНИЕ: Поле K **алгебраически замкнуто**, если любой многочлен $P(t) \in k[t]$ имеет корень в K.

Алгебраические числа (продолжение)

ТЕОРЕМА: Поле $\bar{\mathbb{Q}}$ алгебраически замкнуто.

Доказательство. Шаг 1: $\mathbb{C}$ алгебраически замкнуто, значит, **любой многочлен $P(t) \in \bar{\mathbb{Q}}[t]$ над $\bar{Q}$ имеет корень в $\mathbb{C}$.**

Шаг 2: Пусть α – корень многочлена $P(t)$ с коэффициентами в $\bar{\mathbb{Q}}$. Рассмотрим **поле K, порожденное этими коэффициентами.** Поскольку коэффициенты $P(t)$ алгебраичны, расширение $[K : k]$ конечно. Значит, α алгебраичен над K.

Шаг 3: Расширение $[K : \mathbb{Q}]$ конечно и $[K[\alpha] : K]$ тоже конечно. **В силу «Утверждения 1» со 2-й страницы, $[K[\alpha] : \mathbb{Q}]$ – конечное расширение.** ■

ЗАМЕЧАНИЕ: Коль скоро $\bar{\mathbb{Q}}$ счетно **(проверьте это!)** а $\mathbb{C}$ несчетно, в $\mathbb{C}$ существуют неалгебраические числа. Они называются **трансцендентными**.

Трансцендентными являются числа e, π, e^α для любого алгебраического $\alpha \neq 0$, e^π, $2^{\sqrt{2}}$, $\ln(\alpha)$ для любого алгебраического $\alpha \neq 1$, и число Фредгольма $\sum_{i=0}^{\infty} 2^{-2^i}$.

Алгоритм Евклида

ЗАМЕЧАНИЕ: В дальнейшем, все полиномы предполагаются по умолчанию **положительной степени.**

ТЕОРЕМА: (Алгоритм Евклида)
Пусть $P(t), Q(t) \in k[t]$ – полиномы над полем k. **Тогда существует полином $V(t)$, делящий $P(t)$ и $Q(t)$, который можно можно выразить как линейную комбинацию P и Q** над $k[t]$. ■

УПРАЖНЕНИЕ: Докажите эту теорему.

ОПРЕДЕЛЕНИЕ: Наибольший общий делитель P и Q есть полином наибольшей степени, который делит P и Q.

ЗАМЕЧАНИЕ: Наибольший общий делитель $P(t)$ и $Q(t)$ пропорционален $V(t)$, построенному выше. Действительно, **любой делитель $P(t)$ и $Q(t)$ обязан делить их линейную комбинацию $V(t) = A(t)P(t) + B(t)Q(t)$.**

СЛЕДСТВИЕ: Кольцо полиномов $k[t]$ **факториально** (обладает однозначным разложением на простые множители).

Неприводимые полиномы

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал, $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо $k[t]/(P)$ не имеет делителей нуля.**

Доказательство. Шаг 1: Произведение полиномов, взаимно простых с $P(t)$, снова взаимно просто с $P(t)$, в силу факториальности.

Шаг 2: Поэтому, если полином $P(t)$ неприводим, то любой полином $Q(t)$ **либо делится на $P(t)$, либо взаимно прост с ним.** Значит $k[t]/(P)$ не имеет делителей нуля.

Шаг 3: Наоборот, если $k[t]/(P)$ не имеет делителей нуля, то произведение полиномов, которые не делятся на $P(t)$, тоже не делится на $P(t)$. ■

Минимальный полином

УТВЕРЖДЕНИЕ: Пусть v – элемент конечномерной алгебры R над k. Рассмотрим подпространство R, порожденное $1, v, v^2, v^3, \dots$ (для всех степеней v). Пусть оно n-мерно. **Тогда $P(v) = 0$ для некоторого полинома $P = t^n + a_{n-1}t^{n-1} + \dots$ с коэффициентами из k. Более того, этот полином единственный**.

Доказательство. Шаг 1: Существование нетривиального полинома P степени $d \leqslant n$, удовлетворяющего $P(v) = 0$, **сразу следует из наличия линейных соотношений между $1, v, v^2, v^3, \dots$.** (если таких соотношений нет, R должно быть как минимум $n+1$-мерно).

Шаг 2: $\deg P \leqslant n$, потому что $v^d, v^{d+1}, \dots$ **выражаются через** 1, v, v^2, v^3, $\dots$, v^{d-1}**.** Мы получили, что $\deg P = n$

Шаг 3: Если таких полиномов 2, то **они равны, либо их разность $Q(t)$ – полином степени $< n$, удовлетворяющий $Q(v) = 0$.** Это доказывает единственность. ■

Минимальный полином (продолжение)

ОПРЕДЕЛЕНИЕ: Пусть v – элемент конечномерной алгебры R над k, а $P(t) == t^n + a_{n-1}t^{n-1} + \dots$ полином минимальной степени с коэффициентами из k, удовлетворяющий $P(v) = 0$. Этот полином называется **минимальный полином** $v \in R$.

ЗАМЕЧАНИЕ: Минимальный полином линейного оператора определяется точно также.

Утверждение 2: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра $R_v \subset R$, порожденная v, изоморфна $k[t]/(P)$.**

ДОКАЗАТЕЛЬСТВО: Определим гомоморфизм $k[t]/(P) \to R_v$, переводящий t в v. Он по построению сюръективен. Поскольку $\dim R_v = \deg P$, размерность этих колец одинаковая. ■

Примитивные расширения

Пусть $P(t) \in k[t]$ – неприводимый полином. **Поскольку $k[t]/(P)$ конечномерно над k и не имеет делителей нуля, это поле.** А поскольку $P(t) = 0$ имеет решение t в $k[t]/(P)$, $P(t)$ имеет корень в этом поле.

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно.

Доказательство. Шаг 1: Возьмем $\alpha \in K$, и пусть $K_1 = k[\alpha]$ – кольцо, порожденное α. Тогда $[K_1 : K_0]$ **примитивно, в силу Утверждения 2.**

Шаг 2: Если $K_1 \neq K$, повторим эту процедуру, получив примитивное расширение $[K_2 : K_1]$ и так далее. На каждом шаге размерность K_i над k увеличивается, но она не может быть больше $\dim_k K$, поэтому **этот процесс остановится, когда $K_n = K$.** ■

Идеалы в кольце

ЗАМЕЧАНИЕ: Все кольца в дальнейшем предполагаются коммутативные, с единицей, и $1 \neq 0$. Все гомоморфизмы сохраняют 1. Все идеалы в кольце R по умолчанию предполагаются **нетривиальными**, то есть не равными R. Кольцо, содержащее поле k, называется **коммутативной k-алгеброй**, или **кольцом над k**.

ОПРЕДЕЛЕНИЕ: **Максимальный идеал** в кольце есть идеал, который не содержится ни в каком большем.

УПРАЖНЕНИЕ: Докажите, что **идеал $I \subset R$ максимален тогда и только тогда, когда R/I – поле.**

ТЕОРЕМА: Каждый идеал I в кольце **содержится в максимальном идеале.** ■

УПРАЖНЕНИЕ: Докажите это.

Тензорные произведения колец

УТВЕРЖДЕНИЕ: Пусть A и B – кольца над полем k. В силу билинейности произведения, **существует мультипликативная операция** $(A \otimes_k B) \times (A \otimes_k B) \to A \otimes_k B$, **переводящая** $a \otimes b, a' \otimes b'$ **в** $aa' \otimes bb'$.

ОПРЕДЕЛЕНИЕ: Это кольцо называется **тензорным произведением колец** A **и** B, и обозначается $A \otimes_k B$.

ПРИМЕР: Пусть $k[t_1, t_2, ..., t_p]$, $k[u_1, u_2, ..., u_q]$ – кольца полиномов. **Тогда**

$$k[t_1, t_2, ..., t_p] \otimes_k k[u_1, u_2, ..., u_q] \cong k[t_1, t_2, ..., t_p, u_1, u_2, ..., u_q].$$

УТВЕРЖДЕНИЕ: Пусть $R = k[u_1, u_2, ..., u_d]$ кольцо полиномов от какого-то набора переменных, а $F_i \in k[u_i]$ – полином положительной степени. Рассмотрим идеал $I \subset R$, порожденный $F_i(u_i)$. **Тогда** $R/I = \bigotimes_{i=1}^{d} \Big(k[u_i]/(F_i) \Big)$.

Доказательство. Шаг 1: Положим $R' := k[u_1, u_2, ..., u_{d-1}]$, и пусть идеал I' порожден $F_1(u_1), ..., F_{d-1}(u_{d-1})$. **Воспользовавшись индукцией, получим** $R'/I' = \bigotimes_{i=1}^{d-1} \Big(k[u_i]/(F_i) \Big)$.

Тензорные произведения колец (продолжение)

ЛЕММА: Пусть $R = k[u_1, u_2, ..., u_d]$ кольцо полиномов от какого-то набора переменных, а $F_i \in k[u_i]$, $i = 1, ..., d$ – полиномы положительной степени. Рассмотрим идеал $I \subset R$, порожденный $F_i(u_i)$. **Тогда**

$$R/I = \bigotimes_{i=1}^{d} \Big(k[u_i]/(F_i) \Big).$$

Доказательство. Шаг 1: Положим $R' := k[u_1, u_2, ..., u_{d-1}]$, и пусть идеал I' порожден $F_1(u_1), ..., F_{d-1}(u_{d-1})$. **Воспользовавшись индукцией, получим** $R'/I' = \bigotimes_{i=1}^{d-1} \Big(k[u_i]/(F_i) \Big)$.

Шаг 2: $R = R' \otimes_k k[u_d]/(F_d(u_d))$, ибо **по модулю** I' **идеал** I **главный и порожден** $(F_d(u_d))$.

Шаг 3: Искомый изоморфизм получается из объединения утверждений шага 1 и шага 2. ■

СЛЕДСТВИЕ: Кольцо R/I**, определенное в этом утверждении, ненулевое.**

Тензорные произведения колец (окончание)

ЛЕММА: Пусть $R = k[u_1, u_2, ...,]$ кольцо полиномов от какого-то набора переменных, не обязательно конечного, а $F_i \in k[u_i]$, $i = 1, 2, ...$ – полиномы положительной степени. Рассмотрим идеал I, порожденный $F_i(u_i)$. **Тогда** I **– собственный идеал, то есть не содержит 1.**

Доказательство. Шаг 1: Если I содержит 1, то существует конечное линейное выражение вида $1 = \sum_{l=1}^{k} A_l F_{i_l}(u_{i_l})$, где $A_l \in k[u_1, u_2, ...,]$. Рассмотрим конечно-порожденное подкольцо $R' = k[u_1, u_2, ..., u_d]$, в которое входят все переменные, встречающиеся в полиномах A_l, и все u_{i_l}. **Из** $1 = \sum_{l=1}^{k} A_l F_{i_l}(u_{i_l})$ **следует, что** $1 \in I \cap R'$.

Шаг 2: В силу предыдущей леммы, $R'/I \cap R' \neq 0$, но это противоречит тому, что $1 \in I \cap R'$. ■

Конструкция алгебраического замыкания

Пусть $\mathfrak{S}$ – множество всех полиномов положительной степени $F_\alpha \in k[t]$ над полем k, $R_{\mathfrak{S}} = k[u_1, u_2, ...,]$ кольцо полиномов, проиндексированное $\alpha \in \mathfrak{S}$, а $F_\alpha(u_\alpha)$ – соответствующие полиномы. Пусть $I \subset R$ – идеал, порожденный всеми $F_\alpha(u_\alpha)$, а $\mathfrak{I}$ – максимальный идеал, содержащий I.

ТЕОРЕМА: Пусть $K := R_{\mathfrak{S}}/\mathfrak{I}$ – поле, полученное как фактор $R_{\mathfrak{S}}$ по $\mathfrak{I}$. **Тогда** $[K : k]$ **алгебраично, а любой полином** $P(t) \in k[t]$ **положительной степени имеет корень в** K.

Доказательство. Шаг 1: Я буду обозначать элементы K, полученные из $u_\alpha \in R$, той же буквой. Пусть $F_\alpha(t) \in k[t]$ – какой-то полином. Поскольку $F_\alpha(u_\alpha) = 0$ в R/I, $F_\alpha(t)$ имеет корень в K.

Шаг 2: Любой u_α является корнем полинома $F_\alpha(t)$, то есть алгебраичен над k. Но все элементы K выражаются через полиномы от u_α. ■

СЛЕДСТВИЕ: Для каждого поля k **существует алгебраическое расширение** $[k' : k]$ **такое, что все многочлены** $P(t) \in k[t]$ **положительной степени имеют корни в** K**.**

ВОПРОС: А почему из этого не следует сразу что $[k' : k]$ – алгебраическое замыкание k?

Конструкция алгебраического замыкания (продолжение)

Напомню, что **алгебраическое замыкание** поля k есть алгебраическое расширение $[\bar{k} : k]$, которое алгебраически замкнуто.

ТЕОРЕМА: Пусть k – поле. **Тогда существует алгебраическое замыкание** $[\bar{k} : k]$**.**

ДОКАЗАТЕЛЬСТВО: Мы можем построить расширение $[k' : k]$ такое, что все полиномы над k имеют корни в k'. Нам нужно, чтобы все полиномы над k' имели корни в k; это верно, но не вполне очевидно. Вместо этого мы рассмотрим цепочку расширений $k \subset k' \subset k'' \subset ...$, и **положим** $\bar{k} := k \cup k' \cup k'' \cup ...$**.**

Шаг 2: Возьмем полином $P(t) \in \bar{k}$. Каждый из его коэффициентов лежит в одном из полей $k^{(i)}$, их конечное число, что дает $P(t) \in k^{(n)}[t]$. Тогда $P(t)$ имеет корень в $k^{(n+1)}$.

Шаг 3: Осталось убедиться, что $\bar{k}$ алгебраично над k. Каждый элемент $x \in \bar{k}$ лежит в каком-то $k^{(n)}$, значит, **достаточно доказать, что** $[k^{(n)} : k]$ **алгебраично.**

Конструкция алгебраического замыкания (окончание)

Шаг 3: Осталось убедиться, что $\bar{k}$ алгебраично над k. Каждый элемент $x \in \bar{k}$ лежит в каком-то $k^{(n)}$, значит, **достаточно доказать, что** $[k^{(n)} : k]$ **алгебраично.**

Шаг 4: Имеем конечную цепочку расширений $[k^{(n)} : k^{(n-1)} : \ldots : k]$, и каждое последовательное расширение алгебраично. Поэтому **алгебраичность** $[k^{(n)} : k]$ **вытекает из следующей леммы.**

ЛЕММА: Пусть $K_2 \supset K_1 \supset K_0$ – расширения полей, причем $[K_i : K_{i-1}]$ алгебраично. **Тогда** $[K_2 : K_0]$ **алгебраично.**

ДОКАЗАТЕЛЬСТВО: Каждый $x \in K_2$ является корнем многочлена $P(t) \in K_1[t]$. Возьмем поле $[K_1' : K_0]$, содержащее все коэффициенты $P(t)$. Оно конечно над K_0, потому что порождено конечным числом алгебраических элементов. **Получаем цепочку конечных расширений** $[K_1'[x] : K_1' : K_0]$**,** то есть $[K_1'[x] : K_0]$ конечно (Утверждение 1). ■

Лекция 3: тензорные произведения полей

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k. Отношение «быть расширением» обозначается $[K : k]$.

ОПРЕДЕЛЕНИЕ: Конечное расширение есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

Алгебраические числа (повторение)

ТЕОРЕМА: Сумма, произведение, частное алгебраических над k **элементов алгебраично над** k**.** ■

ОПРЕДЕЛЕНИЕ: Поле $\bar{\mathbb{Q}}$ **алгебраических чисел** есть множество всех элементов $\mathbb{C}$, алгебраичных над $\mathbb{Q}$.

ОПРЕДЕЛЕНИЕ: Поле K **алгебраически замкнуто**, если любой многочлен $P(t) \in k[t]$ имеет корень в K.

ТЕОРЕМА: Поле $\bar{\mathbb{Q}}$ алгебраически замкнуто. ■

ЗАМЕЧАНИЕ: Коль скоро $\bar{\mathbb{Q}}$ счетно **(проверьте это!)** а $\mathbb{C}$ несчетно, в $\mathbb{C}$ существуют неалгебраические числа. Они называются **трансцендентными**.

Трансцендентными являются числа e, π, e^α для любого алгебраического $\alpha \neq 0$, e^π, $2^{\sqrt{2}}$, $\ln(\alpha)$ для любого алгебраического $\alpha \neq 1$, и число Фредгольма $\sum_{i=0}^{\infty} 2^{-2^i}$.

Минимальные полиномы (повторение)

УТВЕРЖДЕНИЕ: Пусть K – конечномерное пространство над k, снабженное структурой кольца. **Если K не имеет делителей нуля, то это поле.** ■

ОПРЕДЕЛЕНИЕ: Пусть v – элемент конечномерной алгебры R над k, а $P(t) = t^n + a_{n-1}t^{n-1} + \dots$ полином минимальной степени с коэффициентами из k, удовлетворяющий $P(v) = 0$. Этот полином называется **минимальный полином** $v \in R$.

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра $R_v \subset R$, порожденная v, изоморфна $k[t]/(P)$.** ■

Неприводимые полиномы (повторение)

ТЕОРЕМА: Кольцо полиномов $k[t]$ **факториально** (с однозначным разложением на множители). ■

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал, $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо $k[t]/(P)$ является полем.** ■

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно. ■

Тензорные произведения колец (повторение)

УТВЕРЖДЕНИЕ: Пусть A и B – кольца над полем k. В силу билинейности произведения, **существует мультипликативная операция** $(A \otimes_k B) \times (A \otimes_k B) \to A \otimes_k B$**, переводящая** $a \otimes b, a' \otimes b'$ **в** $aa' \otimes bb'$**.**

ОПРЕДЕЛЕНИЕ: Это кольцо называется **тензорным произведением колец A и B**, и обозначается $A \otimes_k B$.

ПРИМЕР: Пусть $k[t_1, t_2, ..., t_p]$, $k[u_1, u_2, ..., u_q]$ – кольца полиномов. **Тогда**

$$k[t_1, t_2, ..., t_p] \otimes_k k[u_1, u_2, ..., u_q] \cong k[t_1, t_2, ..., t_p, u_1, u_2, ..., u_q].$$

ПРИМЕР: $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \oplus \mathbb{C}$.

ПРИМЕР: Пусть $\mathbb{R}(t)$ – поле рациональных функций с коэффициентами из $\mathbb{R}$. Тогда $\mathbb{R}(t) \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}(t)$.

ЗАМЕЧАНИЕ: Как будет доказано на следующей лекции, **тензорное произведение полей есть «почти всегда» прямая сумма полей.**

Бесконечное тензорное произведение

Я сейчас буду определять **"бесконечное тензорное произведение"** для бесконечного набора колец $R_\alpha \supset k$, проиндексированных набором индексов $\alpha \in \mathfrak{S}$.

Пусть $S \subset \mathfrak{S}$ – конечное подмножество, а $R_S := \bigotimes_{\alpha \in S} R_\alpha$ – произведение (над k) всех колец, входящих в S.

ЛЕММА: Пусть $S \subset S'$ – подмножество, а $\zeta = x_1 \otimes_k x_2 \otimes ... \in R_S$ какой-то моном, а $\zeta' := x_1 \otimes_k x_2 \otimes ... \otimes 1 \otimes 1 \in R_{S'}$ соответствующий моном в $R_{S'}$, дополненный единицами. Рассмотрим отображение $R_S \xrightarrow{\varphi(S,S')} R_{S'}$, переводящее ζ в ζ'. **Тогда φ индуцирует вложение колец.** ■

ОПРЕДЕЛЕНИЕ: Бесконечное тензорное произведение $\bigoplus_{\alpha\in\mathfrak{S}} R_\alpha$ есть объединение R_S для всех конечных подмножеств $S \subset \mathfrak{S}$ по вложениям $\varphi(S, S')$.

Конструкция алгебраического замыкания

Пусть $\mathfrak{S}$ – множество всех конечных расширений $[K_\alpha : k]$, проиндексированных $\alpha \in \mathfrak{S}$, а $R_{\mathfrak{S}} := \bigotimes_{\alpha\in\mathfrak{S}} K_\alpha$ – произведение (над k) всех полей, входящих в S.

ТЕОРЕМА: Пусть$\mathfrak{I}$ – максимальный идеал, а $K := R_{\mathfrak{S}}/\mathfrak{I}$ – поле, полученное как фактор $R_{\mathfrak{S}}$ по $\mathfrak{I}$. **Тогда $[K : k]$ алгебраично, а любой полином $P(t) \in k[t]$ положительной степени имеет корень в K.**

Доказательство. Шаг 1: Каждый элемент $R_{\mathfrak{S}}$ происходит из конечного произведения, то есть представлен в виде $\zeta \in R_S \hookrightarrow R_{\mathfrak{S}}$, где R_S – алгебра, которая конечномерна над k. Поскольку ζ лежит в конечномерной алгебре, у ζ есть минимальный полином $P(t)$, с коэффициентами из k. **Значит, все элементы K алгебраичны.**

Шаг 2: Для любого неприводимого полинома $P(t)$, соответствующее поле $K_P := k[t]/(P)$ содержит корень $P(t)$. Поскольку $R_{\mathfrak{S}}$ содержит K_P, существует $\zeta \in R_{\mathfrak{S}}$ такой, что $P(\zeta) = 0$

Шаг 3: Образ ζ в K является корнем $P(t)$. ■

Конструкция алгебраического замыкания (продолжение)

СЛЕДСТВИЕ: Для каждого поля k **существует алгебраическое расширение $[k' : k]$ такое, что все многочлены $P(t) \in k[t]$ положительной степени имеют корни в K.**

Напомню, что **алгебраическое замыкание** поля k есть алгебраическое расширение $[\bar{k} : k]$, которое алгебраически замкнуто.

ТЕОРЕМА: Пусть k – поле. **Тогда существует алгебраическое замыкание $[\bar{k} : k]$.**

Доказательство. Шаг 1: Мы можем построить расширение $[k' : k]$ такое, что все полиномы над k имеют корни в k'. Нам нужно, чтобы все полиномы

над k' имели корни в k; это верно, но не вполне очевидно. Вместо этого мы рассмотрим цепочку расширений $k \subset k' \subset k'' \subset ...$, и **положим** $\bar{k} := k \cup k' \cup k'' \cup ...$.

Шаг 2: Возьмем полином $P(t) \in \bar{k}$. Каждый из его коэффициентов лежит в одном из полей $k^{(i)}$, их конечное число, что дает $P(t) \in k^{(n)}[t]$. Тогда $P(t)$ имеет корень в $k^{(n+1)}$.

Конструкция алгебраического замыкания (окончание)

Шаг 2: Возьмем полином $P(t) \in \bar{k}$. Каждый из его коэффициентов лежит в одном из полей $k^{(i)}$, их конечное число, что дает $P(t) \in k^{(n)}[t]$. Тогда $P(t)$ имеет корень в $k^{(n+1)}$.

Шаг 3: Осталось убедиться, что $\bar{k}$ алгебраично над k. Каждый элемент $x \in \bar{k}$ лежит в каком-то $k^{(n)}$, значит, **достаточно доказать, что** $[k^{(n)} : k]$ **алгебраично.**

Шаг 4: Имеем конечную цепочку расширений $[k^{(n)} : k^{(n-1)} : ... : k]$, и каждое последовательное расширение алгебраично. Поэтому **алгебраичность** $[k^{(n)} : k]$ **вытекает из следующей леммы.**

ЛЕММА: Пусть $K_2 \supset K_1 \supset K_0$ – расширения полей, причем $[K_i : K_{i-1}]$ алгебраично. **Тогда** $[K_2 : K_0]$ **алгебраично.**

ДОКАЗАТЕЛЬСТВО: Каждый $x \in K_2$ является корнем многочлена $P(t) \in K_1[t]$. Возьмем поле $[K_1' : K_0]$, содержащее все коэффициенты $P(t)$. Оно конечно над K_0, потому что порождено конечным числом алгебраических элементов. **Получаем цепочку конечных расширений** $[K_1'[x] : K_1' : K_0]$**,** то есть $[K_1'[x] : K_0]$ конечно. ■

Идеалы в кольцах (повторение)

ЗАМЕЧАНИЕ: Все кольца в дальнейшем предполагаются коммутативные, с единицей, и $1 \neq 0$. Все гомоморфизмы сохраняют 1. Все идеалы в кольце R по умолчанию предполагаются **нетривиальными**, то есть не равными R. Кольцо, содержащее поле k, называется **коммутативной k-алгеброй**, или **кольцом над k**.

ОПРЕДЕЛЕНИЕ: **Максимальный идеал** в кольце есть идеал, который не содержится ни в каком большем.

ТЕОРЕМА: Каждый идеал I в кольце **содержится в максимальном идеале.** ■

ОПРЕДЕЛЕНИЕ: Элемент $r \in R$ в кольце R называется **нильпотентным**, если $r^k = 0$, для какого-то $k \in \mathbb{N}$.

ЗАМЕЧАНИЕ: Множество всех нильпотентов в кольце образует идеал **(проверьте это).** Этот идеал называется **нильрадикалом** кольца.

УПРАЖНЕНИЕ: Докажите, что **фактор кольца по нильрадикалу не имеет ненулевых нильпотентов.**

Артиновы кольца

ОПРЕДЕЛЕНИЕ: Кольцо над полем (ассоциативное, коммутативное, но не обязательно с единицей) будем называть **коммутативной алгеброй**.

ОПРЕДЕЛЕНИЕ: Пусть дана коммутативная алгебра R с единицей над полем k. Говорят, что R **артиново кольцо над полем** k, если R конечномерна как векторное пространство.

ОПРЕДЕЛЕНИЕ: Артиново кольцо R называется **полупростым**, если в нем нет ненулевых нильпотентов.

ОПРЕДЕЛЕНИЕ: Пусть $R_1, \dots, R_n$ – алгебры над полем. Возьмем прямую сумму $\oplus R_i$, с естественным (почленным) умножением и сложением. Получившаяся алгебра называется **прямой суммой** R_i, обозначается $\oplus R_i$.

Сейчас я буду доказывать такую теорему.

ТЕОРЕМА: Пусть A – полупростое артиново кольцо. **Тогда A есть прямая сумма полей.**

Конечномерные алгебры над полем и идемпотенты

ОПРЕДЕЛЕНИЕ: Пусть $v \in R$ – такой элемент алгебры R, что $v^2 = v$. Тогда v называется **идемпотентом**.

ЗАМЕЧАНИЕ: Произведение идемпотентов - идемпотент. Если e – идемпотент, то $1 - e$ – тоже идемпотент.

СЛЕДСТВИЕ: Для идемпотента e, произведение $e(1 - e)$ равно нулю. Поэтому **каждый идемпотент $e \in A$ задает разложение A в прямую сумму:** $A = eA + (1 - e)A$ **(проверьте это)**

Конечномерные алгебры над полем и идемпотенты (продолжение)

УТВЕРЖДЕНИЕ: Пусть A – коммутативная алгебра, в которой нет нильпотентов и конечномерная над полем. **Тогда A содержит идемпотент.**

Доказательство. Шаг 1: Поскольку A конечномерно, любая убывающая цепочка идеалов обрывается. Значит, **есть идеал $I \subset A$, который не содержит ненулевых идеалов.** Дальше мы будем рассматривать этот идеал как подалгебру в A (без единицы).

Шаг 2: Поскольку в A нет нильпотентов, $z^2 \neq 0$. А поскольку I минимальный, для любого ненулевого $z \in I$, имеем $zI = I$.

Шаг 3: Му доказали, что умножение на любой $z \in I$ не имеет ядра в I. Следовательно, **все элементы I обратимы,** как эндоморфизмы I.

Шаг 4: Поскольку I конечномерно, элементы $z, z^2, z^3, ... \in \operatorname{End} I$ линейно зависимы, что дает выражение вида $P(z) = 0$. Если у этого полинома нет свободного члена, разделим на z, пользуясь тем, что у z нет ядра. Получим соотношение $\mathrm{Id}_I = az + bz^2 + cz^3 + ...$ в кольце эндоморфизмов I.

Шаг 5: Элемент $U := az + bz^2 + cz^3 + ...$ удовлетворяет $Ux = x$ для любого $x \in I$, **поэтому является идемпотентом.** ■

Структурная теорема для полупростых артиновых алгебр

ЗАМЕЧАНИЕ: Аргумент шага 5 доказывает следующее утверждение. Пусть I – коммутативная алгебра без делителей нуля, конечномерная над полем. **Тогда I содержит единицу, т.е. является полем.**

СЛЕДСТВИЕ: Пусть A есть кольцо, конечномерное над полем, и без нильпотентов. **Тогда A есть прямая сумма полей.**

Доказательство. Шаг 1: Пусть $I \subset A$ – нетривиальный идеал. В силу доказанного утверждения, I содержит ненулевой идемпотент a.

Тогда a и $a-1$ – идемпотенты, произведение которых равно нулю, а сумма равна 1. **Это дает $A = aA \oplus (1-a)A$, где aA и $(1-a)A$ – подалгебры с единицей.** Воспользовавшись индукцией по $\dim A$, можно считать, что aA и $(1-a)A$ – прямые суммы полей. ■

В следующей лекции я буду применять эти знания к тензорным произведениям полей.

Структурная теорема для полупростых артиновых алгебр: единственность разложения

ЛЕММА: Пусть A есть прямая сумма полей, $A = \bigoplus_i k_i$. **Тогда разложение $A = \bigoplus_i k_i$ определено однозначно** с точностью до перестановки слагаемых.

ДОКАЗАТЕЛЬСТВО: Если $A = \bigoplus_i k_i = \bigoplus_i k'_i$, каждое из полей k_i разложится в прямую сумму, $k_i = \bigoplus_j k_i \cap k'_j$. Поскольку поле не имеет нетривиальных разложений такого вида, **получаем, что $k_i = k'_j$ для какого-то индекса j.** ■

Лекция 4: тензорные произведения полей и композиты

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k. Отношение «быть расширением» обозначается $[K : k]$.

ОПРЕДЕЛЕНИЕ: **Конечное расширение** есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

УТВЕРЖДЕНИЕ: Пусть $[K_2 : K_1 : K]$ – расширения полей. **Если** $[K_1 : K]$ **и** $[K_2 : K_1]$ **алгебраичны, то** $[K_2 : K]$ **алгебраично. Если они конечны, то** $[K_2 : K]$ **конечно.**

Алгебраические числа (повторение)

ТЕОРЕМА: Сумма, произведение, частное алгебраических над k **элементов алгебраично над** k**.** ■

ОПРЕДЕЛЕНИЕ: **Поле** $\bar{\mathbb{Q}}$ **алгебраических чисел** есть множество всех элементов $\mathbb{C}$, алгебраичных над $\mathbb{Q}$.

ОПРЕДЕЛЕНИЕ: Поле K **алгебраически замкнуто**, если любой многочлен $P(t) \in k[t]$ имеет корень в K.

ТЕОРЕМА: Поле $\bar{\mathbb{Q}}$ **алгебраически замкнуто.** ■

ЗАМЕЧАНИЕ: Коль скоро $\bar{\mathbb{Q}}$ счетно **(проверьте это!)** а $\mathbb{C}$ несчетно, в $\mathbb{C}$ существуют неалгебраические числа. Они называются **трансцендентными**.

Примитивные расширения (повторение)

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра** $R_v \subset R$**, порожденная** v**, изоморфна** $k[t]/(P)$**.** ■

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо** $k[t]/(P)$ **является полем.** ■

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно. ■

Нильрадикал и идемпотенты (повторение)

ОПРЕДЕЛЕНИЕ: Элемент $r \in R$ в кольце R называется **нильпотентным**, если $r^k = 0$, для какого-то $k \in \mathbb{N}$.

ЗАМЕЧАНИЕ: Множество всех нильпотентов в кольце образует идеал. Этот идеал называется **нильрадикалом** кольца.

УТВЕРЖДЕНИЕ: Фактор кольца по нильрадикалу не имеет ненулевых нильпотентов.

ОПРЕДЕЛЕНИЕ: Пусть $v \in R$ – такой элемент алгебры R, что $v^2 = v$. Тогда v называется **идемпотентом**.

ЗАМЕЧАНИЕ: Произведение идемпотентов - идемпотент. Если e – идемпотент, то $1 - e$ – тоже идемпотент.

СЛЕДСТВИЕ: Для идемпотента e, произведение $e(1 - e)$ равно нулю. Поэтому **каждый идемпотент $e \in A$ задает разложение A в прямую сумму:** $A = eA + (1 - e)A$ **(проверьте это)**

Артиновы кольца (продолжение)

ОПРЕДЕЛЕНИЕ: Кольцо над полем (ассоциативное, коммутативное, но не обязательно с единицей) будем называть **коммутативной алгеброй**.

ОПРЕДЕЛЕНИЕ: Пусть дана коммутативная алгебра R с единицей над полем k. Говорят, что R **артиново кольцо над полем k**, если R конечномерна как векторное пространство.

ОПРЕДЕЛЕНИЕ: Артиново кольцо R называется **полупростым**, если в нем нет ненулевых нильпотентов.

ОПРЕДЕЛЕНИЕ: Пусть $R_1, \dots, R_n$ – алгебры над полем. Возьмем прямую сумму $\oplus R_i$, с естественным (почленным) умножением и сложением. Получившаяся алгебра называется **прямой суммой** R_i, обозначается $\oplus R_i$.

ЛЕММА: Пусть K – конечномерное пространство над k, снабженное структурой кольца. **Если K не имеет делителей нуля, то это поле.** ■

ТЕОРЕМА: Пусть A – полупростое артиново кольцо. **Тогда A есть прямая сумма полей.**

Тензорные произведения колец (повторение)

УТВЕРЖДЕНИЕ: Пусть A и B – кольца над полем k. В силу билинейности произведения, **существует мультипликативная операция** $(A \otimes_k B) \times (A \otimes_k B) \to A \otimes_k B$**, переводящая** $a \otimes b, a' \otimes b'$ **в** $aa' \otimes bb'$**.**

ОПРЕДЕЛЕНИЕ: Это кольцо называется **тензорным произведением колец** A **и** B, и обозначается $A \otimes_k B$.

ПРИМЕР: Пусть $k[t_1, t_2, ..., t_p]$, $k[u_1, u_2, ..., u_q]$ – кольца полиномов. **Тогда**

$$k[t_1, t_2, ..., t_p] \otimes_k k[u_1, u_2, ..., u_q] \cong k[t_1, t_2, ..., t_p, u_1, u_2, ..., u_q].$$

ПРИМЕР: $H^*(X \times Y, k) = H^*(X, k) \otimes_k H^*(Y, k)$ **(формула Кюннета)**

ПРИМЕР: $k[x, y]/(x^n, y^n) = k[x]/(x^n) \otimes_k k[y]/(y^n)$.

Инвариантные билинейные формы

ОПРЕДЕЛЕНИЕ: Пусть R – алгебра над полем k, а g – симметричная билинейная форма на R. Форма g называется **инвариантной**, если $g(x, yz) = g(xy, z)$ для любых x, y, z.

ЗАМЕЧАНИЕ: Если R содержит единицу, то для любой инвариантной формы g, имеем $g(x, y) = h(xy, 1)$, то есть g определяется линейным функционалом.

ПРИМЕР: На кольце $\mathbb{R}[x,y]/(x^{n+1},y^{n+1}) = H^*(\mathbb{C}P^n \times \mathbb{C}P^n)$ есть функционал $\varepsilon(\sum a_{ij}x^iy^j) := a_{nn}$. **Соответствующая билинейная инвариантная форма $g(x,y) := \varepsilon(xy)$ невырождена (проверьте).** Это форма Пуанкаре на $H^*(\mathbb{C}P^n \times \mathbb{C}P^n)$

ОПРЕДЕЛЕНИЕ: **Фробениусова алгебра** есть конечномерная алгебра над полем, снабженная невырожденной билинейной инвариантной формой.

УПРАЖНЕНИЕ: Приведите пример артинова кольца, не допускающего такой формы.

Форма следа

УТВЕРЖДЕНИЕ: Пусть $[K:k]$ – расширение полей, а ε – ненулевой k-линейный функционал на K. **Тогда форма $g(x,y) := \varepsilon(xy)$ невырождена.**

ДОКАЗАТЕЛЬСТВО: Пусть $\varepsilon(a) \neq 0$. Тогда $g(x, x^{-1}a) \neq 0$. ■

ОПРЕДЕЛЕНИЕ: **След** линейного оператора есть сумма всех диагональных членов в каком-то матричном представлении.

ОПРЕДЕЛЕНИЕ: Пусть R – артиново кольцо над полем k. Рассмотрим билинейную форму $a,b \to \operatorname{tr}(ab)$, где $\operatorname{tr}(ab)$ – след эндоморфизма $L_{ab} \in \operatorname{End}_k R$, $x \stackrel{L_{ab}}{\to} abx$. Эта форма называется **формой следа**, и обозначается $\operatorname{tr}_k(ab)$.

ЗАМЕЧАНИЕ: Пусть $[K:k]$ – конечное расширение полей. В силу доказанного выше утверждения, **форма следа $\operatorname{tr}_k(ab)$ невырождена, если tr_k не тождественно равен нулю.**

Форма следа и сепарабельность

ОПРЕДЕЛЕНИЕ: Расширение $[K:k]$ называется **сепарабельным**, если форма следа $\operatorname{tr}_k(ab)$ ненулевая.

ЗАМЕЧАНИЕ: В характеристике 0, любое расширение сепарабельно, ибо $\operatorname{tr}_k(1) = \dim_k K$.

ТЕОРЕМА: Пусть R – артинова алгебра над k с невырожденной формой следа. **Тогда R полупросто.**

ДОКАЗАТЕЛЬСТВО: Поскольку $\mathrm{tr}_k(ab) = 0$ для любого нильпотента a (след нильпотентного оператора равен нулю), **в R нет нильпотентов.** ■

Тензорное произведение полей

ЛЕММА: Пусть R, R' – артиновы кольца над k. Обозначим естественные билинейные формы $a, b \to \mathrm{tr}(ab)$ на них через g, g'. Рассмотрим тензорное произведение $R \otimes_k R'$ с естественной структурой артинова кольца. **Тогда форма следа на $R \otimes_k R'$ равна $g \otimes g'$.**

ДОКАЗАТЕЛЬСТВО: Если V, W – векторные пространства над k, μ, ρ – эндоморфизмы V, W, то след $\mu \otimes \rho$ на $V \otimes W$ равен $\mathrm{tr}(\mu)\,\mathrm{tr}(\rho)$, что ясно из блочного разложение матрицы $\mu \otimes \rho$. **Это дает след для разложимых векторов вида $r \otimes r' \in R \otimes_k R'$, на все остальные оно продолжается по линейности.** ■

СЛЕДСТВИЕ: Если $[K_1 : k]$, $[K_2 : k]$ – сепарабельные расширения, то $K_1 \otimes_k K_2$ **полупросто,** то есть изоморфно прямой сумме полей.

ДОКАЗАТЕЛЬСТВО: Потому что форма следа невырождена. ■

ЗАМЕЧАНИЕ: В частности, **в характеристике 0 произведение конечных расширений поля k есть всегда прямая сумма полей.**

Тензорные произведения полей: примеры

УТВЕРЖДЕНИЕ: Пусть $P(t)$ – полином над полем k, $[K : k]$ – расширение, а $K_1 = k[t]/P(t)$. **Тогда $K_1 \otimes K \cong K[t]/P(t)$.** ■

УТВЕРЖДЕНИЕ: Пусть $P(t)$ – полином над полем k, $[K : k]$ – расширение, а $K_1 = k[t]/P(t)$. Предположим, что $P(t)$ разлагается на линейные множители над K. **Тогда $K_1 \otimes K \cong K[t]/P(t) = \bigoplus$**

ДОКАЗАТЕЛЬСТВО: Пусть $P = (t - a_1)(t - a_2)...(t - a_n)$. **По китайской теореме об остатках, отображение $K[t]/(P) \to \bigoplus_i K[t]/(t - a_i) = K$ сюръективно,** и по соображениям размерности, это изоморфизм. ■

УПРАЖНЕНИЕ: Пусть $P(t) \in \mathbb{Q}[t]$ – многочлен, у которого есть ровно r вещественных корней и ровно $2s$ комплексных, но не вещественных, причем все корни разные. **Докажите, что $(\mathbb{Q}[t]/P) \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_s \mathbb{C} \oplus \bigoplus_r \mathbb{R}$.**

ЗАДАЧА: Докажите, что $[K : k]$ **несепарабельно тогда и только тогда, когда** $K \otimes_k K$ **содержит нильпотенты.**

Композит расширений

ОПРЕДЕЛЕНИЕ: Пусть K_1, K_2 – расширения k, причем $[K_1 : k]$ конечное. Обозначим за $\mathfrak{n}$ нильрадикал произведения $K_1 \otimes_k K_2$, и пусть $R = K_1 \otimes_k K_2/\mathfrak{n}$. Поскольку R конечномерно над K_2 и без нильпотентов, это прямая сумма полей. Каждое из этих полей называется **композитом** K_1 и K_2.

УТВЕРЖДЕНИЕ: K_1 **и** K_2 **канонически вложено в любой их композит.**

ДОКАЗАТЕЛЬСТВО: $K_1 \otimes_k 1 \subset K_1 \otimes_k K_2$ есть подполе, содержащее 1, и проекция $K_1 \otimes_k 1$ переводит 1 в 1, значит, не равна нулю. С другой стороны, ненулевой гомоморфизм из поля куда угодно есть вложение. ■

УТВЕРЖДЕНИЕ: Для каждого поля, допускающего k-линейный гомоморфизм $K_1 \stackrel{\mu_1}{\to} L$, $K_2 \stackrel{\mu_2}{\to} L$, **естественное отображение** $K_1 \otimes_k K_2 \stackrel{\mu_1 \otimes \mu_2}{\to} L$ **инъективно на каком-то из композитов** $K \subset K_1 \otimes_k K_2$**.**

ДОКАЗАТЕЛЬСТВО: Гомоморфизм из поля куда угодно инъективен либо равен нулю. С другой стороны, ограничение $\mu_1 \otimes \mu_2$ на $K_1 \otimes_k 1 \subset K_1 \otimes_k K_2$ равно μ_1, значит ненулевое. ■

Универсальное свойство композита

ТЕОРЕМА: (Универсальное свойство композита) Пусть K_1, K_2 – расширения k, причем одно из них конечное, а L – расширение k, снабженное k-линейными гомоморфизмами $K_1 \stackrel{\varphi}{\to} L$, $K_2 \stackrel{\psi}{\to} L$. Предположим, что L порождено образами φ и ψ. **Тогда** L **это композит** K_1 **и** K_2**.**

ДОКАЗАТЕЛЬСТВО: В силу предыдущего утверждения, существует инъективное отображение $K \to L$, где K есть какой-то композит K_1 и K_2. **Поскольку** L **порожден образами** K_1 **и** K_2**, это отображение сюръективно.** ■

УТВЕРЖДЕНИЕ: Пусть $K = k[t]/P(t)$ – расширение, полученное добавлением корня неприводимого многочлена $P(t)$, а $P(t) = P_1(t)P_2(t)...P_n(t)$ –

неприводимое разложение $P(t)$ над полем $K' \supset k$. **Тогда композиты K и K' суть все поля вида $K'[t]/P_i(t)$.**

ДОКАЗАТЕЛЬСТВО: Следует из того, что
$K \otimes_k K' = k[t]/(P) \otimes_k K = K[t]/(P) = \bigoplus_{i=1}^n K[t]/(P_i)$. ■

УПРАЖНЕНИЕ: Докажите последнее из этих равенств, используя китайскую теорему об остатках.

Расширения Галуа

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – конечное расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

ПРИМЕР: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в $K = k[t]/P$. **Тогда $[K : k]$ – расширение Галуа.** В самом деле, $K \otimes_k K = K[t]/(P) = \bigoplus_i K[t]/(t - a_i)$

ПРИМЕР: Пусть p – простое. Тогда**для любого корня из единицы ζ степени p, $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ – расширение Галуа. (докажите это!)** А если p непростое?

ПРИМЕР: Пусть $[k : \mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). Тогда $[k : \mathbb{Q}]$ – расширение Галуа **(докажите это!)**

Лекция 5: расширения Галуа

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k.

ОПРЕДЕЛЕНИЕ: Конечное расширение есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над k**, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

ТЕОРЕМА: Сумма, произведение, частное алгебраических над k элементов алгебраично над k. ■

Алгебраические числа (повторение)

ОПРЕДЕЛЕНИЕ: Поле $\bar{\mathbb{Q}}$ алгебраических чисел есть множество всех элементов $\mathbb{C}$, алгебраичных над $\mathbb{Q}$.

ОПРЕДЕЛЕНИЕ: Алгебраическое замыкание k есть поле $[\bar{k} : k]$, алгебраически замкнутое и алгебраичное над k.

ПРИМЕР: Поле $\bar{\mathbb{Q}}$ является алгебраическим замыканием $\mathbb{Q}$

ТЕОРЕМА: Для любого поля k, **алгебраическое замыкание $[\bar{k} : k]$ существует, и оно единственно с точностью до изоморфизма.**

Примитивные расширения (повторение)

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра $R_v \subset R$, порожденная v, изоморфна $k[t]/(P)$.** ■

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо $k[t]/(P)$ является полем.** ■

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно. ■

Артиновы кольца (повторение)

ОПРЕДЕЛЕНИЕ: **Артиново кольцо над полем** k, если кольцо, которое конечномерна как векторное пространство над k.

ОПРЕДЕЛЕНИЕ: Артиново кольцо R называется **полупростым**, если в нем нет ненулевых нильпотентов.

ТЕОРЕМА: Пусть A – полупростое артиново кольцо. **Тогда** A **есть прямая сумма полей.**

УТВЕРЖДЕНИЕ: Пусть A и B – кольца над полем k. В силу билинейности произведения, **существует мультипликативная операция** $(A \otimes_k B) \times (A \otimes_k B) \to A \otimes_k B$**, переводящая** $a \otimes b, a' \otimes b'$ **в** $aa' \otimes bb'$**.**

ОПРЕДЕЛЕНИЕ: Это кольцо называется **тензорным произведением колец** A **и** B, и обозначается $A \otimes_k B$.

ТЕОРЕМА: В характеристике 0, тензорное произведение полупростых алгебр всегда полупросто.

ПРИМЕР 1: Пусть $P(t)$ – полином над полем k, $[K : k]$ – расширение, а $K_1 = k[t]/P(t)$. Предположим, что $P(t)$ разлагается на линейные множители над K. **Тогда** $K_1 \otimes K \cong K[t]/P(t) = \bigoplus$

Расширения Галуа

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – конечное расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

ПРИМЕР: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в $K = k[t]/P$. **Тогда** $[K : k]$ **– расширение Галуа.** В самом деле, $K \otimes_k K = K[t]/(P) = \bigoplus_i K[t]/(t - a_i)$

ПРИМЕР: Пусть p – простое. Тогда **для любого корня из единицы** ζ **степени** p**,** $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ **– расширение Галуа. (докажите это!)** А если p не простое?

УПРАЖНЕНИЕ: Пусть $[k : \mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). **Докажите, что** $[k : \mathbb{Q}]$ **– расширение Галуа.**

Кратные корни и производная

Полезное утверждение, которое будет использоваться дальше:

УТВЕРЖДЕНИЕ: Пусть $P(t)$ – неприводимый полином над полем k характеристики 0. **Тогда $P(t)$ имеет n попарно различных корней** в алгебраическом замыкании $\bar{k}$.

ДОКАЗАТЕЛЬСТВО: В поле $\bar{k}$ полином $P(t)$ разлагается на множители: $P(t) = \prod_i (t - \alpha_i)$. **Если среди корней есть кратные, $P(t)$ имеет общий делитель $Q(t)$ с $P'(t)$,** в $\bar{k}[t]$. Поскольку наличие общих делителей проверяется применением алгоритма Евклида, многочлен $Q(t)$ тоже определен над k. ■

Расширения Галуа и корни

ЛЕММА: Пусть $[K : K_1 : k]$ – цепочка конечных расширений, причем $K \otimes_k K_1 = K^{\oplus n}$ и $K \otimes_{K_1} K = K^{\oplus m}$. **Тогда $K \otimes_k K = K^{\oplus nm}$.**

ДОКАЗАТЕЛЬСТВО: Поскольку $K_1 \otimes_{K_1} K = K$, имеем $K \otimes_k K = K \otimes_k K_1 \otimes_{K_1} K = K^{\oplus_n} \otimes_{K_1} K = K^{\oplus nm}$. ■

ТЕОРЕМА: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней $\alpha_1, ..., \alpha_n$ в конечном расширении $[K : k]$. Предположим, что K порождено $\{\alpha_i\}$. **Тогда это расширение Галуа.**

Доказательство. Шаг 1: Рассмотрим цепочку расширений $K_0 = k \subset K_1 \subset K_2 \subset ...K_n = K$, полученных из k последовательным добавлением α_i. Каждое из этих расширений имеет вид $K_i = K_{i-1}[t]/P_i$, где $P_i(t)$ – какой-то из делителей $P(t)$ в $K_{i-1}[t]$. **В силу примера 1, каждое из K_i удовлетворяет $K_i \otimes_{K_{i-1}} K = K^{\oplus n_i}$.**

Шаг 2: Применив индукцию, будем считать, что $K_{i-1} \otimes_k K = K^{\oplus m_i}$. Поскольку $K_i \otimes_{K_{i-1}} K = K^{\oplus n_i}$ в силу леммы выше, получаем

$$K_i \otimes_k K = (K_i \otimes_{K_{i-1}} K_{i-1}) \otimes_k K = K_i \otimes_{K_{i-1}} (K_{i-1} \otimes_k K) = K_i \otimes_{K_{i-1}} K^{\oplus m_i} = K^{\oplus m_i n_i}.$$

Цепочки расширений Галуа

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа, а $[K : K_1 : k]$ – цепочка расширений. **Тогда $[K : K_1]$ – тоже расширение Галуа.**

ДОКАЗАТЕЛЬСТВО: Из определения тензорного произведения, получаем K-линейную сюръекцию $K \otimes_k K \to K \otimes_{K_1} K$. Поскольку $K \otimes_k K = K^{\oplus n}$, а $K \otimes_{K_1} K$ – его фактор по идеалу, $K \otimes_{K_1} K = K^{\oplus n'}$. ■

Поля разложения

ОПРЕДЕЛЕНИЕ: Пусть $P \in k[t]$ – полином степени n без кратных корней над полем k характеристики 0. Положим $K_1 = k$, и рассмотрим последовательность расширений, $K_l \supset K_{l-1} \supset \cdots \supset K_1$, полученных индуктивно следующим образом. Пусть K_j построено. Разложим P на неприводимые сомножители $P = \prod P_i$ в K_j. Если все P_i линейны, мы закончили. В противном случае, пусть P_0 – неприводимый сомножитель P степени > 1. Возьмем $K_{j+1} = K_j[t]/P_0$. **Этот процесс заканчивается через конечное число шагов, (докажите это!)** и в результате мы получаем поле $[K : k]$. Это поле называется **полем разложения** (splitting field) многочлена P.

ЗАМЕЧАНИЕ: Несколько слайдов назад было доказано, что **поле разложения является полем Галуа.**

УТВЕРЖДЕНИЕ: Пусть $[\bar{k} : k]$ – алгебраическое замыкание k, а $K \subset \bar{k}$ – поле, полученное из k добавлением всех корней $\alpha_i \in \bar{k}$. **Тогда K изоморфно полю разложения $P(t)$.** ■

СЛЕДСТВИЕ: Поле разложения многочлена определено однозначно. ■

Группа Галуа

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – расширение Галуа. **Группой Галуа** $[K : k]$ называется группа $\mathrm{Aut}_k(K)$ k-линейных автоморфизмов поля K.

ЗАМЕЧАНИЕ: K^* действует на $K \otimes_k K$ умножениями справа (**правое действие**) и слева (**левое**). Зафиксируем раз и навсегда левое действие, и будем рассматривать $K \otimes_k K$ как векторное пространство над K с левым действием k.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

(в) Гомоморфизмы $K \otimes_k K \to K$, линейные относительно левого действия K.

Доказательство см. следующий слайд.

Группа Галуа (продолжение)

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

(в) Гомоморфизмы $K \otimes_k K \to K$, линейные относительно левого действия K.

ДОКАЗАТЕЛЬСТВО: Биекция между (б) и (в) строится так: **каждому простому идеалу соответствует проекция $K \otimes_k K = K^{\oplus^n} \to K$,** а из K-линейности получаем, что такое отображение однозначно задается своим идеалом.

Ограничивая K-линейный гомоморфизм $\mu : K \otimes_k K \to K$ на $K = k \otimes K \subset K \otimes K$, получаем k-линейный гомоморфизм $\mu\,|_{k\otimes_k K}$: $K \to K$. Это задает отображение из (в) в (а).

Для каждого элемента группы Галуа $\nu \in \mathrm{Aut}_k(K)$, определим гомоморфизм $K \otimes_k K \to K$ по формуле $v_1 \otimes v_2 \to v_1\nu(v_2)$. Это задает обратную биекцию из (а) в (в). ■

Инварианты группы Галуа

Левое и правое действие K на $K \otimes_k K$ отличается на действие группы Галуа.

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $K \otimes_k K = \bigoplus_{\nu\in\mathrm{Aut}_k(K)} K_\nu$ – разложение $K \otimes_k K$ в компоненты, пронумерованные элементами группы

Галуа. Обозначим через μ_l стандартное (левое) действие K^* на $K \otimes_k K$, а за μ_r правое действие. **Тогда $\mu_l(a)e_\nu = \mu_r(\nu(a))e_\nu$.**

ДОКАЗАТЕЛЬСТВО: Каждое $a \in K$ действует на соответствующей компоненте $K_\nu \subset K \otimes_k K$ по формуле $\mu_l(a)(v_1 \otimes v_2) = av_1\nu(v_2)$ и $\mu_r(a)(v_1 \otimes v_2) = v_1\nu(av_2) = \nu(a)v_1\nu(v_2)$. ■

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Aut}_k(K)$. **Тогда $a \in k \subset K$.**

ДОКАЗАТЕЛЬСТВО: Поскольку $\mu_l(a) = \mu_r(a)$ на $K \otimes_k K$, имеем $a \otimes_k 1 = 1 \otimes_k a$, что влечет $a \in K$. ■

Основная теорема теории Галуа

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а K' – промежуточное поле, $K \supset K' \supset k$. **Тогда $K' = K^{G'}$, где $G' \subset \mathrm{Aut}_{K'}(K)$ – группа K'-линейных автоморфизмов K, а $K^{G'}$ обозначает множество G'-инвариантов.**

ДОКАЗАТЕЛЬСТВО: $[K : K']$ – расширение Галуа, а $G' = \mathrm{Aut}_{K'}(K)$ значит, $K^{G'} = K'$. ■

ТЕОРЕМА: Основная теорема теории Галуа:
Пусть $[K : k]$ – расширение Галуа. Тогда **$G' \to K^{G'}$ устанавливает биекцию между множеством подгрупп $G' \subset \mathrm{Aut}_k(K)$ и множеством промежуточных подполей $K \supset K' \supset k$.**

ДОКАЗАТЕЛЬСТВО: Из предыдущей леммы, получаем, что[1] $\mathrm{Aut}_{K'}(K) = G'$ однозначно задает $K' = K^{G'}$. ■

Лекция 6: группа Галуа

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k.

[1] При перекомпиляции $G' = \mathrm{Aut}_{K'}(K)$ заменено на $\mathrm{Aut}_{K'}(K) = G'$ по типографским причинам. — Y. Y.

ОПРЕДЕЛЕНИЕ: Конечное расширение есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

ТЕОРЕМА: Сумма, произведение, частное алгебраических над k элементов алгебраично над k. ■

Примитивные расширения (повторение)

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра $R_v \subset R$, порожденная v, изоморфна $k[t]/(P)$.** ■

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо $k[t]/(P)$ является полем.** ■

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно. ■

Расширения Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – конечное расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

ПРИМЕР: Пусть p – простое. Тогда **для любого корня из единицы ζ степени p, $[\mathbb{Q}[\zeta]:\mathbb{Q}]$ – расширение Галуа.** А если p не простое?

ПРИМЕР: Пусть $[k:\mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). **Тогда $[k:\mathbb{Q}]$ – расширение Галуа.**

ТЕОРЕМА: Пусть $K \supset K' \supset k$ – цепочка конечных расширений. Предположим, что $[K:k]$ – расширение Галуа. **Тогда $[K:K']$ тоже расширение Галуа.** ■

ТЕОРЕМА: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней $\alpha_1, ..., \alpha_n$ в конечном расширении $[K:k]$. Предположим, что K порождено $\{\alpha_i\}$. **Тогда это расширение Галуа.**

ОПРЕДЕЛЕНИЕ: Пусть $[\bar{k}:k]$ – алгебраическое замыкание k, а $K \subset \bar{k}$ – поле, полученное из k добавлением всех корней $\alpha_i \in \bar{k}$. Тогда K называется **полем разложения $P(t)$.**

Группа Галуа и идемпотенты

ОПРЕДЕЛЕНИЕ: Пусть $[K:k]$ – расширение Галуа. **Группой Галуа** $[K:k]$ называется группа $\mathrm{Aut}_k(K)$ k-линейных автоморфизмов поля K.

УТВЕРЖДЕНИЕ: Пусть $[K:k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

(в) Гомоморфизмы $K \otimes_k K \to K$,

тождественные на $K = K \otimes_k k \subset K \otimes_k K$.

Доказательство. Шаг 1: Биекция между (б) и (в) строится так: **каждому простому идеалу соответствует проекция** $K \otimes_k K = K^{\oplus^n} \to K$.

Группа Галуа и идемпотенты (продолжение)

УТВЕРЖДЕНИЕ: Пусть $[K:k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

(в) Гомоморфизмы $K \otimes_k K \to K$,
тождественные на $K = K \otimes_k k \subset K \otimes_k K$.

Шаг 2: Простые идеалы в $K \otimes_k K = \bigoplus K_e$ соответствуют неразложимым идемпотентам, то есть компонентам разложения. Каждый неразложимый идемпотент e задает проекцию $K \otimes_k K \xrightarrow{\pi} K_e$, переводящую 1 в 1. Рассмотрим гомоморфизмы $L_e, R_e : K \to K_e$, полученные композицией $L_e : K = K \otimes_k k \subset K \otimes_k K \xrightarrow{\pi} K_e$ и $R_e : K = k \otimes_k K \subset K \otimes_k K \xrightarrow{\pi} K_e$ Поскольку это поля одинаковой размерности над k, L_e и R_e – изоморфизмы. **Поставим в соответствие идемпотенту e автоморфизм $L_e R_e^{-1} \in \mathrm{Aut}_k(K)$.** Это задает (б) $\Rightarrow$ (а).

Шаг 3: Каждому автоморфизму $\zeta \in \mathrm{Aut}_k(K)$ поставим в соответствие гомоморфизм $v_\zeta : K \otimes_k K \to K$, переводящий $a \otimes b$ в $a\zeta^{-1}(b)$. Ядро этого гомоморфизма - простой идеал. **Мы получили соответствие (а) $\Rightarrow$ (в) $=$ (б).**

Осталось доказать, что это биекция.

Группа Галуа и идемпотенты (окончание)

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$
(б) Простые идеалы в $K \otimes_k K$.
(в) Гомоморфизмы $K \otimes_k K \to K$,
тождественные на $K = K \otimes_k k \subset K \otimes_k K$.

Доказательство биективности построенных отображений из (а) в (б) и наоборот.

Шаг 4: Удобнее доказывать биективность соответствия между (а) и (в). Для каждого $\zeta \in \mathrm{Aut}_k(K)$, соответствующий гомоморфизм v_ζ удовлетворяет $v_\zeta(a \otimes 1) = a$, $v_\zeta(1 \otimes a) = \zeta^{-1}(a)$. **Для соответствующего идемпотента получаем $a \otimes 1 \cdot e = 1 \otimes \zeta(a) \cdot e$, то есть $L_e(a) = R_e(\zeta(a))$.** Значит, соответствие (а) $\Rightarrow$ (в) $\Rightarrow$ (а) биективно на $\mathrm{Aut}_k(K)$.

Шаг 5. В обратную сторону: Достаточно убедиться, что идемпотент однозначно восстанавливается по автоморфизму ζ. Если есть два идемпотента

e, e' с одинаковым ζ, соответствующие гомоморфизмы в K удовлетворяют $v_e(a \otimes 1) = v_{e'}(a \otimes 1) = a$ и $v_e(1 \otimes a) = v_{e'}(1 \otimes a) = \zeta^{-1}(a)$, **то есть равны на** $K \otimes_k K$. ■

Порядок группы Галуа

СЛЕДСТВИЕ: Порядок группы Галуа равен степени $[K : k]$.

ДОКАЗАТЕЛЬСТВО: $\mathrm{Aut}_k(K)$ находится в биективном соответствии с компонентами $K \otimes_k K$, что дает $|\mathrm{Aut}_k(K)| = \dim_K(K \otimes_k K) = \deg[K : k]$. ■

СЛЕДСТВИЕ: Пусть $[K : k]$ – расширение Галуа. Рассмотрим действие группы Галуа $\mathrm{Aut}_k(K)$ на $K \otimes_k K$ автоморфизмами, $\zeta(a \otimes b) = a \otimes \zeta(b)$. **Это действие транзитивно на компонентах разложения в прямую сумму** $K \otimes_k K = \bigoplus K$.

ДОКАЗАТЕЛЬСТВО: Достаточно убедиться, что $\mathrm{Aut}_k(K)$ действует транзитивно на простых идеалах в $K \otimes_k K$. Но **каждый такой простой идеал является ядром гомоморфизма** $K \otimes_k K \to K$ **вида** $a \otimes b \to a\zeta(b)$. ■

Инварианты группы Галуа

Левое и правое действие K **на** $K \otimes_k K$ **отличается на действие группы Галуа.**

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $K \otimes_k K = \bigoplus_{\zeta \in \mathrm{Aut}_k(K)} K_\zeta$ – разложение $K \otimes_k K$ в компоненты, пронумерованные элементами группы Галуа. Обозначим через μ_l левое действие K^* на $K \otimes_k K$, а за μ_r правое действие. **Тогда** $\mu_l(a)e_\zeta = \mu_r(\zeta(a))e_\zeta$.

ДОКАЗАТЕЛЬСТВО: K_ζ отождествляется с образом гомоморфизма $K \otimes_k K \to K$, переводящего $v_1 \otimes v_2$ в $v_1\zeta(v_2)$. Каждое $a \in K$ действует на соответствующей компоненте $K_\zeta \subset K \otimes_k K$ по формуле $\mu_l(a)(v_1 \otimes v_2) = av_1\zeta(v_2)$ и $\mu_r(a)(v_1 \otimes v_2) = v_1\zeta(av_2) = \zeta(a)v_1\zeta(v_2)$. ■

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Aut}_k(K)$. **Тогда** $a \in k \subset K$.

ДОКАЗАТЕЛЬСТВО: Поскольку $\mu_l(a) = \mu_r(a)$ на $K \otimes_k K$, имеем $a \otimes_k 1 = 1 \otimes_k a$, что влечет $a \in K$. ■

Основная теорема теории Галуа

ТЕОРЕМА: (Основная теорема теории Галуа)
Пусть $[K : k]$ – расширение Галуа. Тогда соответствия **стрелки** $G' \to K^{G'}$ **и** $K' \to \mathrm{Aut}_{K'} K \subset G$ **устанавливают биекцию между множеством подгрупп** $G' \subset \mathrm{Aut}_k(K)$ **и множеством промежуточных подполей** $K \supset K' \supset k$**.**

Доказательство. Шаг 1: Для любого промежуточного подполя $K \supset K' \supset k$, расширение $[K : K']$ есть расширение Галуа. В силу предыдущего утверждения, $K^{G'} = K'$, где $G' = \mathrm{Aut}_{K'} K \subset G$. Получаем, что **соответствие (подполя)** $\Rightarrow$ **(подгруппы)** $\Rightarrow$ **(подполя) биективно.**

Шаг 2: Осталось убедиться, что две подгруппы $G_1, G_2 \subset G$ не могут удовлетворять $K' := K^{G_1} = K^{G_2}$. Без ограничения общности можно считать, что $G_1 = \mathrm{Aut}_{K'} K$, а $G_2 \subsetneq G_1$. **Поэтому все следует из такой леммы.**

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $G' \subsetneq \mathrm{Aut}_k K$ есть нетривиальная подгруппа группы Галуа. **Тогда** $K^{G'} \neq k$**.**

Доказательство см. следующий слайд.

Основная теорема теории Галуа (окончание)

ЗАМЕЧАНИЕ: Пусть группа G действует на векторном пространстве V. **Тогда** $(V \otimes_k V)^{G \times G} = V^G \otimes_k V^G$**. Докажите это!**

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $G' \subsetneq \mathrm{Aut}_k K$ есть нетривиальная подгруппа группы Галуа. **Тогда** $K^{G'} \neq k$**.**

Доказательство. Шаг 1: Поскольку $K^{G'} = k$, имеем $(K \otimes_k K)^{G' \times G'} = k$.

Шаг 2: Пусть $\zeta \in G$, а $a \otimes b \xrightarrow{v_\zeta} a\zeta(b)$ – соответствующий гомоморфизм $K \otimes_k K \to K$. Для любого $\chi \times \chi' \in G \times G$, $\chi \times \chi'(v_\zeta)$ переводит $a \otimes b$ в $\chi(a)\chi'\zeta(b)$, то есть имеет то же самое ядро, что у $v_{\chi'\zeta\chi^{-1}}$. Значит, $G \times G$ **переводит идемпотент** e_ζ **в** $e_{\chi'\zeta\chi^{-1}}$**.**

Шаг 3: Получаем, что действие G' **на** $K \otimes_k K$ **сохраняет нетривиальный идемпотент** $\sum_{g \in G'} e_g$**,** что противоречит утверждению шага 1. ■

Лекция 7: группы Галуа конечных полей и другие применения основной теоремы

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: **Расширение поля** k есть поле K, содержащее k.

ОПРЕДЕЛЕНИЕ: **Конечное расширение** есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

ТЕОРЕМА: **Сумма, произведение, частное алгебраических над k элементов алгебраично над k.** ■

Примитивные расширения (повторение)

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра $R_v \subset R$, порожденная v, изоморфна $k[t]/(P)$.** ■

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо $k[t]/(P)$ является полем.** ■

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно. ■

Расширения Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – конечное расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

ТЕОРЕМА: Пусть $K \supset K' \supset k$ – цепочка конечных расширений. Предположим, что $[K : k]$ – расширение Галуа. **Тогда $[K : K']$ тоже расширение Галуа.**

ТЕОРЕМА: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней $\alpha_1, ..., \alpha_n$ в конечном расширении $[K : k]$. Предположим, что K порождено $\{\alpha_i\}$. **Тогда это расширение Галуа.**

ОПРЕДЕЛЕНИЕ: Пусть $[\bar{k} : k]$ – алгебраическое замыкание k, а $K \subset \bar{k}$ – поле, полученное из k добавлением всех корней $\alpha_i \in \bar{k}$. Тогда K называется **полем разложения $P(t)$.**

ЗАМЕЧАНИЕ: В характеристике 0, поля разложения суть поля Галуа (в характеристике p, не обязательно)

УТВЕРЖДЕНИЕ: Если $[K : k]$ – конечное расширение, $\operatorname{char} k = 0$, то **существует расширение $[K_1 : K]$ такое, что $[K_1 : k]$ – расширение Галуа.**

Группа Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – расширение Галуа. **Группой Галуа** $[K : k]$ называется группа $\operatorname{Aut}_k(K)$ k-линейных автоморфизмов поля K.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\operatorname{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

СЛЕДСТВИЕ: Порядок группы Галуа равен степени $[K : k]$.

СЛЕДСТВИЕ: Пусть $[K : k]$ – расширение Галуа. Рассмотрим действие группы Галуа $\operatorname{Aut}_k(K)$ на $K \otimes_k K$ автоморфизмами, $\zeta(a \otimes b) = a \otimes \zeta(b)$. **Это действие транзитивно на компонентах разложения в прямую сумму $K \otimes_k K = \bigoplus K$.**

Основная теорема теории Галуа (повторение)

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $G' \subsetneq \mathrm{Aut}_k K$ есть нетривиальная подгруппа группы Галуа. **Тогда** $K^{G'} \neq k$.

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Aut}_k(K)$. **Тогда** $a \in k \subset K$.

ЗАМЕЧАНИЕ: (осталось с прошлой лекции)
Пусть группа G действует на векторном пространстве V.
Тогда $(V \otimes_k V)^{G\times G} = V^G \otimes_k V^G$. **Докажите это!**

ТЕОРЕМА: (Основная теорема теории Галуа)
Пусть $[K : k]$ – расширение Галуа. Тогда соответствия **стрелки** $G' \to K^{G'}$ **и** $K' \to \mathrm{Aut}_{K'} K \subset G$ **устанавливают биекцию между множеством подгрупп** $G' \subset \mathrm{Aut}_k(K)$ **и множеством промежуточных подполей** $K \supset K' \supset k$.

Теорема о примитивном элементе

ТЕОРЕМА: (теорема Артина о примитивном элементе)
Пусть $[K : k]$ – конечное расширение, причем K бесконечно, и выполнено одно из условий: (1) $\mathrm{char}\, k = 0$ (2) $[K : k]$ – расширение Галуа. **Тогда** $[K : k]$ **примитивно**, то есть порождено одним элементом $x \in K$.

Доказательство. Шаг 1: Заменим $[K : k]$ на расширение Галуа $[K_1 : k]$, содержащее K. В силу основной теоремы теории Галуа, **существует не более чем конечное число промежуточных полей** $K \supsetneq K' \supsetneq k$. Обозначим за Z объединение всех этих подполей.

Шаг 2: Элемент x примитивен тогда и только тогда, когда $x \notin Z$. Значит, **теорема о примитивном элементе вытекает из следующей леммы.**

ЛЕММА: Пусть V – векторное пространство над бесконечным полем, а Z – конечное объединение подпространств $W_i \subsetneq V$, $i = 1, ..., N$. **Тогда** $V \backslash Z$ **непусто.**

УПРАЖНЕНИЕ: Докажите это самостоятельно!

Теорема о примитивном элементе (окончание)

ЛЕММА: Пусть V – векторное пространство над бесконечным полем k, а Z – конечное объединение подпространств $W_i \subsetneq V$, $i = 1, ..., N$. **Тогда $V \backslash Z$ непусто.**

Доказательство. Шаг 1: Без ограничения общности, можно считать все W_i гиперплоскостями, которые пересекаются трансверсально. Применив индукцию по размерности V, **найдем точку $w \in W_0$, которая не принадлежит объединению $\bigcup_{j \neq 0} W_j$.**

Шаг 2: Рассмотрим гиперплоскость V', трансверсальную W_0, и проходящую через W. Эта гиперплоскость **не содержится ни в одном из W_i, $i > 0$, так как она содержит w.**

Шаг 3: Применив индукцию по размерности V, лемму можно считать доказанной для любого V' с $\dim V' < \dim V$. Применим ее к V' из шага 2, с гиперплоскостями $W_i' := V' \cap W_i$, и найдем точку на V', которая не содержится ни в одном из W_i. ■

Конечные поля

Сведения о конечных полях: Порядок конечного поля равен p^n, где p – его характеристика. На любом поле k характеристики p задан **гомоморфизм Фробениуса**, $Fr: \ k \to k$, $x \to x^p$. В любое поле характеристики p естественно вложено конечное поле $\mathbb{F}_p$ из p элементов.

Поле порядка p^n обозначается $\mathbb{F}_{p^n}$. В устаревшей литературе эти поля называются "полями Галуа".

УТВЕРЖДЕНИЕ: Все элементы $\mathbb{F}_{p^n}$ удовлетворяют уравнению $x^{p^n} - x = 0$.

ДОКАЗАТЕЛЬСТВО: Группа обратимых элементов $\mathbb{F}_{p^n}^*$ имеет порядок $p^n - 1$, и **по теореме Лагранжа, все ее элементы удовлетворяют $x^{p^n - 1} = 1$.** ■

СЛЕДСТВИЕ: $\mathbb{F}_{p^n}$ есть поле разложения многочлена $x^{p^n - 1} - 1$ над $\mathbb{F}_p$. **Поэтому все поля из p^n элементов изоморфны.**

Конечные поля и примитивные корни

УТВЕРЖДЕНИЕ: Группа $\mathbb{F}_{p^n}^*$ – циклическая.

Доказательство. Шаг 1: Пусть $p^n - 1 = \prod p_i^{\alpha_i}$ – разложение $p^n - 1$ на простые множители. По теореме о классификации абелевых групп, $G := \mathbb{F}_{p^n}^*$ есть произведение абелевых групп G_{p_i} порядка $p_i^{\alpha_i}$. **G циклическая $\Leftrightarrow$ все G_i циклические** (китайская теорема об остатках).

Шаг 2: Значит, если G не циклическая, то **порядок каждого элемента в $\mathbb{F}_{p^n}^*$ делит $m := \prod p_i^{\alpha_i - k_i}$, где какой-то из k_i больше 0.**

Шаг 3: В этом случае, **все элементы $\mathbb{F}_{p^n}^*$ являются корнями многочлена $x^m = 1$, что противоречит теореме Безу.** ■

ОПРЕДЕЛЕНИЕ: $\alpha \in \mathbb{F}_{p^n}^*$ называется **примитивным корнем** (или первообразным корнем), если его порядок равен $p^n - 1$.

ЗАМЕЧАНИЕ: Нахождение примитивных корней есть **важная народнохозяйственная задача.** К примеру, первая современная криптосистема с открытым ключом (Diffie-Hellman key exchange, 1976) использовала вычислительную трудность нахождения "конечного логарифма", то есть числа $b := \log_\varepsilon(a) \bmod p$ такого, что $\varepsilon^b = a$, где ε первообразный корень, а a какой-то остаток.

Группа Галуа для конечного поля

ТЕОРЕМА: Любое расширение конечных полей есть расширение Галуа.

Доказательство. Шаг 1: Поскольку k содержит $\mathbb{F}_p$, достаточно доказать, что $[K : \mathbb{F}_p]$ расширение Галуа, где $K = \mathbb{F}_{p^n}$.

Шаг 2: Возьмем первообразный корень $\varepsilon \in \mathbb{F}_{p^n}^*$. Тогда $K = \mathbb{F}_p[\varepsilon]$, но ε является корнем многочлена $P(t) = x^{p^n-1} - 1$, который разлагается на множители в K. Значит, $K \otimes_{\mathbb{F}_p} K = K[t]/(P) = \bigoplus K$. ■

ТЕОРЕМА: Группа Галуа $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ **это циклическая группа, порожденная гомоморфизмом Фробениуса** Fr.

Доказательство. Шаг 1: Поскольку порядок группы Галуа равен степени расширения (то есть n), **достаточно убедиться, что порядок Fr равен n.**

Шаг 2: Любой элемент $z \in \mathbb{F}_{p^n}$ удовлетворяет $z^{p^n} = z$, то есть $\mathrm{Fr}^n = 1$. Если $\mathrm{Fr}^k = 1$ для $k < 1$, мы получим, что $z^{p^k} = z$ **имеет** p^n **решений в** $\mathbb{F}_{p^n}$**, что невозможно по теореме Безу.** ■

Лекция 8: циклические расширения и теорема Абеля

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k.

ОПРЕДЕЛЕНИЕ: Конечное расширение есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

ТЕОРЕМА: Сумма, произведение, частное алгебраических над k **элементов алгебраично над** k**.** ■

Примитивные расширения (повторение)

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра** $R_v \subset R$**, порожденная** v**, изоморфна** $k[t]/(P)$**.**

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо** $k[t]/(P)$ **является полем.**

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение** k**, полученное добавлением корня** $P(t)$. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно.

Расширения Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – конечное расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

ТЕОРЕМА: Пусть $K \supset K' \supset k$ – цепочка конечных расширений. Предположим, что $[K : k]$ – расширение Галуа. **Тогда $[K : K']$ тоже расширение Галуа.**

ТЕОРЕМА: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней $\alpha_1, ..., \alpha_n$ в конечном расширении $[K : k]$. Предположим, что K порождено $\{\alpha_i\}$. **Тогда это расширение Галуа.**

ОПРЕДЕЛЕНИЕ: Пусть $[\bar{k} : k]$ – алгебраическое замыкание k, а $K \subset \bar{k}$ – поле, полученное из k добавлением всех корней $\alpha_i \in \bar{k}$. Тогда K называется **полем разложения $P(t)$.**

ЗАМЕЧАНИЕ: В характеристике 0, поля разложения суть поля Галуа (в характеристике p, не обязательно)

УТВЕРЖДЕНИЕ: Если $[K : k]$ – конечное расширение, $\operatorname{char} k = 0$, то **существует расширение $[K_1 : K]$ такое, что $[K_1 : k]$ – расширение Галуа.**

Группа Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – расширение Галуа. **Группой Галуа** $[K : k]$ называется группа $\operatorname{Aut}_k(K)$ k-линейных автоморфизмов поля K.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\operatorname{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

СЛЕДСТВИЕ: Порядок группы Галуа равен степени $[K:k]$.

СЛЕДСТВИЕ: Пусть $[K:k]$ – расширение Галуа. Рассмотрим действие группы Галуа $\mathrm{Aut}_k(K)$ на $K\otimes_k K$ автоморфизмами, $\zeta(a\otimes b)=a\otimes\zeta(b)$. **Это действие транзитивно на компонентах разложения в прямую сумму $K\otimes_k K=\bigoplus K$.**

СЛЕДСТВИЕ: Пусть $[K:k]$ – расширение Галуа, которое примитивно: $K=k[t]/(P)$, где $P(t)\in k[t]$. **Тогда $\mathrm{Aut}_k(K)$ действует транзитивно на корнях $P(t)$.**

Основная теорема теории Галуа (повторение)

ЛЕММА: Пусть $[K:k]$ – расширение Галуа, а $G'\subsetneq \mathrm{Aut}_k K$ есть нетривиальная подгруппа группы Галуа. **Тогда $K^{G'}\neq k$.**

ЛЕММА: Пусть $[K:k]$ – расширение Галуа, а $a\in K$ – элемент, инвариантный относительно $\mathrm{Aut}_k(K)$. **Тогда $a\in k\subset K$.**

ТЕОРЕМА: (Основная теорема теории Галуа)
Пусть $[K:k]$ – расширение Галуа. Тогда соответствия **стрелки $G'\to K^{G'}$ и $K'\to \mathrm{Aut}_{K'}K\subset G$ устанавливают биекцию между множеством подгрупп $G'\subset \mathrm{Aut}_k(K)$ и множеством промежуточных подполей $K\supset K'\supset k$.**

Примитивные расширения

ОПРЕДЕЛЕНИЕ: Расширение $[K:k]$ называется **сепарабельным**, если форма следа на K невырождена.

УПРАЖНЕНИЕ: Докажите, что следующие условия равносильны.
(i) $[K:k]$ сепарабельно
(ii) $K\otimes_k K$ не содержит нильпотентов.
(iii) Для любого $x\in K$, минимальный многочлен $P_x(t)\in k[t]$ не имеет кратных корней.

ТЕОРЕМА: (теорема Артина о примитивном элементе)
Пусть $[K:k]$ – конечное расширение, причем K бесконечно, и выполнено одно из условий: (1) $\mathrm{char}\, k=0$ (2) $[K:k]$ – подполе в расширении Галуа (3)

$[K:k]$ сепарабельно. **Тогда $[K:k]$ примитивно**, то есть порождено одним элементом $x \in K$.

ЗАМЕЧАНИЕ: Первые два утверждения были доказаны на прошлой лекции, 3-е оставлено в качестве упражнения.

Циклотомические расширения

ОПРЕДЕЛЕНИЕ: Циклотомическое расширение есть поле разложения для многочлена $P(t) := \sum_{i=0}^{n-1} t^i$.

ЗАМЕЧАНИЕ: $P(t) = \frac{t^n-1}{t-1}$, то есть **циклотомическое расширение получается добавлением всех корней степени n из единицы.**

УТВЕРЖДЕНИЕ: Группа корней степени n из единицы циклическая.

ДОКАЗАТЕЛЬСТВО: Дословно то же самое, что для $\mathbb{F}_{p^n}$. ■

ОПРЕДЕЛЕНИЕ: $\varepsilon \in \mathbb{C}$ называется **примитивным корнем**, или же **первообразным корнем** степени n из единицы, если ε порождает группу корней степени n.

Группа Галуа циклотомического расширения

ОПРЕДЕЛЕНИЕ: Группа Галуа циклотомического расширения вложена в мультипликативную группу $(\mathbb{Z}/n)^*$ остатков, взаимно простых с n.

Доказательство. Шаг 1: Пусть ε есть примитивный корень, а $\nu \in \mathrm{Aut}[K:\mathbb{Q}]$ – элемент группы Галуа. Тогда ν переводит ε в какой-то другой примитивный корень, то есть в ε^a для a, взаимно простого с n. Значит, **группа Галуа циклотомическоро расширения вложена в $(\mathbb{Z}/n)^*$, и она действует на корнях, переводя корень e в e^a.** ■

ЗАМЕЧАНИЕ: На самом деле группа Галуа $\mathrm{Aut}[K:\mathbb{Q}]$ изоморфна группе $(\mathbb{Z}/n)^*$, но доказать это довольно трудно.

Циклические расширения

ОПРЕДЕЛЕНИЕ: Расширение Галуа $[K : k]$ называется **циклическим**, если его группа Галуа циклическая.

УТВЕРЖДЕНИЕ: Пусть поле k содержит все корни степени n из единицы, а $[K : k]$ – поле разложения многочлена $P(t) = t^n - a$, где $a \neq b^l$ для любого $l|n$. Предположим, что $\operatorname{char} p$ не делит n. **Тогда это расширение циклическое.**

ДОКАЗАТЕЛЬСТВО: Это расширение Галуа, ибо **если $\operatorname{char} p$ не делит n, то $P(t)$ и $P'(t)$ взаимно просты,** а значит, у $P(t)$ нет кратных корней.

Шаг 2: Если α есть корень $P(t)$, можно написать $P(t) = \prod(t - \zeta_i\alpha)$, где $\{\zeta_i\}$ – множество всех корней степени n из 1. Значит, K получается из k добавлением α.

Циклические расширения (окончание)

Шаг 3: Если полином $P(t)$ приводим и раскладывается в произведение $P(t) = Q_1(t)Q_2(t)$, мы имеем $Q_i(t) = \prod(t - \zeta_j\alpha)$, где произведение берется по части корней. Значит, свободный член Q_i имеет вид $\alpha^m\zeta$, где $\zeta \in k$ – корень из единицы. Применив алгоритм Евклида к соотношениям $\alpha^m \in k$ и $\alpha^n \in k$, получим соотношение вида $\alpha^l \in k$ для $l|n$. Значит, $P(t)$ неприводим.

Шаг 4: Пусть ζ – какой-то корень степени n из 1. Рассмотрим автоморфизм $K = k[t]/(P)$, переводящий t в ζt. Группа, порожденная такими автоморфизмами, изоморфна $\mathbb{Z}/n$. **Значит, ее порядок равен степени $[K : k]$.** Поэтому это вся группа Галуа. ■

Резольвента Лагранжа

ТЕОРЕМА: (теорема Куммера) Пусть поле k содержит все корни степени n из единицы, а $[K : k]$ – циклическое расширение степени n. **Тогда $K = k[t]/(P)$, где $P(t) = t^n - a$.**

Доказательство. Шаг 1: Для конечного поля все уже доказано. Будем доказывать для бесконечного.

Шаг 2: Расширение Галуа всегда примитивно. Пусть ν – образующая группы $G := \mathrm{Aut}_k(K)$, $\xi \in k$ – примитивный корень из единицы степени n, а $a \in K$ – примитивный элемент. Напишем **резольвенту Лагранжа** $L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \dots + \xi^{-n+1}\nu^{n-1}(a)$. Тогда $\nu(L) = \xi L$.

Шаг 3: Пусть $V \subset K$ – k-векторное подпространство, порожденное $a, \nu(a), \nu^2(a), \dots$ Число G-инвариантных подпространств $V \subsetneq K$ конечно. Выбрав a вне этих подпространств, можно считать, что все $a, \nu(a), \nu^2(a), \dots$ линейно независимы над k, **а значит,** $L \neq 0$.

Резольвента Лагранжа (окончание)

УТВЕРЖДЕНИЕ: Пусть поле k содержит все корни степени n из единицы, а $[K : k]$ – циклическое расширение степени n. **Тогда** $K = k[t]/(P)$**, где** $P(t) = t^n - a$.

Шаг 2: Расширение Галуа всегда примитивно. Пусть ν – образующая группы $G := \mathrm{Aut}_k(K)$, $\xi \in k$ – примитивный корень из единицы степени n, а $a \in K$ – примитивный элемент. Напишем **резольвенту Лагранжа** $L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \dots + \xi^{-n+1}\nu^{n-1}(a)$. Тогда $\nu(L) = \xi L$.

Шаг 3: Пусть $V \subset K$ – k-векторное подпространство, порожденное $a, \nu(a), \nu^2(a), \dots$ Число G-инвариантных подпространств $V \subsetneq K$ конечно. Выбрав a вне этих подпространств, можно считать, что все $a, \nu(a), \nu^2(a), \dots$ линейно независимы над k, **а значит,** $L \neq 0$.

Шаг 4: Тот же аргумент показывает, что **можно выбрать** a **таким образом, что** L **тоже примитивно.**

Шаг 5: $\prod_{i=0}^{n-1}(t - \nu^i(L)) = t^n - L^n$, но L^n инвариантно относительно $\mathrm{Aut}_k(K)$, а значит, лежит в k. **Мы получаем, что** $K = k[t]/(P)$**, где** $P(t) = t^n - L^n$. ■

Расширения Галуа и корни

ТЕОРЕМА: Пусть $[K : k]$ – конечное, сепарабельное, примитивное расширение. Тогда следующие условия равносильны.

(i) $[K : k]$ **– расширение Галуа.**

(ii) **Для любого $x \in K$, все корни его минимального многочлена $P_x(t) \in k[t]$ содержатся в K.**

Доказательство. Шаг 1: Импликация (ii) $\Rightarrow$ (i) следует из теоремы о примитивном элементе, ибо $K = k[x]$ есть поле разложения многочлена $P_x(t) \in k[t]$.

Шаг 2: Пусть K – расширение Галуа, $x \in K$, а $K' := k[x]$ – порожденное им подполе. Тогда $K' \otimes_k K$ есть подкольцо в $K \otimes_k K = \bigoplus K$. Поскольку $K' \otimes_k K$ линейно относительно умножения на K справа, **$K' \otimes_k K$ – тоже прямая сумма нескольких копий K.**

Шаг 3: Поскольку $K' = k[t]/(P_x)$, $K' \otimes_k K = K[t]/(P_x)$, а **коль скоро все слагаемые $K[t]/(P_x)$ одномерны над K, многочлен $P_x(t)$ разлагается на линейные множители в $K[t]$.** Это доказывает импликацию (i) $\Rightarrow$ (ii). ■

Группа Галуа и корни

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа, $x \in K$, а $P_x(t) \in k[t]$ его минимальный многочлен. **Тогда группа Галуа $\mathrm{Aut}_k(K)$ действует транзитивно на корнях $P_x(t)$.**

ДОКАЗАТЕЛЬСТВО: Все коэффициенты многочлена $\prod_{\in \in \mathrm{Aut}_k(K)} (t - \nu(x)$ $\mathrm{Aut}_k(K)$-инвариантны, значит, лежат в k. Поэтому этот многочлен делится на $P_x(t)$. ■

Последовательности расширений Галуа

ТЕОРЕМА: Пусть $[K : K' : k]$ конечные расширения, причем $[K : k]$ – расширение Галуа. Тогда следующие условия равносильны.

(i) **$[K' : k]$ – расширение Галуа.**

(ii) Группа Галуа $\mathrm{Aut}_{K'}(K)$ **– нормальная подгруппа в $\mathrm{Aut}_k(K)$.**

(iii) **Действие $\mathrm{Aut}_k(K)$ сохраняет $K' \subset K$.**

В этой ситуации, $\mathrm{Aut}_k(K') = \mathrm{Aut}_k(K)/\mathrm{Aut}_{K'}(K)$.

Доказательство. Шаг 1: Подполя в $K \supset K'' \supset k$ находятся в биективном соответствии с подгруппами в $\mathrm{Aut}_k(K)$. Группа Галуа $G := \mathrm{Aut}_k(K)$ переставляет подгруппы G, действуя на них сопряжениями. **Нормальные подгруппы суть такие, которые неподвижны при действии G.** Поэтому

соответствующие поля – тоже неподвижны (при действии G на K). Это доказывает равносильность (ii) и (iii).

Последовательности расширений Галуа (окончание)

ТЕОРЕМА: Пусть $[K : K' : k]$ конечные расширения, причем $[K : k]$ – расширение Галуа. Тогда следующие условия равносильны.

(i) $[K' : k]$ **– расширение Галуа.**

(ii) Группа Галуа $\mathrm{Aut}_{K'}(K)$ **– нормальная подгруппа в** $\mathrm{Aut}_k(K)$**.**

(iii) **Действие** $\mathrm{Aut}_k(K)$ **сохраняет** $K' \subset K$**.**

Шаг 2: Пусть $x \in K'$ – какой-то элемент, а $P_x(t) \in k[t]$ – его минимальный полином. В силу предыдущей теоремы, K' есть расширение Галуа тогда и только тогда, когда $P_x(t)$ разложим в K', причем в этом случае G действует на его корнях транзитивно. **Группа Галуа** G **переставляет корни многочлена** $P_x(t)$**, действуя на них транзитивно.** Значит, если G сохраняет K', все корни $P_x(t)$ лежат в K'. Это доказывает импликацию (iii) $\Rightarrow$ (i).

Шаг 3: Если же $[K' : k]$ – расширение Галуа, то G **сохраняет** K'**, потому что она переставляет корни многочленов** $P(t) \in k[t]$**,** а для каждого корня $P(t)$, содержащегося в K', все остальные тоже там содержатся.

Шаг 4: Изоморфизм $\mathrm{Aut}_k(K') = \mathrm{Aut}_k(K)/\mathrm{Aut}_{K'}(K)$ следует из того, что $\mathrm{Aut}_k(K)$ действует на K' автоморфизмами, без инвариантов, а ядро отображения $\mathrm{Aut}_k(K) \to \mathrm{Aut}_k(K')$ есть $\mathrm{Aut}_{K'}(K)$. ■

Разрешимые группы

ОПРЕДЕЛЕНИЕ: Группа G называется **разрешимой**, если содержит цепочку нормальных подгрупп $G = G_0 \supset G_1 \supset ... \supset G_n = \{e\}$, причем каждая из факторгрупп коммутативна.

УТВЕРЖДЕНИЕ: Пусть расширение Галуа $[K : k]$ содержит цепочку подполей $K = K_1 \supset K_2 \supset ... \supset K_n = k$ со следующими свойствами:

(i) Для всех i, $[K_i : k]$ – расширение Галуа.

(ii) Группа Галуа $\mathrm{Aut}_{K_{i+1}}(K_i)$ абелева.

Тогда группа Галуа $[K : k]$ **разрешима.** Обратное тоже верно: **каждое расширение с разрешимой группой Галуа может быть получено таким образом.**

ДОКАЗАТЕЛЬСТВО: Сразу следует из предыдущей теоремы. ■

Теорема Абеля

ТЕОРЕМА: (теорема Абеля)
Пусть поле k содержит все корни из 1, а расширение Галуа $[K:k]$ содержит цепочку подполей $K = K_1 \supset K_2 \supset ... \supset K_n = k$ со следующими свойствами:

(i) Для всех i, $[K_i : k]$ – расширение Галуа.

(ii) Расширение $[K_i : K_{i-1}]$ получено добавлением корней многочлена $P(t) = t^{n_i} - a_i$.

Тогда группа Галуа $\mathrm{Aut}_k(K)$ разрешима. Обратное тоже верно: **любое расширение Галуа $[K:k]$ с разрешимой группой Галуа может быть получено таким образом.**

ДОКАЗАТЕЛЬСТВО: Разрешимость $\mathrm{Aut}_k(K)$ следует из предыдущего утверждения, и вычисления группы Галуа для циклического расширения. Обратное утверждение следует из теоремы Куммера, утверждающей, что каждое циклическое расширение получено добавлением корней многочлена $P(t) = t^{n_i} - a_i$. ■

СЛЕДСТВИЕ: (теорема Абеля)
Полиномиальное уравнение разрешимо в радикалах тогда и только тогда, когда его группа Галуа разрешима.

Экзамены, сессия

В следующую пятницу (22.03.2013), будет коллоквиум в виде устной контрольной. Письменная контрольная (тоже задачи) будет 29.03.2013, с 12:00 до 15:30.

Вместе с решениями, 29 марта студенты **должны сдать копии своих ведомостей,** с отметками о том, **сколько баллов им причитается за каждый листочек**, и кратким объяснением, почему именно столько. Показ работ и окончательная расстановка оценок – среда, 3-го апреля (первая половина дня).

Студенты, которые не сдадут свои ведомости 29-го, ничего за листочки не получат (или получат, но не сразу и без удовольствия).

Окончательная оценка вычисляется по формуле $F = 0.1B$, где B есть сумма баллов за все (округление вниз).

Глава 4

Письменное задание, задачи коллоквиума и письменного экзамена

Письменное задание 1: тензорные произведения, инварианты групп и поля

Версия 1.0, 18.01.2013.

Число очков за это задание вычисляется по формуле $\frac{4}{3}s - \max(s-5, 0)$, где s – сумма баллов за задачи. Можно ссылаться на теоремы из сданного студентом курса алгебры для ВШЭ, но нужно привести точную формулировку теоремы, и сказать, какой именно курс ее содержал. Кроме того, студент, ссылающийся на какую-то теорему. берет на себя обязанность рассказать ее доказательство, по первому требованию.

Решение письменное, сдается до 22:00 пятницы, 18-го января (можно положить на стол рядом с комнатой 210). Через неделю будет обсуждение задач, пожалуйста, будьте готовы рассказать то, что вы нарешали. Также решение можно сдать устно во время семинара.

Успешно учащиеся студенты должны получать по 10 баллов в неделю, во избежание пересдач и других эксцессов.

Задача 1. Пусть V – конечномерное пространство над полем k, снабженное действием группы G. Всегда ли в $V \otimes_k V$ найдется ненулевой G-инвариантный вектор?

а. [1 балл] G конечна, $k = \mathbb{R}$.

б. [3 балла] G бесконечна, $k = \mathbb{R}$.

в. [2 балла] G конечна, $k = \mathbb{Q}$

г. [2 балла] G конечна, k – конечное поле

д. [2 балла] G конечна, $k = \mathbb{C}$

е. [5 баллов] G конечна, $k = \mathbb{Z}/2\mathbb{Z}$.

Задача 2. V – векторное пространство, не обязательно конечномерное. **Естественное отображение** $V \longrightarrow V^{**}$ есть отображение, которое инвариантно относительно канонического действия группы $GL(V)$ (постройте каноническое действие самостоятельно, если вы не помните определение).

а. [1 балл] Постройте нетривиальное естественное отображение $V \to V^{**}$. Докажите, что оно инъективно.

б. [4 балла] Проверьте, что такое отображение единственно с точностью до множителя, или убедитесь, что это не так.

в. [2 балла] Докажите, что естественное вложение $V \longrightarrow V^{**}$ сюръективно $\Leftrightarrow V$ конечномерно.

Задача 3. A, B – векторные пространства (не обязательно конечномерные). **Естественное отображение** $A^* \otimes B \longrightarrow \mathrm{Hom}(A, B)$ есть отображение, которое инвариантно относительно канонического действия группы $GL(A) \times GL(B)$.

а. [2 балл] Постройте нетривиальное естественное отображение

$$A^* \otimes B \longrightarrow \mathrm{Hom}(A, B).$$

Докажите, что построенное вами отображение инъективно.

б. [4 балла] Докажите, что такое отображение единственно с точностью до множителя.

в. [3 балла] Всегда ли это изоморфизм?

Определение 1. Групповая алгебра группы G над полем k есть векторное пространство над k с базисом G, где умножение определено на векторах базиса как в G, а на всех остальных векторах по линейности.

Определение 2. Двусторонний идеал в алгебре A есть такое подмножество $I \subset A$, что $A \cdot I \subset I$ и $I \cdot A \subset I$.

Задача 4 (2 балла). Докажите, что в групповой алгебре $k[G]$ любой группы найдется нетривиальный двусторонний идеал.

Задача 5 (4 балла). Найдите все двусторонние идеалы в $\mathbb{R}[G]$, где $G = \mathbb{Z}/3\mathbb{Z}$.

Задача 6 (5 баллов). Пусть K есть поле, а $\phi : K \longrightarrow K$ – гомоморфизм. Докажите, что ϕ инъективно. Всегда ли ϕ сюръективно?

Задачи коллоквиума

`Впервые выдано 22.03.2013. Версия 1.2, 19.03.2013.`

Каждому студенту выдается список задач для решения, по две из каждого раздела, созданный заранее с помощью специального рандомайзера. Число очков за это задание вычисляется по формуле $b = 4\max(s, 8)$, где s – сумма баллов за задачи. Можно ссылаться на теоремы из сданного студентом курса алгебры для ВШЭ, но нужно привести точную формулировку теоремы, и сказать, какой именно курс ее содержал. Кроме того, студент, ссылающийся на какую-то теорему. берет на себя обязанность рассказать ее доказательство по первому требованию экзаменатора. Также можно ссылаться на сданные задачи из листочков, но нужно хорошо представлять себе доказательство.

Решение устное, сдается с 12:00 до 15:30, пятница, 22.03.2013. Аналогичное задание для письменного решения будет выдаваться в пятницу с 12:00 до 15:30, 29.03.2013. Вместе с решениями, 29 марта студенты должны сдать копии своих ведомостей, с отметками о том, сколько баллов им причитается за листочки (и объяснением, почему именно столько). Показ работ и окончательная расстановка оценок – среда, 3-го апреля (первая половина дня). Студенты, которые не сдадут свои ведомости 29-го, ничего за листочки не получат.

Окончательная оценка вычисляется по формуле $F = 0.1B$, где B есть сумма баллов за все (округление вниз).

Алгебраические числа и конечные расширения

Определение 1. Степень $\deg_k(x)$ алгебраического числа $x \in \bar{k}$ есть степень расширения $[k[x] : k]$, порожденного x.

Задача 1. Пусть α, β – корни неприводимого многочлена $P(t) \in k[t]$ степени n. Докажите, что $\deg(\alpha + \beta) \leqslant \frac{n(n-1)}{2}$.

Задача 2. Пусть α, β – разные корни корни неприводимого многочлена $P(t) \in k[t]$, $\operatorname{char} k = 0$. Докажите, что $\deg(\alpha - \beta) \geqslant 2$, или найдите контрпример.

Задача 3. Пусть α, β – разные корни корни неприводимого многочлена $P(t) \in k[t]$, $\operatorname{char} k = 0$ степени > 2. Докажите, что $\deg(\alpha + \beta) \geqslant 2$, или найдите контрпример.

Задача 4. Пусть α, β – разные корни корни неприводимого многочлена $P(t) \in k[t]$, $\operatorname{char} k = 0$. Докажите, что $\deg(\alpha\beta^{-1}) \geqslant 2$, или найдите контрпример.

Задача 5. Пусть α, β – разные корни корни неприводимого многочлена $P(t) \in k[t]$, $\operatorname{char} k = 0$ степени > 2. Докажите, что $\deg(\alpha\beta) \geqslant 2$, или найдите контрпример.

Конечномерные кольца

Задача 6. Докажите, что $\mathbb{F}_4 \otimes_{\mathbb{F}_2} \mathbb{F}_8 \cong \mathbb{F}_{64}$.

Задача 7. Докажите, что $\mathbb{F}_9 \otimes_{\mathbb{F}_3} \mathbb{F}_{81} \cong \mathbb{F}_{81} \oplus \mathbb{F}_{81}$.

Задача 8. Докажите, что $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}]$ – поле.

Задача 9. Докажите, что $\mathbb{F}_p[t] \otimes_{\mathbb{F}_p[t^p]} \mathbb{F}_p[t]$ содержит нильпотенты.

Задача 10 (2 балла). Докажите, что форма следа в расширении $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ невырождена.

Задача 11. Найдите расширение $[K : k]$ степени 3, такое, что $K \otimes_k K$ есть прямая сумма двух полей.

Расширения Галуа

Задача 12. Пусть $K \subsetneq \mathbb{R}$ – расширение $\mathbb{Q}$ степени 3. Может ли $[K : \mathbb{Q}]$ быть расширением Галуа?

Задача 13. Пусть $[k : \mathbb{Q}]$ – квадратичное расширение. Докажите, что $[k[\sqrt[11]{3}] : k]$ – не расширение Галуа.

Задача 14. Докажите, что $[\mathbb{Q}[\sqrt[n]{5}] : \mathbb{Q}]$ – не расширение Галуа для любого $n \geqslant 3$.

Задача 15. Пусть $k := \mathbb{F}_p(t)$ – поле рациональных функций над $\mathbb{F}_p$. Постройте конечное расширение $[K : k]$, которое не является расширением Галуа.

Задача 16 (2 балла). Пусть G – конечная группа, которая действует на поле K автоморфизмами. Докажите, что $[K : K^G]$ – конечное расширение. Докажите, что это расширение Галуа.

Группы Галуа

Задача 17 (2 балла). Найдите расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа $\mathbb{Z}/15\mathbb{Z}$.

Задача 18 (2 балла). Найдите расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа $\mathbb{Z}/9\mathbb{Z}$.

Задача 19 (2 балла). Постройте расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа $(\mathbb{Z}/3\mathbb{Z})^2$.

Задача 20 (2 балла). Пусть $k = \mathbb{R}(t)$ поле рациональных функций над $\mathbb{R}$, а $[K : k]$ расширение Галуа с абелевой группой Галуа G. Предположим, что порядок G нечетный. Докажите, что G циклическая, или найдите контрпример.

Задача 21 (2 балла). Постройте расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа $\mathbb{Z}/20\mathbb{Z}$.

Вычисление группы Галуа

Задача 22 (2 балла). Пусть $P(t) = t^3 + 5t + 5$. Докажите, что этот полином неприводим над $\mathbb{Q}$. Найдите группу Галуа его поля разложения над $\mathbb{Q}$.

Задача 23 (2 балла). Пусть $P(t) = t^4 - 2$. Докажите, что этот полином неприводим над $\mathbb{Q}$. Докажите, что группа Галуа его поля разложения над $\mathbb{Q}$ изоморфна группе D_4 симметрий квадрата.

Задача 24 (2 балла). Пусть $P(t) \in \mathbb{F}_p(t)$ – неприводимый полином степени n, а K его поле разложения. Докажите, что $\mathrm{Aut}_{\mathbb{F}_p}(K) = \mathbb{Z}/n\mathbb{Z}$, или найдите контрпример.

Задача 25. Пусть K – циклотомическое поле, полученное добавлением всех корней степени 17 из 1. Докажите, что все подполя $K' \subset K$ суть расширения Галуа $\mathbb{Q}$.

Задача 26 (2 балла). Пусть $k = \mathbb{F}_{13}(x)$ есть поле рациональных функций над $\mathbb{F}_{13}$, а $P(t) = t^5 - x$. Докажите, что этот полином неприводим, и найдите порядок группы Галуа его поля разложения.

Задачи письменного экзамена

`Впервые выдано 29.03.2013. Версия 1.0, 25.03.2013.`

Каждому студенту выдается список задач для решения, по одной из каждого раздела, созданный заранее с помощью специального рандомайзера. Число очков за это задание вычисляется по формуле $b = 8\min(s, 3)$, где s – сумма баллов за задачи. Можно ссылаться на теоремы из сданного студентом курса алгебры для ВШЭ и сданные задачи из листочков. Все ответы должны быть снабжены доказательством, по возможности полным и понятным (иначе баллы будут снижаться).

Письменный экзамен проходит с 12:00 до 15:30, 29.03.2013. Вместе с решениями, 29 марта студенты должны сдать копии своих ведомостей, с отметками о том, сколько баллов им причитается за листочки (и объяснением, почему именно столько). Показ работ и окончательная расстановка оценок – среда, 3-го апреля (первая половина дня). Студенты, которые не сдадут свои ведомости 29-го, ничего за листочки не получат.

Окончательная оценка вычисляется по формуле $F = 0.1B$, где B есть сумма баллов за все (округление вниз).

Теория Галуа

Задача 1. Пусть $K := \mathbb{F}_p(x, y)$ – поле рациональных функций от x, y, а $k \subset K$ его подполе, порожденное x^p, y^p. Докажите, что расширение $[K : k]$ не примитивно.

Задача 2. Пусть k поле конечной характеристики, а $[K : k]$ – примитивное расширение k. Докажите, что любое промежуточное поле $K \supset K' \supset k$ примитивно.

Задача 3. Пусть $[K : \mathbb{Q}]$ – расширение Галуа с группой Галуа $(\mathbb{Z}/2)^2$. Докажите, что $K = \mathbb{Q}[\sqrt{a}, \sqrt{b}]$, для каких-то $a, b \in \mathbb{Q}$.

Задача 4. Найдите неприводимый полином степени 3 над $\mathbb{Q}$ такой, что группа Галуа его поля разложения изоморфна S_3 (симметрической группе).

Задача 5. Найдите неприводимый полином степени 3 над $\mathbb{Q}$ такой, что группа Галуа его поля разложения изоморфна $\mathbb{Z}/3\mathbb{Z}$.

Неприводимые полиномы

Задача 6. Пусть k есть поле рациональных функций над $\mathbb{C}$: $k = \mathbb{C}(t)$. Докажите, что для любого $n > 0$ найдется неприводимый полином $P(x) \in k[x]$ степени n.

Задача 7. Пусть k есть конечное расширение $\mathbb{Q}$. Докажите, что для любого $n > 0$ найдется неприводимый полином $P(x) \in k[x]$ степени n.

Задача 8. Пусть k – конечное поле. Докажите, что для любого $n > 0$ найдется неприводимый полином $P(x) \in k[x]$ степени n.

Задача 9. Пусть k – поле рациональных функций над $\mathbb{C}$: $k = \mathbb{C}(t)$. Докажите, что полином $x^n + t^n + 1$ неприводим в $k[x]$.

Задача 10. Докажите, что полином $x^3 + y + y^5$ неприводим в $\mathbb{Z}[x, y]$.

Задача 11. Пусть k есть поле рациональных функций над $\mathbb{C}$: $k = \mathbb{C}(t)$. Докажите, что $x^7 + t^3x + t$ неприводим в $k[x]$.

Расширения Галуа поля $k = \mathbb{C}(t)$

В этом разделе, поле k есть поле рациональных функций над $\mathbb{C}$: $k = \mathbb{C}(t)$.

Задача 12. Найдите расширение Галуа $[K : k]$ с группой Галуа $(\mathbb{Z}/2\mathbb{Z})^3$.

Задача 13. Пусть $[K : k]$ есть поле разложения многочлена $P(x) = x^4 + 2tx^2 + t^2 - t$. Докажите, что он неприводим, и найдите группу Галуа $[K : k]$.

Задача 14. Пусть $P(x) = x^4 + bx^2 + c$, а уравнение $0 = x^2 + bx + c$ не имеет решений в k. Докажите, что полином $P(x)$ неприводим в $k[x]$, или найдите контрпример.

Задача 15. Найдите расширение Галуа $[K : k]$ с группой Галуа $(\mathbb{Z}/3\mathbb{Z})^2$.

Задача 16. Пусть $P_1, P_2, P_3 \in \mathbb{C}[t]$ – неприводимые полиномы без кратных корней, не имеющие общих корней, а $[K : k]$ – расширение k, полученное добавлением квадратных корней $\alpha_i := \sqrt{P_i}$. Докажите, что α_1, α_2, α_3 линейно независимы в K (над k).

Задача 17. В условиях предыдущей задачи, найдите группу Галуа $[K : k]$ (в решении этой задачи, линейную независимость корней α_i можно считать установленной).

Конечные поля и группы Галуа

Задача 18. Пусть $P(t) \in \mathbb{F}_p(t)$ – неприводимый полином степени n, а K его поле разложения. Докажите, что $\mathrm{Aut}_{\mathbb{F}_p}(K) = \mathbb{Z}/n\mathbb{Z}$, или найдите контрпример.

Задача 19. Пусть $k = \mathbb{F}_{41}(t)$ есть поле рациональных функций над $\mathbb{F}_{41}$, а $P(x) = x^5 - t \in k[x]$. Докажите, что этот полином неприводим, и найдите порядок группы Галуа его поля разложения.

Задача 20. Пусть $k = \mathbb{F}_p(t)$ есть поле рациональных функций над $\mathbb{F}_p$, а $[K : k]$ – расширение Галуа. Докажите, что группа Галуа $[K : k]$ абелева, или найдите контрпример.

Задача 21. Пусть $k = \mathbb{F}_{13}(t)$ есть поле рациональных функций над $\mathbb{F}_{13}$. Постройте расширение Галуа $[K : k]$ с группой Галуа $(\mathbb{Z}/2)^2$.

Задача 22. Пусть $k = \mathbb{F}_{83}(t)$ есть поле рациональных функций над $\mathbb{F}_{83}$. Постройте расширение Галуа $[K : k]$ с группой Галуа $\mathbb{Z}/41\mathbb{Z}$.

Задача 23. Докажите, что полином $P(t) = t^4 + 1$ неприводим над $\mathbb{Q}$. Докажите, что он приводим над $\mathbb{F}_p$, для любого p вида $4k + 1$.

Расширения Галуа поля $\mathbb{Q}$

Задача 24. Докажите, что $P(t) = t^4+1$ неприводим в $\mathbb{Q}[t]$, но приводим в $\mathbb{R}[t]$. Найдите группу Галуа его поля разложения.

Задача 25. Докажите, что $P(t) = t^4 - 24$ неприводим в $\mathbb{Q}[t]$. Найдите группу Галуа его поля разложения.

Задача 26. Пусть $K := \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$. Докажите, что $[K : \mathbb{Q}]$ – расширение Галуа, и найдите его группу Галуа.

Задача 27. Пусть K – поле разложения полинома $P(t) = t^4 - 2$ над $\mathbb{Q}$. Найдите группу Галуа $[K : \mathbb{Q}]$ и перечислите все подполя $K' \subset K$. Какие из этих подполей являются полями Галуа над $\mathbb{Q}$?

Задача 28. Докажите, что $\left[\mathbb{Q}\left[\sqrt{2+\sqrt{2+\sqrt{2}}}\right] : \mathbb{Q}\right]$ – расширение Галуа.

Задача 29. Докажите, что $x^n + x + 3$ неприводим над $\mathbb{Q}$ для любого $n > 1$.