

Алгебра. Неофициальный конспект

Лектор: Алексей Владимирович Степанов
Конспектировал Леонид Данилевич

IV семестр, весна 2024 г.

Оглавление

1	Гомологическая алгебра	2
1.1	Абелевы категории	2
1.2	Комплексы	4
1.3	Гомологии	5
1.4	Функторы между абелевыми категориями	8
1.5	Резольвенты	11
1.6	Резольвенты. Левый производный функтор	12
1.6.1	Длинная точная последовательность левых производных функторов	14
1.7	Производные функторы для \otimes	17
1.8	Производные функторы для Hom	18
1.9	Гомологии и когомологии групп	19
2	Теория Галуа	21
2.1	Базовые понятия про расширения полей	21
2.1.1	Алгебраическое замыкание одного поля в другом	22
2.1.2	Поле разложения	23
2.1.3	Сепарабельность	27
2.1.4	О сепарабельных расширениях	31
2.2	Соответствие Галуа	31

Глава 1

Гомологическая алгебра

Лекция I 12 февраля 2024 г.

1.1 Абелевы категории

Напомним некоторые определения из предыдущей лекции.

Определение 1.1.1 (Предаддитивная категория \mathcal{A}). $\forall A, B \in \mathcal{A} : \text{Mor}_{\mathcal{A}}(A, B)$ образует абелеву группу, и везде, где определена, выполнена дистрибутивность:

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma \quad (\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha$$

Определение 1.1.2 (Бипроизведение). Такая диаграмма, что

$$A \begin{array}{c} \xleftarrow{\pi_1} \\ \xrightarrow{\iota_1} \end{array} C \begin{array}{c} \xleftarrow{\pi_2} \\ \xrightarrow{\iota_2} \end{array} B$$

1. $\pi_1 \iota_1 = \text{id}_A$.
2. $\pi_2 \iota_2 = \text{id}_B$.
3. $\iota_2 \pi_2 + \iota_1 \pi_1 = \text{id}_C$.
4. $\pi_2 \iota_1 = 0$.
5. $\pi_1 \iota_2 = 0$.

Определение 1.1.3 (Аддитивная категория). Предаддитивная категория с финальным объектом и произведениями (любых двух объектов).

Эквивалентно, существуют инициальный объект и копроизведения, эквивалентно существуют нулевой объект и бипроизведения.

Определение 1.1.4 (Предабелева категория). Аддитивная категория, в которой у всех морфизмов есть ядро и коядро.

Определение 1.1.5 ((Ко)нормальный мономорфизм (эпиморфизм)). Он является (ко)эквалайзером (какой-то, неважно какой, пары стрелок).

Определение 1.1.6 (Абелева категория). Предабелева категория, в которой все мономорфизмы нормальны.

Пусть \mathcal{C} — категория. Вспомним про категорию стрелок $Arr\mathcal{C}$, в которой объекты — стрелки из $Mor(\mathcal{C})$, множество морфизмов между ϕ, ψ — это

$$Mor_{Arr\mathcal{C}}(\phi, \psi) = \{(\alpha, \beta) | \alpha : source(\phi) \rightarrow source(\psi), \beta : target(\phi) \rightarrow target(\psi), \beta\phi = \psi\alpha\}$$

$$\begin{array}{ccc} \bullet & \xrightarrow{\phi} & \bullet \\ \downarrow \alpha & & \downarrow \beta \\ \bullet & \xrightarrow{\psi} & \bullet \end{array}$$

Далее будем обозначать за $\ker f$ ядро стрелки, как уравнитель стрелки и нуля, а за $Ker f := source(\ker f)$ — объект (в конкретных категориях типа $mod\text{-}R$ это докатегорное понятие ядра — подмодуль без стрелки-вложения).

Лемма 1.1.1. \ker, coker — функторы $Arr\mathcal{A} \rightarrow Arr\mathcal{A}$.

Доказательство. Достаточно доказать для ядер, для коядер двойственно.

Определим действие \ker на морфизмах:

$$\begin{array}{ccccc} Ker f & \xrightarrow{\ker f} & A & \xrightarrow{f} & B \\ \downarrow \exists! \phi & & \downarrow \alpha & & \downarrow \beta \\ Ker f' & \xrightarrow{\ker f'} & A' & \xrightarrow{f'} & B' \end{array}$$

$f \cdot \ker f = 0 \Rightarrow \beta \cdot f \cdot \ker f = 0 \Rightarrow f' \cdot \alpha \cdot \ker f = 0$, откуда по универсальному свойству ядра $\exists! \phi : \ker f' \cdot \phi = \alpha \cdot \ker f$.

Положим $\ker(\alpha, \beta) = (\phi, \alpha)$. Далее несложно проверить, что данное определение сохраняет композицию и id . \square

Определение 1.1.7 (Точный функтор). Функтор, сохраняющий ядра и коядра.

Интересный факт (Теорема Фрейда — Митчелла (Freyd — Mitchell)). Для любой малой абелевой категории \mathcal{A} : $\exists R \in Ring$ (необязательно коммутативное кольцо с единицей) и строгий, полный, точный функтор $\mathcal{A} \rightarrow mod\text{-}R$.

Предложение 1.1.1. Для всякого морфизма $f : A \rightarrow B$ найдётся пунктирная стрелка, делающая диаграмму коммутативной.

$$\begin{array}{ccccccc} Ker f & \xrightarrow{\ker f} & A & \xrightarrow{f} & B & \xrightarrow{\text{coker } f} & CoKer f \\ & & \downarrow \text{coker } \ker f & & \uparrow \ker \text{coker } f & & \\ & & CoKer \ker f & \dashrightarrow^{\exists!} & Ker \text{coker } f & & \end{array}$$

Более того, в абелевой категории эта стрелка — изоморфизм.

Доказательство. Следует из эпи-моно разложения, доказанного на прошлой лекции, или из теоремы Митчелла.

Само построение пунктирной стрелки получается из универсальных свойств, а доказательство того, что это — изо — непростое. \square

Лемма 1.1.2. Пусть \mathcal{C} — полная подкатегория в абелевой категории \mathcal{A} . Следующие условия равносильны

- \mathcal{C} является абелевой.
- — $0_{\mathcal{A}} \in \mathcal{C}$, здесь, как обычно, $0_{\mathcal{A}}$ — нулевой объект категории \mathcal{A} .
- — \mathcal{C} содержит бипроизведение любых двух своих объектов.

– Ядра и коядра (взяты в \mathcal{A}) любых морфизмов из \mathcal{C} лежат в \mathcal{C} .

Доказательство.

\Leftarrow . Очевидно.

\Rightarrow . Чуть сложнее, доказывать не будем (и использовать тоже). \square

1.2 Комплексы

Если противное не оговорено, то всё происходит в абелевой категории \mathcal{A} , большими буквами обозначены объекты данной категории, маленькими — морфизмы.

Определение 1.2.1 (Комплекс). Такая диаграмма, что $\forall k \in \mathbb{Z} : d_k \cdot d_{k+1} = 0$.

$$\cdots \xrightarrow{d_{n+1}} C_{n+1} \xrightarrow{d_n} C_n \xrightarrow{d_{n-1}} C_{n-1} \xrightarrow{d_{n-2}} \cdots$$

Альтернативно, комплекс можно рассматривать, как функтор из категории (\mathbb{Z}, \geq) (полученной из частично упорядоченного множества) в \mathcal{A} (при котором образ композиции любых двух нетождественных морфизмов нулевой). Таким образом, комплексы — полная подкатегория в категории этих функторов.

Ещё один, следующий, взгляд на комплексы работает только для конкретной категории, уже вложенной в R -модули.

Определение 1.2.2 (Градуированный объект). $C_\bullet = \bigoplus_{n \in \mathbb{Z}} C_n$ с морфизмом $d : C_\bullet \rightarrow C_\bullet$, таким, что $d(C_n) \subset C_{n+p}$ для некоторой фиксированной *степени объекта* p (чаще всего она равна ± 1).

Определение 1.2.3 (Дифференциальный модуль). Градуированный объект (C_\bullet, d) со свойством $d^2 = 0$.

Определение 1.2.4 (Комплекс). Дифференциальный модуль степени -1 .

При развороте стрелок получается дифференциальный модуль степени $+1$, также известный, как *кокомплекс*:

$$\cdots \xleftarrow{d^{n+2}} C^{n+1} \xleftarrow{d^{n+1}} C^n \xleftarrow{d^n} C^{n-1} \xleftarrow{d^{n-1}} \cdots$$

Предостережение. У кокомплекса несколько другая нумерация стрелок, но мы их практически не будем использовать.

Определение 1.2.5 (Сдвиг комплекса (C_\bullet, d) на $p \in \mathbb{Z}$). Комплекс $(C[p]_\bullet, d[p])$, где $C[p]_n = C_{n+p}$ и $d[p]_n = d_{n+p}$.

Иногда при сдвиге комплекса определяют $d[p]_n = (-1)^p d_{n+p}$, но мы так делать не будем.

Лекция II

19 февраля 2024 г.

Определение 1.2.6 (Морфизм дифференциальных модулей $\bigoplus A_n \rightarrow \bigoplus B_n$). Такое $f : \bigoplus A_n \rightarrow \bigoplus B_n$, что $f(A_n) \subset B_n$, и диаграммы коммутативны:

$$\begin{array}{ccc} A_{n+1} & \xrightarrow{d_n^A} & A_n \\ \downarrow f & & \downarrow f \\ B_{n+1} & \xrightarrow{d_n^B} & B_n \end{array}$$

На языке абелевых категорий, надо рассматривать не одно отображение f , так как отношение $f(A_n) \subset B_n$ не выражается, а серию морфизмов $f_n : A_n \rightarrow B_n$.

Для всякого морфизма f коммутативна диаграмма в категории комплексов:

$$\begin{array}{ccc} A[1] & \xrightarrow{d^A} & A \\ \downarrow f[1] & & \downarrow f \\ B[1] & \xrightarrow{d^B} & B \end{array}$$

Если рассматривать комплексы, как функторы из категории (\mathbb{Z}, \geq) , то морфизмы между комплексами — естественные преобразования между функторами.

Теорема 1.2.1. Категория комплексов абелева.

Доказательство.

Лемма 1.2.1. Если \mathcal{C} — малая категория, \mathcal{A} — абелева, то $\text{Func}(\mathcal{C}, \mathcal{A})$ — тоже абелева категория.

Доказательство леммы.

Нулевой объект — функтор 0 , сопоставляющий каждому объекту $0_{\mathcal{A}}$, и каждой стрелке — нуль-стрелку.

Для двух функторов \mathcal{F}, \mathcal{G} : $(\mathcal{F} \oplus \mathcal{G})(C) = \mathcal{F}(C) \oplus \mathcal{G}(C)$.

Если $\eta \in \text{Mor}_{\text{Func}(\mathcal{C}, \mathcal{A})}(\mathcal{F}, \mathcal{G})$ (то есть η — естественное преобразование $\mathcal{F} \rightarrow \mathcal{G}$), то $(\text{Ker } \eta)(C) = \text{Ker}(\eta_C)$.

ker определяется аналогично лемме (лемма 1.1.1). Аналогично с коядрами.

Далее по-хорошему надо проверить, что выполняются все универсальные свойства, но мы этого делать не будем. \square

Ссылаемся на (лемма 1.1.2).

$$\begin{array}{ccccccc} \cdots & \longrightarrow & A_{n+1} & \xrightarrow{d_n^A} & A_n & \xrightarrow{d_{n-1}^A} & A_{n-1} \longrightarrow \cdots \\ & & & & & & \\ \cdots & \longrightarrow & B_{n+1} & \xrightarrow{d_n^B} & B_n & \xrightarrow{d_{n-1}^B} & B_{n-1} \longrightarrow \cdots \\ & & & & & & \\ \cdots & \longrightarrow & A_{n+1} \oplus B_{n+1} & \xrightarrow{d_n^{A \oplus B}} & A_n \oplus B_n & \xrightarrow{d_{n-1}^{A \oplus B}} & A_{n-1} \oplus B_{n-1} \longrightarrow \cdots \end{array}$$

Если $d^A \cdot d^A = 0$, и $d^B \cdot d^B = 0$, то (из теоремы Митчелла уж точно очевидно) $d^{A \oplus B} \cdot d^{A \oplus B} = 0$.

Ядра тоже являются комплексами, так как на языке конкретных категорий это просто подмодули. Двойственно с коядрами. \square

1.3 Гомологии

Дифференциал d является морфизмом комплексов $d : C[1] \rightarrow C$ (по-хорошему, $C[1]_{\bullet} \rightarrow C_{\bullet}$, но точку будем опускать):

$$\begin{array}{ccccccc} \cdots & \longrightarrow & C_{n+1} & \xrightarrow{d_n} & C_n & \longrightarrow & \cdots \\ & & \downarrow d_n & & \downarrow d_{n-1} & & \\ \cdots & \longrightarrow & C_n & \xrightarrow{d_{n-1}} & C_{n-1} & \longrightarrow & \cdots \end{array}$$

Ниже мы по произвольному комплексу C строим новые комплексы.

Определение 1.3.1 (Циклы). Комплекс $Z = Z(C) \stackrel{\text{def}}{=} \text{Ker } d[-1]$.

Определение 1.3.2 (Границы). Комплекс $B = B(C) \stackrel{def}{=} \text{Im } d[-1]$.

По определению, образ — это ядро коядра: $\text{Im } \phi \stackrel{def}{=} \text{Ker}(\text{coker } \phi)$. В абелевой категории канонически $\text{Im } \phi \cong \text{CoIm } \phi \stackrel{def}{=} \text{CoKer}(\text{ker } \phi)$.

На языке конкретных категорий, так как $d^2 = 0$, то $B \subset Z$, и можно определить фактормодуль $H := Z/B$ — *гомологии*.

То же самое можно сказать на языке универсальных свойств, хотя в будущем мы, ссылаясь на теорему Митчелла, будем всё писать исключительно в терминах элементов.

$$\begin{array}{ccccccc} Z[1] & \xrightarrow{z[1]} & C[1] & \xrightarrow{d} & C & \xrightarrow{d[-1]} & C[-1] \\ & & \downarrow b & \searrow \alpha & \uparrow z & & \\ & & B & \xrightarrow{\beta} & Z & \xrightarrow{\text{coker } \beta} & H \cdots \cdots \cdots 0 \end{array}$$

Построение H в терминах универсальных свойств. Так как $d[-1] \cdot d = 0$, то можно пропуститьсь через ядро: $\exists! \alpha : z \cdot \alpha = d$.

Далее, $z \cdot \alpha \cdot z[1] = d \cdot z[1] = 0$, а так как z — моно, то $\alpha \cdot z[1] = 0$. Значит, можно пропуститьсь через коядро, то есть $\exists! \beta : \beta b = \alpha$. Далее H определяется, как коядро β . \square

Следствие 1.3.1. В комплексах Z, B, H нулевые дифференциалы.

Доказательство. Из диаграммы следует, что в комплексе Z нулевые дифференциалы. B состоит из подмодулей в Z , H — из фактормодулей, понятно, что там дифференциалы тоже нулевые. \square

Примеры (Гомологии окружности).

- Рассмотрим окружность, как симплициальное множество: 

Построим $C_0 = \mathbb{Z}a + \mathbb{Z}b$ — свободная абелева группа на $\{a, b\}$, $C_1 = \mathbb{Z}x + \mathbb{Z}y$ — тоже свободная абелева группа, но на образующих $\{x, y\}$. Вместо \mathbb{Z} можно было взять любое другое кольцо.

Все остальные элементы комплекса объявляются нулями.

$$0 \longrightarrow C_1 \xrightarrow{d_1} C_0 \longrightarrow 0$$

Определим d_1 , как «конец минус начало»: $\begin{cases} d_1(x) = b - a, \\ d_1(y) = a - b \end{cases}$.

$$\text{Теперь } \begin{cases} Z_0 = C_0 \\ Z_1 = \mathbb{Z}(x + y) \end{cases} \quad \begin{cases} B_0 = \mathbb{Z}(b - a) \\ B_1 = 0 \end{cases} \quad \text{и} \quad \begin{cases} H_0 = Z_0/B_0 = (\mathbb{Z}a + \mathbb{Z}b)/\mathbb{Z}(b - a) \cong \mathbb{Z} \\ H_1 = Z_1/B_1 = \mathbb{Z}(x + y) \cong \mathbb{Z} \end{cases}.$$

- Теперь триангулируем окружность по-другому:  $\begin{cases} d_1(x) = b - a, \\ d_1(y) = c - b, \\ d_1(z) = a - c \end{cases}$.

$$\text{Теперь } \begin{cases} Z_0 = C_0 \\ Z_1 = \mathbb{Z}(x + y + z) \end{cases}, \quad \begin{cases} B_0 = \mathbb{Z}(b - a) + \mathbb{Z}(c - b) \\ B_1 = 0 \end{cases} \quad \text{и} \quad \begin{cases} H_0 \cong \mathbb{Z} \\ H_1 = \mathbb{Z}(x + y + z)/0 \cong \mathbb{Z} \end{cases}.$$

Ответ получился тот же самый, и это не случайно — есть теорема, что сингулярные/симплициальные гомологии (они равны для клеточных пространств) не зависят от триангуляции.

Упражнение 1.3.1. Триангулировать сферу, и вычислить гомологии. Дифференциал от треугольника ABC (ориентация — порядок вершин — важна) определяют, как его обход вдоль периметра: $AB + BC + CA$.

Теорема 1.3.1 (Длинная точная последовательность гомологий). Пусть имеется точная последовательность комплексов $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$.

Существует длинная точная последовательность гомологических групп

$$\dots \longrightarrow H' \longrightarrow H \longrightarrow H'' \longrightarrow H'[-1] \longrightarrow H[-1] \longrightarrow \dots$$

где связующий морфизм δ будет построен в доказательстве.

Более того, это всё функториально: если есть другая короткая точная последовательность, и морфизм между ними, то по отношению к ним найдётся естественный морфизм полученных длинных точных последовательностей гомологий.

Доказательство. Сначала строим δ .

Для $z \in Z_n''$, обозначим за $[z]$ класс z в H_n'' .

$$\begin{array}{ccccccc} 0 & \longrightarrow & A'_n & \longrightarrow & A_n & \xrightarrow{\pi} & A''_n \longrightarrow 0 \\ & & \downarrow d' & & \downarrow d & & \downarrow d'' \\ 0 & \longrightarrow & A'_{n-1} & \xrightarrow{i} & A_{n-1} & \longrightarrow & A''_{n-1} \longrightarrow 0 \end{array}$$

Положим $\delta([z]) := [i^{-1}(d(\pi^{-1}(z)))]$, где $\pi^{-1}(z)$ — произвольный прообраз (он есть, так как π сюръективно).

Дальше надо проверить, что определение корректно, и последовательность точна. Это типичный диаграммный поиск, который невозможно записывать, и его несложно воспроизвести самостоятельно. \square

Лекция III

4 марта 2024 г.

Теперь приведём другое доказательство существования длинной точной последовательности гомологий, опирающееся на лемму о змее.

Лемма 1.3.1 (О змее). Пусть даны два комплекса $A' \rightarrow A \rightarrow A'' \rightarrow 0$ и $0 \rightarrow B' \rightarrow B \rightarrow B''$, и морфизм между ними. Тогда имеется длинная точная последовательность из пунктирных стрелок.

Короткие стрелки получены из действия соответственных функторов (ядра и коядра), а связующий гомоморфизм определён δ определён в доказательстве, и естественен (функториален).

$$\begin{array}{ccccccc} \text{Ker } \phi' & \dashrightarrow & \text{Ker } \phi & \dashrightarrow & \text{Ker } \phi'' & & \\ \downarrow \ker \phi' & & \downarrow \ker \phi & & \downarrow \ker \phi'' & & \\ A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ \downarrow \phi & & \downarrow \phi & & \downarrow \phi'' & & \delta \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' \\ \downarrow \text{coker } \phi' & & \downarrow \text{coker } \phi & & \downarrow \text{coker } \phi'' & & \\ & \dashrightarrow & \text{CoKer } \phi' & \dashrightarrow & \text{CoKer } \phi & \dashrightarrow & \text{CoKer } \phi'' \end{array}$$

Доказательство. Диаграммный поиск. \square

Теорема 1.3.2 (Длинная точная последовательность гомологий на бис). Пусть имеется точная последовательность комплексов $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$.

Существует длинная точная последовательность гомологических групп

$$\dots \longrightarrow H' \longrightarrow H \longrightarrow H'' \longrightarrow H'[-1] \longrightarrow H[-1] \longrightarrow \dots$$

где связующий морфизм δ будет построен в доказательстве.

Более того, это всё функториально.

Доказательство. Длинная точная последовательность комплексов означает наличие следующей коммутативной диаграммы (где строки точны, и столбцы — комплексы)

$$\begin{array}{ccccccc} & \vdots & & \vdots & & \vdots & \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & A'_n & \longrightarrow & A_n & \longrightarrow & A''_n \longrightarrow 0 \\ & & \downarrow d'_n & & \downarrow d_n & & \downarrow d''_n \\ 0 & \longrightarrow & A'_{n-1} & \longrightarrow & A_{n-1} & \longrightarrow & A''_{n-1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & \vdots & & \vdots & & \vdots \end{array}$$

Пусть циклы, границы и гомологии в комплексе A обозначаются $Z_\bullet, B_\bullet, H_\bullet$ соответственно, в $A' - Z'_\bullet, B'_\bullet, H'_\bullet$, в $A'' - Z''_\bullet, B''_\bullet, H''_\bullet$. Из коммутативности диаграммы B'_n вправо уходит в B_n , а B_n , в свою очередь — в B''_n .

Чтобы воспользоваться леммой о змее, построим следующую диаграмму, взяв коядро верхней строки, ядро — нижней, и дорисовав сверху — ядра вертикальных стрелок, снизу — коядра.

$$\begin{array}{ccccccc} & H'_n & & H_n & & H''_n & \\ & \downarrow & & \downarrow & & \downarrow & \\ & A'_n/B'_n & \longrightarrow & A_n/B_n & \longrightarrow & A''_n/B''_n & \longrightarrow 0 \\ & \downarrow \tilde{d}'_n & & \downarrow \tilde{d}_n & & \downarrow \tilde{d}''_n & \\ 0 & \longrightarrow & Z'_{n-1} & \longrightarrow & Z_{n-1} & \longrightarrow & Z''_{n-1} \\ & & \downarrow & & \downarrow & & \downarrow \\ & & H'_{n-1} & & H_{n-1} & & H''_{n-1} \end{array}$$

Обоснуем, каким образом получилась такая диаграмма. По определению $d_n(B_n) = \{0\}$, поэтому $A_n \xrightarrow{d_n} A_{n-1}$ пропускается через фактор, и получается отображение $\tilde{d}_n : A_n/B_n \rightarrow A_{n-1}$. Так как A — комплекс, то $\tilde{d}_n(A_n/B_n) \subset Z_{n-1}$, можно сузить codomain, получая \tilde{d}_n . По определению $H_n = Z_n/B_n$, поэтому действительно $H_n = \text{Ker}(d_n)$. В свою очередь, $H_{n-1} = Z_{n-1}/B_{n-1}$, и это действительно $\text{CoKer}(d_n)$.

Отображение $A_n \rightarrow A''_n$ было эпиморфизмом, после взятия коядра эпиморфизмом оно и осталось. Двойственно, $A'_{n-1} \rightarrow A_{n-1}$ было мономорфизмом, мономорфизмом оно и осталось.

Применяя лемму о змее, получаем утверждение теоремы. \square

1.4 Функторы между абелевыми категориями

Пусть \mathcal{A}, \mathcal{B} — абелевы категории.

Определение 1.4.1 (Аддитивный функтор $\mathcal{F} : \mathcal{A} \rightarrow \mathcal{B}$). Такой функтор, что $\forall \alpha, \beta \in \text{Mor}(\mathcal{A}) : \mathcal{F}(\alpha + \beta) = \mathcal{F}(\alpha) + \mathcal{F}(\beta)$ всегда, когда определено.

Рассмотрим произвольную короткую точную последовательность $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ в \mathcal{A} . Подействовав на неё функтором \mathcal{F} , мы получим последовательность $0 \rightarrow \mathcal{F}(A') \rightarrow \mathcal{F}(A) \rightarrow \mathcal{F}(A'') \rightarrow 0$. Точность, вообще говоря, пропадёт, но если \mathcal{F} сохраняет точность в каком-то члене для всех таких коротких точных последовательностей, то функтор \mathcal{F} имеет соответствующее название:

1. Если всегда имеется точность в члене $\mathcal{F}(A)$, то \mathcal{F} — *полуточный функтор*.
2. Если всегда имеется точность в членах $\mathcal{F}(A')$ и $\mathcal{F}(A)$, то \mathcal{F} — *точный слева функтор*.
3. Если всегда имеется точность в членах $\mathcal{F}(A)$ и $\mathcal{F}(A'')$, то \mathcal{F} — *точный справа функтор*.
4. Если всякая короткая точная последовательность переходит в короткую точную последовательность, то \mathcal{F} — *точный функтор*.

Лемма 1.4.1. Пусть \mathcal{F} — аддитивный функтор. Следующие условия эквивалентны:

1. \mathcal{F} точен справа.
2. \mathcal{F} сохраняет нуль и коядра: $\mathcal{F}(0) = 0, \mathcal{F}(\text{coker}(\phi)) = \text{coker}(\mathcal{F}(\phi))$.
3. \mathcal{F} сохраняет конечные копределы.

Доказательство.

- (3) \Rightarrow (2) Коядро — конечный копредел, поэтому очевидно.
- (2) \Rightarrow (3) В свою очередь, копроизведение в абелевой категории — бипроизведение, а это «внутренний объект», поэтому всякий аддитивный функтор сохраняет его.
- (2) \Rightarrow (1) Короткая точная последовательность $A' \xrightarrow{\phi} A \xrightarrow{\psi} A'' \rightarrow 0$ характеризуется свойствами $\psi = \text{coker } \phi, 0 = \text{coker } \psi$.
- (1) \Rightarrow (2) Рассмотрим произвольный $\phi : A' \rightarrow A$. У него есть эпи-моно разложение $\phi = \mu \varepsilon$ (μ — моно, ε — эпи), и $\text{coker}(\mu \varepsilon) = \text{coker}(\mu)$, так как ε — эпиморфизм. Значит, без потери общности ϕ — мономорфизм.

Тогда последовательность $0 \rightarrow A' \xrightarrow{\phi} A \xrightarrow{\text{coker } \phi} \text{CoKer } \phi \rightarrow 0$ точна, и так как \mathcal{F} — точен справа, то $\mathcal{F}(\text{coker } \phi) = \text{coker}(\mathcal{F}(\phi))$.

Также точный справа функтор сохраняет нуль: $0 \rightarrow A \xrightarrow{\text{id}} A \rightarrow 0 \rightarrow 0$ переходит в $\mathcal{F}(A) \xrightarrow{\text{id}} \mathcal{F}(A) \rightarrow \mathcal{F}(0) \rightarrow 0$. \square

Следствие 1.4.1. Левый сопряжённый функтор точен справа.

Доказательство. Он сохраняет копределы. \square

Копредел (который является левым сопряжённым к диагональному Δ) сохраняет копределы, значит, точен справа. Другими словами, копределы коммутируют.

К сожалению, в лемме о змее это не помогает в доказательстве того, что последовательность точна в члене $\text{Ker } \phi$, так как нет точной последовательности $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$.

При доказательстве существования длинной точной последовательности гомологий на бис, мы использовали, что коядро точно справа, ядро — точно слева.

Лекция IV

11 марта 2024 г.

Факт 1.4.1. Если точный справа функтор сохраняет мономорфизмы, то функтор точен. Двойственно, точный слева функтор, сохраняющий эпиморфизмы, точен.

1.5 Резольвенты

Пусть \mathcal{A} — абелева категория, $P \in \mathcal{A}$.

Определение 1.5.1 (Объект P проективен). $\forall \phi : A \rightarrow B: \phi \text{ — эпи} \Rightarrow \forall \psi : P \rightarrow B: \exists \theta : P \rightarrow A$, причём диаграмма коммутует. При этом θ должно найтись какое-то, не факт, что оно единственно.

$$\begin{array}{ccc} & P & \\ \swarrow \exists \theta & \downarrow \forall \psi & \\ A & \xrightarrow{\forall \phi} B & \longrightarrow 0 \end{array}$$

Факт 1.5.1. В $\mathcal{S}et$ все множества — проективные объекты.

Теорема 1.5.1. Пусть $\mathcal{A} = R\text{-mod}$. Модуль P проективен $\iff P$ является прямым слагаемым свободного модуля.

Доказательство.

1. Свободный модуль проективен: пусть $\{p_\alpha\}$ — базис P . Определим $\theta(p_\alpha) = \psi(\phi^{-1}(p_\alpha))$, где прообраз выбран произвольно, и продолжим по линейности.
2. Прямое слагаемое проективного модуля проективно. Рассмотрим каноническое вложение $M \hookrightarrow M \oplus N$, где $M \oplus N$ — проективен.

$$\begin{array}{ccc} & M & \longrightarrow M \oplus N \\ & \downarrow \psi & \swarrow \text{---} \\ A & \longrightarrow B & \longrightarrow 0 \end{array}$$

Определим $M \oplus N \rightarrow B, (m, n) \mapsto \psi(m)$. Так как $M \oplus N$ проективен, то найдётся $M \oplus N \rightarrow A$, и композиция $M \rightarrow M \oplus N \rightarrow A$ подходит в качестве морфизма, который должен найтись из определения проективного модуля.

3. Пусть P проективен. Возьмём свободный модуль F , сюръективно накрывающий P (например, подойдёт свободный модуль на всех элементах P , но на практике, конечно, удобно брать модуль поменьше).

$$\begin{array}{ccc} & P & \\ \swarrow \exists & \downarrow \text{id} & \\ F & \xrightarrow{\pi} P & \end{array}$$

Так как модуль проективен, то найдётся пунктирная стрелка. Значит, $F \cong P \oplus \text{Ker } \pi$ ($\forall f \in F : \pi^{-1}(f) = P(f) + \text{Ker } \pi$). \square

Примеры.

- Пусть $R = \mathbb{Z}/6\mathbb{Z}$. Тогда $\mathbb{Z}/6\mathbb{Z}$ является R -модулем, но $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, значит, модули $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$ все проективны.
- Можно предъявить проективный модуль, исходя из топологического факта о том, что шар нельзя причисать.

Определение 1.5.2 (Проективная резольвента модуля M). Ациклический комплекс вида $\cdots \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_0 \rightarrow M \rightarrow 0$, где P_i — проективные модули.

В будущем докажем, что любые две проективные резольвенты гомотопически эквивалентны.

Определение 1.5.3 (В категории \mathcal{A} достаточно много проективных объектов). $\forall A \in \mathcal{A}$ найдётся проективный объект $P \in \mathcal{A}$ вместе с эпиморфизмом $P \twoheadrightarrow A$.

Если в нашей категории \mathcal{A} достаточно много проективных объектов, то у всякого модуля M найдётся резольвента — надо просто подряд накрывать возникающие ядра.

Лекция V

18 марта 2024 г.

1.6 Резольвенты. Левый производный функтор

Зафиксируем некоторый аддитивный функтор $\mathcal{F} : \mathcal{A} \rightarrow \mathcal{B}$, который обычно будет точен справа. Пусть у объекта $A \in \mathcal{A}$ имеется проективная резольвента, которую я выделил стрелками \rightsquigarrow .

$$\begin{array}{ccccccc} \cdots & \rightsquigarrow & P_1 & \rightsquigarrow & P_0 & \longrightarrow & 0 \\ & & & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & A & \rightsquigarrow & 0 \end{array}$$

Иными словами, проективная резольвента — это некоторый морфизм комплексов P и A_\bullet . Под комплексом A_\bullet подразумевается такой комплекс, в котором в нулевой градуировке сидит A , а в остальных — нули (следовательно, все дифференциалы — тоже нули).

Раз \mathcal{F} точен справа, то он сохраняет нуль. Применим \mathcal{F} к верхней строчке. Тогда получится комплекс вида

$$\cdots \longrightarrow \mathcal{F}(P_1) \longrightarrow \mathcal{F}(P_0) \longrightarrow 0$$

Чуть ниже мы определим $L_n \mathcal{F}(A) := H_n \mathcal{F}(P)$ — левый производный функтор, измеряющий неточность \mathcal{F} — но пока, например, неясна корректность (независимость от резольвенты) такого определения.

Теорема 1.6.1. Пусть P_i проективные, сверху комплекс (и ноль в верхней строчке вообще-то неважен), снизу — точный комплекс.

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow f \\ \cdots & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & B \longrightarrow 0 \end{array}$$

Тогда найдутся пунктирные стрелки, и они определены с точностью до гомотопии.

Доказательство.

- Сначала построим $f_i : P_i \rightarrow Q_i$.
 $Q_0 \rightarrow B$ сюръективно, значит, найдётся f_0 , такое, что квадрат коммутативен.
- Далее по индукции: пусть построены f_0, \dots, f_n .

$$\begin{array}{ccccc} P_{n+1} & \longrightarrow & P_n & \longrightarrow & P_{n-1} \\ \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} \\ Q_{n+1} & \longrightarrow & Q_n & \xrightarrow{d_{n-1}^Q} & Q_{n-1} \end{array}$$

Хочется заполнить стрелку $P_{n+1} \rightarrow Q_{n+1}$, воспользовавшись проективностью P_{n+1} . Для этого надо найти сюръективное $Q_{n+1} \rightarrow ?$. Так как внизу — точная последовательность, то $Q_{n+1} \rightarrow \text{Ker}(d_{n-1}^Q)$ подойдёт: оно сюръективно, так как $P_{n+1} \rightarrow P_{n-1}$ нулевой,

а квадрат $\begin{array}{ccc} P_n & \longrightarrow & P_{n-1} \\ \downarrow & & \downarrow \\ Q_n & \longrightarrow & Q_{n-1} \end{array}$ коммутативен. Тем самым, по определению проективного модуля $\exists f_{n+1}$.

- Теперь пусть имеются два морфизма комплексов, продолжающих f , f_i и g_i .

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A \\ & & f_1 \downarrow & \downarrow g_1 & f_0 \downarrow & \downarrow g_0 & \downarrow f \\ \cdots & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & B \longrightarrow 0 \end{array}$$

Распишем разность: пусть $h_i := f_i - g_i$. Понятно, что $A \rightarrow Q_0$ надо взять нулевым.

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A \longrightarrow 0 \\ & & \downarrow h_1 & \swarrow s_0 & \downarrow h_0 & \swarrow 0 & \downarrow 0 \\ \cdots & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & B \longrightarrow 0 \end{array}$$

s_0 строится по основному свойству проективного модуля P_0 : ведь $h_0(P_0) \subset \text{Ker}(d_{-1}^Q) = \text{Im } d_0^Q$

- Далее индукция. Пусть построены s_0, \dots, s_{n-1} , строим s_n .

$$\begin{array}{ccccccc} & & P_n & \xrightarrow{d_{n-1}^P} & P_{n-1} & \xrightarrow{d_{n-2}^P} & P_{n-2} \\ & \swarrow s_n & \downarrow h_n & \swarrow s_{n-1} & \downarrow h_{n-1} & \swarrow s_{n-2} & \\ Q_{n+1} & \xrightarrow{d_n^Q} & Q_n & \xrightarrow{d_{n-1}^Q} & Q_{n-1} & & \end{array}$$

Хочется, чтобы выполнялось $h_n = d_n^Q s_n + s_{n-1} d_{n-1}^P$, эквивалентно $d_n^Q s_n = h_n - s_{n-1} d_{n-1}^P$.

Надо проверить, что образ правой части лежит в $\text{Im}(d_n^Q)$, то есть $\text{Ker}(d_{n-1}^Q)$. Применим d_{n-1}^Q . Получим

$$d_{n-1}^Q h_n - d_{n-1}^Q s_{n-1} d_{n-1}^P = h_{n-1} d_{n-1}^P - (h_{n-1} - s_{n-2} d_{n-2}^P) d_{n-1}^P = 0$$

Тем самым, s_n действительно найдётся согласно свойству проективного модуля.

□

Следствие 1.6.1. Любые две проективные резольвенты одного и того же объекта гомотопически эквивалентны.

$$\begin{array}{ccc} P & \longrightarrow & A_\bullet \\ g \uparrow & \downarrow f & \downarrow \text{id} \\ Q & \longrightarrow & A_\bullet \end{array} \quad \begin{array}{ccc} P & \longrightarrow & A_\bullet \\ \text{id} \downarrow & \downarrow fg & \downarrow \text{id} \\ P & \longrightarrow & A_\bullet \end{array}$$

Строим по только что доказанной теореме f, g , по теореме $fg \simeq \text{id}_Q$ и $gf \simeq \text{id}_Q$.

Таким образом, определение левого производного функтора L_n корректно.

С некоторой точки зрения «правильно» рассматривать категорию комплексов с точностью до гомотопической эквивалентности, назовём её $\mathcal{H}\mathcal{C}ompr(\mathcal{A})$: там объекты — $\text{Obj } \mathcal{A}$, а группа морфизмов $\text{Mor}_{\mathcal{H}\mathcal{C}ompr(\mathcal{A})}(P, Q) = \text{Mor}(\mathcal{C}ompr(\mathcal{A}))/\text{Ho}(P, Q)$, где $\text{Ho}(P, Q)$ — группа морфизмов, гомотопных 0.

Примеры (Что такое L_0 от точного справа функтора).

- Предположим, что \mathcal{F} точен справа. Тогда

$$\mathcal{F}(P_1) \longrightarrow \mathcal{F}(P_0) \longrightarrow \mathcal{F}(A) \longrightarrow 0$$

точна. $L_0 \mathcal{F}(A) = H_0(\mathcal{F}(P)) = \text{CoKer}(\mathcal{F}(P_1) \rightarrow \mathcal{F}(P_0))$. Если функтор точен справа, то $\text{CoKer}(\mathcal{F}(P_1) \rightarrow \mathcal{F}(P_0)) = \mathcal{F}(A)$.

Тем самым, $L_0 \mathcal{F} = \mathcal{F}$.

- Обратно, если $L_0\mathcal{F} = \mathcal{F}$, то \mathcal{F} сохраняет коядра, значит, точен справа. (По-хорошему, надо ещё проверить, что $L_0\mathcal{F}$ действует на морфизмах так же, но это банально).

Следствие 1.6.2. Если P_A, P_B — проективные резольвенты A, B соответственно, и $f : A \rightarrow B$, то $\exists \tilde{f} : P_A \rightarrow P_B$, делающий диаграмму коммутативной. Он определён однозначно с точностью до гомотопии.

$$\begin{array}{ccc} P_A & \longrightarrow & A_\bullet \\ \tilde{f} \downarrow & & f \downarrow \\ P_B & \longrightarrow & B_\bullet \end{array}$$

Здесь A_\bullet — комплекс, где A сосредоточен в нулевом члене.

Таким образом, морфизму f объектов из \mathcal{A} сопоставляется морфизм резольвент \tilde{f} , а он, в свою очередь, индуцирует морфизм гомологий $H_n(P_A) \rightarrow H_n(P_B)$. Значит, конструкция L функториальна.

1.6.1 Длинная точная последовательность левых производных функторов

Зафиксируем некоторый функтор \mathcal{F} . Далее мы исследуем $L_n\mathcal{F}$, для упрощения записи будем писать $L_n := L_n\mathcal{F}$.

Пусть имеется короткая точная последовательность $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ в \mathcal{A} . Построим длинную точную последовательность производных функторов. Это так говорится? Скорее всё-таки их значений на A, B, C

$$\cdots \rightarrow L_1(A) \rightarrow L_1(B) \rightarrow L_1(C) \rightarrow L_0(A) \rightarrow L_0(B) \rightarrow L_0(C) \rightarrow \cdots$$

Для получения такой штуки было бы неплохо заполучить точную последовательность резольвент $P_A \rightarrow P_B \rightarrow P_C$, причём не абы какую, а сохраняющую свою точность под действием любого аддитивного функтора. Оказывается, это сделать несложно, и в этом нам поможет лемма о подковке.

Лемма 1.6.1 (О подковке). Пусть P — проективный модуль, все строки и столбцы (состоящие из чёрных сплошных стрелок) точны.

$$\begin{array}{ccccccc} Q & \xrightarrow{\quad i \quad} & Q \oplus P & \xrightarrow{\quad \pi \quad} & P & & \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 & & 0 & & 0 & & \end{array}$$

Утверждается, что диаграмму можно достроить до коммутативной, добавив зелёные пунктирные стрелки. Новые строки и столбцы также станут точны.

Доказательство. Так как P — проективен, а g — эпи, то найдётся сечение s такое, что $gs = h_C$.

$$\begin{array}{ccccccc} Q & \xrightarrow{\quad i \quad} & Q \oplus P & \xrightarrow{\quad \pi \quad} & P & & \\ \downarrow h_A & & \downarrow h_B & & \downarrow h_C & & \\ 0 \longrightarrow & A & \xrightarrow{\quad f \quad} & B & \xrightarrow{\quad g \quad} & C & \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 & & 0 & & 0 & & \end{array}$$

Определим стрелку h_B исходя из того, что квадраты должны в итоге получиться коммутативными. Из коммутативности левого квадрата $h_B(u, 0) = f(h_A(u))$. Из коммутативности правого треугольника $h_B(0, v) = h_C(v) = gs(v)$. Тем самым, подойдёт $h_B(u, v) := f(h_A(u)) + s(v)$.

При таком определении правый квадрат будет коммутативен: $g(s(v)) = h_C(\pi(u, v)) \stackrel{?}{=} g(h_B(u, v)) = g(s(v))$, так как $gf = 0$.

Также несложно убедиться, что построенный морфизм h_B — эпи (видимо, диаграммный поиск). \square

Теорема 1.6.2. Для короткой точной последовательности $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ существует точная последовательность резольвент $0 \rightarrow P_A \rightarrow P_B \rightarrow P_C \rightarrow 0$, точность которой сохраняется под действием любого аддитивного функтора.

Доказательство. Возьмём произвольные резольвенты P_A, P_C . Резольвенту P_B будем строить пошагово, по индукции. $(P_B)_0 := (P_A)_0 \oplus (P_C)_0$ строится прямым применением леммы о подкове.

Далее необходимо провести индукционный переход.

$$\begin{array}{ccccccc}
 (P_A)_{n+1} & \xrightarrow{\text{---}i\text{---}} & (P_A)_{n+1} \oplus (P_C)_{n+1} & \xrightarrow{\text{---}\pi\text{---}} & (P_C)_{n+1} & & \\
 \downarrow & & \downarrow d_n^B & & \downarrow & & \\
 0 \longrightarrow & \text{Ker}(d_{n-1}^A) & \longrightarrow & \text{Ker}(d_{n-1}^B) & \longrightarrow & \text{Ker}(d_{n-1}^C) & \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \longrightarrow & (P_A)_n & \longrightarrow & (P_B)_n & \longrightarrow & (P_C)_n & \longrightarrow 0 \\
 & \downarrow d_{n-1}^A & & \downarrow d_{n-1}^B & & \downarrow d_{n-1}^C & \\
 0 \longrightarrow & \text{Ker}(d_{n-2}^A) & \longrightarrow & \text{Ker}(d_{n-2}^B) & \longrightarrow & \text{Ker}(d_{n-2}^C) & \longrightarrow 0
 \end{array}$$

Вычленим некоторый кусочек диаграммы, и попробуем применить лемму о подкове для получения d_n^B . Для этого необходимо потребовать от стрелки $\text{Ker}(d_{n-1}^B) \rightarrow \text{Ker}(d_{n-1}^C)$, чтобы она была эпиморфизмом.

Докажем последнее по индукции: короткая последовательность ядер $0 \rightarrow \text{Ker}(d_n^A) \rightarrow \text{Ker}(d_n^B) \rightarrow \text{Ker}(d_n^C) \rightarrow 0$ точна (так как ядро точно слева, то точность в остальных членах не вызывает сомнений, надо лишь проверить эпиморфность). В качестве базы здесь удобно применить лемму о змее:

$$\begin{array}{ccccccc}
 0 \longrightarrow & \text{Ker}(d_{-1}^A) & \longrightarrow & \text{Ker}(d_{-1}^B) & \longrightarrow & \text{Ker}(d_{-1}^C) & \xrightarrow{\text{---}} \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \longrightarrow & P_A & \longrightarrow & P_B & \longrightarrow & P_C & \longrightarrow 0 \\
 & \downarrow d_{-1}^A & & \downarrow d_{-1}^B & & \downarrow d_{-1}^C & \\
 0 \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
 \end{array}$$

А индукционный переход я не знаю, ну, можно просто убедиться, используя определение d_n^B из леммы о подкове.

Тем самым, так как прямая сумма проективных проективна, то $(P_A)_{n+1} \oplus (P_C)_{n+1} \twoheadrightarrow \text{Ker}(d_{n-1}^B)$, и определение резольвенты B по индукции корректно.

Точность $0 \rightarrow P_A \rightarrow P_B \rightarrow P_C$ под действием всякого аддитивного функтора, конечно, сохраняется, так как $(P_B)_n = (P_A)_n \oplus (P_C)_n$, а аддитивные функторы сохраняют бипроизведение. \square

Следствие 1.6.3 (Длинная точная последовательность производных функторов). Для короткой точной последовательности $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ имеет место длинная точная последовательность

$$\cdots \rightarrow L_1(A) \rightarrow L_1(B) \rightarrow L_1(C) \rightarrow L_0(A) \rightarrow L_0(B) \rightarrow L_0(C) \rightarrow \cdots$$

Доказательство. Из (теорема 1.6.2) найдётся точная последовательность проективных резольвент $0 \rightarrow P_A \rightarrow P_B \rightarrow P_C \rightarrow 0$. Применяя \mathcal{F} , получаем точную последовательность $0 \rightarrow \mathcal{F}(P_A) \rightarrow \mathcal{F}(P_B) \rightarrow \mathcal{F}(P_C) \rightarrow 0$.

Возьмём у $\mathcal{F}(P_A), \mathcal{F}(P_B), \mathcal{F}(P_C)$ гомологии. Составленная из них длинная точная гомологическая последовательность как раз и сконструирует искомую длинную точную последовательность левых производных функторов. \square

Замечание. Если \mathcal{F} точен справа, то длинная точная последовательность производных функторов обрывается эпиморфизмом: $L_0(B) \rightarrow L_0(C) \rightarrow 0$.

Лекция VI

25 марта 2024 г.

Рассмотрим формальное обобщение производных функторов.

Пусть имеется семейство $\{\mathcal{F}_i\}_{i \in \mathbb{N}}$ функторов $\mathcal{F}_i : \mathcal{A} \rightarrow \mathcal{A}'$.

Определение 1.6.1 ((Левая) связанная последовательность функторов). Такая последовательность функторов $\{\mathcal{F}_i\}_{i \in \mathbb{N}}$, что для любой точной последовательности $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ существует функториальная длинная точная последовательность

$$\cdots \rightarrow \mathcal{F}_1(A) \rightarrow \mathcal{F}_1(B) \rightarrow \mathcal{F}_1(C) \rightarrow \mathcal{F}_0(A) \rightarrow \mathcal{F}_0(B) \rightarrow \mathcal{F}_0(C)$$

Пример. Последовательность $\{L_i \mathcal{F}\}_{i \in \mathbb{N}}$ — связанная последовательность функторов.

Заметим, что $\forall i > 0 : L_i \mathcal{F}(P) = 0$, если P проективен. Это очевидным образом следует из существования резольвенты $0 \rightarrow P \rightarrow P \rightarrow 0$. Если \mathcal{F} точен справа (а мы это предполагаем), то он сохраняет ноль. Тогда $L_n \mathcal{F}$ — гомологии $\cdots \rightarrow 0 \rightarrow 0 \rightarrow \mathcal{F}(P) \rightarrow 0$, которые в нулевом члене — $\mathcal{F}(P)$, а в остальных — нулевые.

Оказывается, этого условия достаточно, чтобы определить связанную последовательность по нулевому элементу:

Теорема 1.6.3. Пусть $\{\mathcal{F}_i\}, \{\mathcal{G}_i\}$ — две связанные последовательности функторов, такие, что имеется естественный изоморфизм $\mathcal{F}_0 \cong \mathcal{G}_0$, и для любого проективного P : $\forall i > 0 : \mathcal{F}_i(P) = \mathcal{G}_i(P) = 0$.

Также предположим, что в \mathcal{A} достаточно много проективных объектов.

Тогда $\forall i : \mathcal{F}_i \cong \mathcal{G}_i$ — естественный изоморфизм.

Доказательство. Пусть $A \in \mathcal{A}$. Накроем A проективным, возьмём ядро, получим точную последовательность

$$0 \rightarrow M \rightarrow P \rightarrow A \rightarrow 0$$

Так как последовательности функторов — связаны — то имеется длинная точная последовательность:

$$\begin{array}{ccccccc} 0 = \mathcal{F}_1(P) & \longrightarrow & \mathcal{F}_1(A) & \longrightarrow & \mathcal{F}_0(M) & \longrightarrow & \mathcal{F}_0(P) \\ & & \updownarrow & & \updownarrow & & \updownarrow \\ 0 = \mathcal{G}_1(P) & \longrightarrow & \mathcal{G}_1(A) & \longrightarrow & \mathcal{G}_0(M) & \longrightarrow & \mathcal{G}_0(P) \end{array}$$

Значит, имеется естественный изоморфизм ядер, $\mathcal{F}_1(A) \cong \mathcal{G}_1(A)$, тем самым, $\mathcal{F}_1 \cong \mathcal{G}_1$ (естественность — упражнение).

Теперь займёмся индукционным переходом:

$$\begin{array}{ccccccc} 0 = \mathcal{F}_i(P) & \longrightarrow & \mathcal{F}_i(A) & \longrightarrow & \mathcal{F}_{i-1}(M) & \longrightarrow & \mathcal{F}_{i-1}(P) = 0 \\ & & \updownarrow & & \updownarrow & & \\ 0 = \mathcal{G}_i(P) & \longrightarrow & \mathcal{G}_i(A) & \longrightarrow & \mathcal{G}_{i-1}(M) & \longrightarrow & \mathcal{G}_{i-1}(P) = 0 \end{array}$$

Зажав $\mathcal{F}_i(A)$ и $\mathcal{F}_{i-1}(M)$ между двумя нулями, мы доказали, что все четыре ненулевых объекта изоморфны (естественность, опять же, доказывается несложно). \square

Следствие 1.6.4. Пусть \mathcal{F} точен справа (например $\mathcal{F} = _ \otimes M$, где M — фиксированный модуль). Пусть $\mathcal{F}_0 \cong \mathcal{F}$, где $\{\mathcal{F}_i\}$ — связанная последовательность функторов, такая, что для любого проективного $P : \mathcal{F}(P) = 0$.

По-прежнему предполагаем, что в \mathcal{A} достаточно много проективных объектов.

Тогда $\forall i \in \mathbb{N} : \mathcal{F}_i \cong L_i \mathcal{F}$.

1.7 Производные функторы для \otimes

Пусть R — необязательно коммутативное кольцо с единицей, $M \in \text{mod-}R, N \in R\text{-mod}$, напомним, что тогда $M \otimes_R N \in \mathcal{A}$.

Изучим производные функторы тензорного произведения (функтор тензорного произведения точен справа, так как он — левый сопряжённый к Hom). Обозначим $\text{LTor}_i(M, _) \stackrel{\text{def}}{=} L_i(M \otimes _)$, $\text{RTor}_i(_, N) \stackrel{\text{def}}{=} L_i(_ \otimes N)$.

Примеры.

- Изучим $\text{Tor}_1(M, R/aR)$, где R — коммутативная область целостности. Для R/aR несложно написать проективную резольвенту: $0 \rightarrow R \xrightarrow{a} R \rightarrow R/aR \rightarrow 0$ ($a(m) = am$).

Тензорно домножая на M , мы получаем $0 \rightarrow M \xrightarrow{m \otimes r \mapsto m \otimes ar} M \rightarrow M \otimes R/aR \rightarrow 0$. Так как кольцо коммутативное, то тензорное произведение — $\text{mod-}R$, поэтому $m \otimes r \mapsto m \otimes ar$ — тоже просто отображение умножения на a .

Так как естественно $M \otimes R/aR \cong M/aM \otimes R \cong M/aM$, то гомологии в среднем члене — нуль, а в левом члене — a -*кручение* в M , то есть $\{x \in M \mid ax = 0\}$.

Теорема 1.7.1. Имеет место естественный изоморфизм: $\forall i : \text{LTor}_i \cong \text{RTor}_i$.

Идея доказательства.

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \downarrow & & \downarrow & & \downarrow \\
 \cdots & \longrightarrow & P_1 \otimes Q_1 & \longrightarrow & P_0 \otimes Q_1 & \longrightarrow & M \otimes Q_1 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 \cdots & \longrightarrow & P_1 \otimes Q_0 & \longrightarrow & P_0 \otimes Q_0 & \longrightarrow & M \otimes Q_0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 \cdots & \longrightarrow & P_1 \otimes N & \longrightarrow & P_0 \otimes N & \longrightarrow & M \otimes N \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
 \end{array}$$

Домножение на свободный объект — точный справа функтор — из дистрибутивности тензорного произведения. Домножение на проективный объект — точный справа функтор — опять же из дистрибутивности.

Все строки точны, кроме нижней, и все столбцы точны, кроме правого, в которых мы и хотим посчитать гомологии, и доказать, что они равны.

Заведём тотальный комплекс $\text{Tot}(M, N)_n := \bigoplus_{i=0}^n P_i \otimes Q_{n-i}$, и теперь надо определить дифференциал D . Необходимо, чтобы выполнялось требование $D^2 = 0$, поэтому абы какой не подойдёт.

Пусть $d_p : P \rightarrow P_{p-1}$, $d_q : Q_q \rightarrow Q_{q-1}$ — дифференциалы резольвент, определим

$$\begin{aligned}
 D_{p,q} : P_p \otimes Q_q &\rightarrow \text{Tot}(M, N)_{p+q-1} \\
 (x \otimes y) &\mapsto d_p(x) \otimes y + (-1)^p x \otimes d_q(y)
 \end{aligned}$$

Теперь полный дифференциал $D_n = \bigoplus_{p+q=n} D_{p,q} : \text{Tot}(M, N)_{p+q} \rightarrow \text{Tot}_{p+q-1}$.

Упражнение 1.7.1. $D_{n-1} \cdot D_n = 0$.

Осталось показать, что гомологии нижней строки, как и гомологии правого столбца, совпадают с гомологиями тотального комплекса. \square

1.8 Производные функторы для Hom

Теперь разберёмся с функторами Hom — эти функторы являются правыми сопряжёнными к \otimes , поэтому точны слева.

Конкретнее, имеются ковариантный $\text{Hom}(M, _)$, и контравариантный $\text{Hom}(_, N)$.

Для изучения точных слева функторов будем строить последовательность правых сопряжённых функторов.

Определение 1.8.1 (Инъективный модуль Q). Такой модуль Q , что для любой инъекции $A \hookrightarrow B$, и для любого морфизма $A \rightarrow Q$, существует морфизм $B \rightarrow Q$ такой, что диаграмма коммутативна:

$$\begin{array}{ccc} A & \xrightarrow{\quad} & B \\ \downarrow & \swarrow \exists & \\ Q & & \end{array}$$

Интересный факт. Инъективный модуль — делимый модуль, то есть $\forall r \in R \setminus \{0\}, q \in M : \exists x \in M : rx = q$.

В одну сторону доказательство очевидно — в качестве A надо взять кольцо R , а в качестве B — поле частных R .

В категории, где *достаточно много инъективных объектов*, двойственно проективной, строится инъективная резольвента, в которой коядро предыдущего морфизма вкладывается в следующий инъективный модуль:

$$0 \rightarrow N \rightarrow Q_0 \rightarrow Q_1 \rightarrow Q_2 \rightarrow \dots$$

Далее аналогично определяются правые производные функторы, в частности, имеется комплекс

$$0 \rightarrow \text{Hom}(M, Q_0) \rightarrow \text{Hom}(M, Q_1) \rightarrow \dots$$

Гомологии такого комплекса обозначают $\text{Ext}^i(M, N)$.

Построив проективную резольвенту для $M: \dots \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$. Применяя к этой последовательности контравариантный Hom, получаем $0 \rightarrow \text{Hom}(P_0, N) \rightarrow \text{Hom}(P_1, N) \rightarrow \dots$. Гомологии этого комплекса обозначают $\text{Ext}^i(M, N)$ (это уже другой Ext, но они, как и Tor, естественно изоморфны, доказательство абсолютно аналогично)

Название Ext происходит от extensions, элементы Ext^1 находятся в биекции с классами коротких точных последовательностей $0 \rightarrow M \rightarrow ? \rightarrow N \rightarrow 0$. В качестве среднего члена всегда подойдёт $M \oplus N$, но, может быть, и ещё что-то, и за это отвечает Ext.

Для функторов Ext более высокой степени надо брать более длинные последовательности.

Лекция VII

1 апреля 2024 г.

Пусть $M, N \in \text{mod-}R$.

Определение 1.8.2 (Расширение N при помощи M). Точная последовательность $0 \rightarrow M \rightarrow X \rightarrow N \rightarrow 0$.

Морфизм расширений $0 \rightarrow M \rightarrow X \rightarrow N \rightarrow 0$ и $0 \rightarrow M \rightarrow X' \rightarrow N \rightarrow 0$ — такая стрелка $X \rightarrow X'$, что два получившихся треугольника коммутативны.

Теорема 1.8.1. $\text{Ext}^1(M, N)$ естественно изоморфен множеству классов изоморфизмов расширений N при помощи M .

Доказательство. Рассмотрим расширение $0 \rightarrow M \rightarrow X \rightarrow N \rightarrow 0$. Запишем длинную точную последовательность для $\text{Ext}^1(_, N)$ и данной короткой точной последовательности.

$$\text{Ext}^1(N, M) \longleftarrow \text{Hom}(M, M) \longleftarrow \text{Hom}(X, M) \longleftarrow \text{Hom}(N, M) \longleftarrow 0$$

Теперь построим $x \in \text{Ext}^1(N, M) \cong \text{Ext}^1(M, N)$, как образ $\text{id} \in \text{Hom}(M, M)$.

Теперь построим стрелку обратно: накроем N проективным объектом: $0 \rightarrow A \rightarrow P \rightarrow N \rightarrow 0$.

$$0 = \text{Ext}^1(P, M) \longleftarrow \text{Ext}^1(N, M) \longleftarrow \text{Hom}(A, M) \longleftarrow \text{Hom}(P, M) \longleftarrow \text{Hom}(N, M)$$

Так как домножение на проективный модуль — точный функтор, то $\text{Ext}^1(P, M) = 0$. Теперь пусть X — пушаут диаграммы $M \xleftarrow{\beta} A \rightarrow P$. Следующая диаграмма будет коммутативна:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & P & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow \beta & & \downarrow & & \parallel & & \\ 0 & \longrightarrow & M & \longrightarrow & X & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

Далее можно проверить, что в одну сторону эти отображения взаимно обратны:

$$\begin{array}{ccccccccc} 0 = \text{Ext}^1(P, M) & \longleftarrow & \text{Ext}^1(N, M) & \longleftarrow & \text{Hom}(A, M) & \longleftarrow & \text{Hom}(P, M) & \longleftarrow & \text{Hom}(N, M) \\ & & \uparrow ? & & \uparrow & & \uparrow & & \uparrow \\ \text{Ext}^1(N, M) & \longleftarrow & \text{Hom}(M, M) & \longleftarrow & \text{Hom}(X, M) & \longleftarrow & \text{Hom}(N, M) & \longleftarrow & 0 \end{array}$$

$\text{id} \in \text{Hom}(M, M)$ уходит вверх при $_ \cdot \beta$ в β , далее влево — в x по определению x . Если же отправить id вправо, то он тоже уйдёт в x . **Почему?** И надо ещё проверить, что $? = \text{id}$. \square

Далее идёт отступление про то, что быть определённым с точностью изоморфизма, и быть определённым — разные вещи, и я не справился это записать.

Если же хочется изучить всё кручение M , то оказывается, $\text{Tor}_1(M, F/R) = \{x \in M \mid \exists a \in R \setminus \{0\} : ax = 0\}$ (здесь F/R — фактор R -модулей). Здесь используется, что $F/R = \varinjlim R/aR$, значит, $\text{Tor}_1(F/R, M) = \varinjlim \text{Tor}_1(R/aR, M)$.

1.9 Гомологии и когомологии групп

Пусть G — группа, A — абелева группа, на которой действует G . Иными словами, A — $\mathbb{Z}[G]$ -модуль.

Рассматриваем \mathbb{Z} , либо как кольцо, либо как $\mathbb{Z}[G]$ -модуль с тривиальным действием G .

Определим гомологии $H_n(G, A) \stackrel{\text{def}}{=} \text{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A)$ (верхний индекс $\mathbb{Z}[G]$ указывает, что мы работаем в категории $\mathbb{Z}[G]$ -модулей). Также определим когомологии $H^n(G, A) \stackrel{\text{def}}{=} \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A)$.

Запишем проективную резольвенту по первому аргументу.

- Пусть P_n — свободный \mathbb{Z} -модуль с базисом $\{(g_0, \dots, g_n) \mid g_i \in G\}$. По совместительству P_n — свободный $\mathbb{Z}[G]$ -модуль с базисом $\{(1, g_1, \dots, g_n) \mid g_i \in G\}$ и действием $g \cdot (g_0, \dots, g_n) = (gg_0, \dots, gg_n)$.

- Теперь определим гомоморфизмы.

$$\cdots \longrightarrow P_0 = \mathbb{Z}[G] \longrightarrow \mathbb{Z}$$

Граничные гомоморфизмы определены так: $d_n(g_0, \dots, g_n) = \sum_{i=0}^n (-1)^i (g_0, \dots, \widehat{g_i}, \dots, g_n)$. Несложно проверить, что $d_{n-1} \cdot d_n = 0$.

- Посчитаем нулевые гомологии и когомологии группы G . $H_0(G, A) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$.

$\mathbb{Z} = \mathbb{Z}[G]/I_G$, где $I_G = \text{Ker}(\phi)$, здесь $\phi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$ — \mathbb{Z} -линейный гомоморфизм аугментации, определённый на базисе $g \mapsto 1$. Иными словами, $I_G = \langle g - 1 | g \in G \rangle = \left\{ \sum_{g \in G} \alpha_g \cdot g \mid \sum_{g \in G} \alpha_g = 0 \right\}$, все суммы финитные.

Тем самым, $H_0(G, A) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \cong A/(I_G A)$ — *коинварианты*. $I_G A = \langle ga - a | g \in G, a \in A \rangle$.

- Теперь посчитаем когомологии. $H^0(G, A) = \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$. Всякому гомоморфизму $\varphi \in \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ можно $\phi(1)$. Из G -линейности $\forall g \in G : \phi(1) = \phi(g \cdot 1) = g \cdot \phi(1)$, значит, $\phi(1) \in A^G \stackrel{\text{def}}{=} \{a \in A | \forall g \in G : ga = a\}$ — *инварианты*. Значит, нулевые когомологии — инварианты.

- $H_1(G, \mathbb{Z}) = G^{\text{ab}} \stackrel{\text{def}}{=} G/[G, G]$.

- $H^1(G, A) = \text{Der}(G, A)$ — множество скрещённых гомоморфизмов.

Скрещенный гомоморфизм — это такое отображение $\phi : G \rightarrow A$, которое обладает свойством $\phi(gh) = g \cdot \phi(h) + \phi(g)$.

- $H_2(G, \mathbb{Z}) = ?$ Предположим, что имеется точная последовательность групп $0 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$, то есть $G \cong F/R$.

$$\text{Тогда } H_2(G, \mathbb{Z}) = \frac{R \cap [F, F]}{[R, F]}.$$

Если $[G, G] = G$ (G совершенна), то существует универсальное центральное расширение $\pi : S \twoheadrightarrow G$, то есть $\text{Ker}(\pi) \in C(S)$, и

$$\begin{array}{ccc} S & \twoheadrightarrow & G \\ & \searrow \exists! & \uparrow \forall \text{ центрального расширения} \\ & & H \end{array}$$

В этом случае $H_2(G, \mathbb{Z}) = \text{Ker } \pi$. Например, в случае $G = SL_n(F) : S = \text{St}_n(F)$ — *группа Штейнберга*. Ядро $\text{St}_n(F) \twoheadrightarrow SL_n(F)$ — это $K_{2,n}(F) = H_2(G, \mathbb{Z})$. Для $n \geq 5$ от поля ничего не зависит.

Глава 2

Теория Галуа

Лекция VIII

15 апреля 2024 г.

2.1 Базовые понятия про расширения полей

Мы будем изучать расширения полей, и базовое поле будем обозначать F (от английского Field), а расширенное — K (от немецкого Körper). Имеется теоретико-множественное включение $F \subset K$, и включение полей обозначается K/F (это не надо путать с факторкольцом, никаких факторов здесь не берётся, просто общепринятое обозначение).

K является векторным пространством над F , и $\dim_F K \stackrel{\text{def}}{=} [K : F]$ — *степень расширения*.

Для элемента $\alpha \in K$ поле $F(\alpha)$ — наименьшее подполе в K , содержащее F и α .

Лемма 2.1.1 (О простых расширениях). *Либо $F(\alpha) \cong F(t)$ — поле дробно-рациональных функций, оно же поле частных $K[t]$, его общий элемент имеет вид $\frac{p}{q}$ ($p \in F[t], q \in F[t]^*$).*

Либо $F(\alpha) \cong F[t]/(p)$, где $p \in F[t]$ — неприводимый. В этом случае $\deg p$ — степень расширения.

Доказательство. Рассмотрим гомоморфизм F -алгебр $\phi : F[t] \rightarrow F(\alpha), t \mapsto \alpha$.

- Если $\text{Ker } \phi = \{0\}$, то $\text{Im } \phi \cong F[t]$. Тем самым, $F(\alpha) \supset \text{Im } \phi$, а раз $F(\alpha)$ — поле, то оно содержит и поле частных $Q(\text{Im } \phi) \cong Q(F[t])$.

Так как $F[t]$ — наименьшее подполе, то $F(\alpha) \cong F(t)$.

- Иначе, так как многочлены — PID — то $\text{Ker } \phi = p \cdot F[t]$, и $\text{Im } \phi \cong F[t]/(p)$. То, что p неприводим, легко видеть от противного: если $p = rs$, то один из r, s ассоциирован с p , иначе в кольце появляются делители нуля.

Тем самым, раз p неприводим, то (p) — максимальный идеал, откуда $\text{Im } \phi \cong F[t]/(p)$ — уже поле. Базисом $F[t]/(p)$ над K является, например, $(1, \bar{t}, \dots, \bar{t}^{\deg(p)-1})$.

□

В первом случае $F(\alpha) \cong F(t)$ элемент $\alpha \in K$ называется *трансцендентным*.

Во втором случае $F(\alpha) \cong F[t]/(p)$ элемент $\alpha \in K$ называется *алгебраическим*. В таком случае $p \in F[t]$ — *минимальный многочлен* α . Таким образом, $F(\alpha) = F[\alpha]$, где $F[\alpha]$ — наименьшее кольцо в K , содержащее F и α .

В случае расширений колец вместо слова алгебраический используют *целый* при дополнительном условии унитарности минимального многочлена.

Определение 2.1.1 (Алгебраическое расширение K/F). Такое расширение, что $\forall \alpha \in K$: α — алгебраический. Иначе ($\exists \alpha \in K$: α — трансцендентный) расширение называют трансцендентным.

Определение 2.1.2 (Конечное расширение F/K). Расширение конечной степени: $[K : F] < \infty$.

Конечные и алгебраические расширения тесно связаны между собой, но, конечно, существует бесконечное алгебраическое расширение. Например, $\mathbb{Q}(\sqrt{p} | p \in \mathbb{P})$ — имеет бесконечную степень над \mathbb{Q} , так как корни из простых чисел линейно независимы над \mathbb{Q} (что ещё надо обосновать).

Лемма 2.1.2. Пусть имеется композиция расширений $L/K/F$. Тогда $[L : F] = [L : K] \cdot [K : F]$.

Доказательство. Пусть $(a_\alpha)_{\alpha \in A}$ — базис K над F , и $(b_\beta)_{\beta \in B}$ — базис L над K .

Тогда несложно видеть, что $(a_\alpha \cdot b_\beta)_{\alpha \in A, \beta \in B}$ — базис L над F . □

Теорема 2.1.1. Следующие условия равносильны

1. Расширение K/F конечно.
2. K/F — алгебраическое и конечнопорождённое.
3. $K = F[\alpha_1, \dots, \alpha_n]$, где все α_i алгебраичны над F .

Доказательство.

(3) \Rightarrow (1) Индукция по n .

База: $n = 0 \Rightarrow K = F$.

Переход: $F[\alpha_1, \dots, \alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n]$. Так как α_n алгебраично над F , то оно алгебраично и над $F[\alpha_1, \dots, \alpha_{n-1}]$ (впрочем, степень трансцендентности при увеличении поля может стать меньше).

(1) \Rightarrow (2) **Лемма 2.1.3.** Любой элемент конечного расширения K/F алгебраический.

Доказательство леммы.

Рассмотрим $\alpha \in K$. Так как расширение конечно, то $1, \alpha, \alpha^2, \dots$ линейно зависимы. Выбрав линейную зависимость $\beta_0 + \beta_1 \alpha + \dots + \beta_d \alpha^d = 0$. Тогда $\beta_0 + \beta_1 t + \dots + \beta_d t^d$ аннулирует α , то есть ядро ϕ из доказательства (лемма 2.1.1) ненулевое. □

Пусть $[K : F] = d$, значит, K имеет базис $(\alpha_1, \dots, \alpha_d)$ над F . Тогда K порождено элементами $\alpha_1, \dots, \alpha_d$ даже просто как векторное пространство, а не как F -алгебра □

(2) \Rightarrow (3) Тавтологично.

2.1.1 Алгебраическое замыкание одного поля в другом

Пусть имеется расширение полей K/F , тогда $\text{Int}_K F \stackrel{\text{def}}{=} \{\alpha \in K | \alpha \text{ алгебраичен над } F\}$ — целое (алгебраическое) замыкание F в K .

$\text{Int}_K F$ является полем: $\forall \alpha, \beta \in \text{Int}_K F$: $\alpha - \beta, \alpha + \beta, \alpha \cdot \beta, \frac{\alpha}{\beta}$ (последнее при $\beta \neq 0$) лежат в $F[\alpha, \beta]$, а это — конечное расширение согласно (теорема 2.1.1).

Пусть $X \subset K$, где по-прежнему K/F .

Определение 2.1.3 (X алгебраически независим над F). $\forall f \in F[t_1, \dots, t_m], \forall x_1, \dots, x_m \in X$ (где x_i попарно различны): $f(x_1, \dots, x_m) \neq 0$.

Иными словами, отображение из универсальной F -алгебры, порождённой элементами X в $F[X]$ (определённое на образующих $x \mapsto x$) имеет нулевое ядро.

Определение 2.1.4 (Линейная оболочка X над F). $\langle X \rangle \stackrel{\text{def}}{=} \text{Int}_K F(X)$.

Определение 2.1.5 (X — (алгебраический) базис расширения K/F). Алгебраически независимое X такое, что $\langle X \rangle = K$. При этом $|X|$ называется *степенью трансцендентности* K/F .

Пример. В кольце $F(t)$: $\{t\}$ — базис трансцендентности.

Для алгебраического базиса X верны те же аксиомы, что и для базиса векторных полей:

1. todo
2. todo
3. todo

Я не смог найти эти аксиомы, а интересно, может кто-то другой подскажет, как они выглядят?

Теорема 2.1.2. Степень трансцендентности не зависит от выбора базиса.

Доказательство. Аналогично подобному факту из линейной алгебры. □

2.1.2 Поле разложения

Пусть F — поле, $f \in F[t]$.

Определение 2.1.6 (Поле разложения f над F). Поле F_f/F , в котором f раскладывается на линейные множители, и вкладывающееся (**не факт**, что единственным образом) в любое другое поле, обладающее тем же свойством.

Примеры.

- $F = \mathbb{R}, f = t^2 + 1$. В этом случае $F_f \cong \mathbb{C}$.
- $F = \mathbb{Q}, f = t^3 - 2$. В этом случае $\mathbb{Q}(\sqrt[3]{2})$ — не поле разложения, оно вкладывается в \mathbb{R} , а f в \mathbb{R} на линейные множители не раскладывается.

Надо присоединить ещё какой-то корень f , достаточно присоединить какой-то $\sqrt[3]{1}$, отличный от 1; это то же самое, что присоединить $\sqrt{-3}$. Тем самым, поле разложения $\mathbb{Q}_f \cong \mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}]$.

Теорема 2.1.3. Для любого $f \in F[t]$ существует его поле разложения.

Доказательство. Индукция по $\deg f$.

База: $\deg f = 1 \Rightarrow F_f = F$.

Переход: Пусть $f = pg$, где p — неприводим.

Пусть $E := F[t]/(p)$. В E : $\alpha := \bar{t} = t + (p)$ — корень p .

Над E : $f(t) = (t - \alpha) \cdot h(t)$ для некоторого h : $\deg h = \deg f - 1$. Положим $F_f := E_h$, E_h существует по индукционному предположению.

Теперь пусть K/F — другое поле, в котором f раскладывается на линейные множители. Сначала устроим вложение $E \hookrightarrow K$, отправив α в любой корень p . Такой корень найдётся в K , так как $F[t] = \text{UFD}$.

При этом h раскладывается в K на линейные множители, по индукции E_h вкладывается в K . □

Пусть K/F и L/F — расширения полей. Тогда гомоморфизм $\phi : K \rightarrow L$ называется *гомоморфизмом полей над F* , если он оставляет F на месте. Все гомоморфизмы полей по определению сохраняют 1, в частности, любой гомоморфизм полей инъективен ($\phi(x) = \phi(y) \iff \phi(xy^{-1}) = \phi(1) \iff xy^{-1} = 1$).

Теорема 2.1.4. Пусть K — поле, в котором $f \in F[t]$ раскладывается на линейные множители. Тогда K — поле разложения $f \iff K \cong F[\alpha_1, \dots, \alpha_n]$, где α_i — корни f .

Доказательство. В одну сторону видно, что построенное в (теорема 2.1.3) поле разложения действительно порождено корнями f .

В другую сторону, можно устроить гомоморфизм $K \rightarrow F[\alpha_1, \dots, \alpha_n]$, он сюръективен (в образе лежит F , так как гомоморфизм — над F , и в образе лежат корни α_i , так как в них отравили корни многочлена f) и инъективен (любой гомоморфизм полей инъективен). \square

Лекция IX

16 апреля 2024 г.

Лемма 2.1.4. Пусть K/F и L/F — конечные расширения, и $K \rightarrow L, L \rightarrow K$ — гомоморфизмы над F . Тогда $K \cong L$ (оба отображения — изоморфизмы).

Доказательство. Достаточно убедиться, что оба гомоморфизма биективны, а это удобно проверить, рассматривая K и L , как векторные пространства над F . Так как гомоморфизмы полей — мономорфизмы, то $\dim_F K = \dim_F L$. \square

Пусть F — конечное поле ($|F| < \infty$). В поле есть единица, и так как поле конечное, то его характеристика ненулевая: в конечной аддитивной группе поля любой элемент, в том числе 1, имеет конечный порядок. Пусть p — эта характеристика. Так как поле — область целостности, то $p \in \mathbb{P}$.

Тем самым, в F вкладывается поле из p элементов, изоморфное факторкольцу $\mathbb{Z}/p\mathbb{Z}$. Обозначим поле из p элементов за \mathbb{F}_p .

Лемма 2.1.5. Любое конечное поле характеристики p содержит p^n элементов, где $n \in \mathbb{N}$.

Доказательство. Так как F — векторное пространство над \mathbb{F}_p , то $F \stackrel{\mathbb{F}_p\text{-Vect}}{\cong} \mathbb{F}_p^n$ для некоторого $n \in \mathbb{N}$. \square

Теорема 2.1.5. Для любого простого p и любого $n \in \mathbb{N}$ существует поле из p^n элементов. При этом все такие поля изоморфны (но изоморфизмов может быть несколько).

Доказательство.

- Обозначим $q := p^n \in \mathbb{N}$. Рассмотрим $f \in \mathbb{F}_p[t], f(t) = t^q - t$, и посмотрим на его поле разложения $(\mathbb{F}_p)_f$. Так как в \mathbb{F}_p : $q = 0$, то $f'(t) = qt^{q-1} - 1 = -1$, что показывает, что у f нет кратных корней. Тем самым, $F := (\mathbb{F}_p)_f$ содержит по меньшей мере q элементов — корни f .
- Рассмотрим корни f в его поле разложения $X := \{x \in F \mid x^q - x = 0\} \subset F$. Заметим, что X замкнуто относительно сложения и умножения:

$$\begin{cases} x^q = x \\ y^q = y \end{cases} \Rightarrow \begin{cases} (xy)^q = xy \\ (x+y)^q = x^q + y^q = x + y \end{cases}$$

Первое следует из коммутативности, второе — из того, что p делит все биномиальные коэффициенты $\binom{q}{k}$, кроме $\binom{q}{0}$ и $\binom{q}{q}$; $x \mapsto x^p$ — эндоморфизм Фробениуса из первого семестра, а $x^q = ((x^p)^\cdot)^p$.

Тем самым, $X \leq F$ — подкольцо в F . Так как $\forall x \in X : x^{q-2} = x^{-1}$, то это даже подполе. Более того, так как $1 \in X$, то X/\mathbb{F}_p — тоже расширение полей.

С другой стороны, X содержит все корни $t^q - t$, а F — поле разложения $t^q - t$, значит, имеется и гомоморфизм $F \rightarrow X$. X/\mathbb{F}_p и F/\mathbb{F}_p конечны, откуда (лемма 2.1.4) $X = F$.

- Пусть E — произвольное поле порядка p^n . Его характеристика равна p , значит, в него вкладывается \mathbb{F}_p . $|E^*| = q - 1$, значит по теореме Лагранжа (о порядке элемента в группе) $\forall x \in E : x^{q-1} = 1$. Тем самым, f раскладывается на линейные множители и в E , откуда опять же имеется вложение $F \hookrightarrow E$. Но $|F| = |E| = q$, значит, $F \cong E$. \square

Лемма 2.1.6. Пусть F — поле. Следующие условия эквивалентны:

1. $\forall f \in F[t] \setminus F : f$ раскладывается на линейные множители в F .
2. $\forall f \in F[t] \setminus F : f$ имеет корень в F .
3. $\forall f \in F[t] \setminus F : (f \text{ неприводим} \iff \deg f = 1)$.
4. Любое алгебраическое расширение F совпадает с F .
5. Любое конечное расширение F совпадает с F .

Доказательство. Тривиально.

- (1) \Rightarrow (2) Тавтологично.
- (2) \Rightarrow (3) \Rightarrow следует из теоремы Безу (α корень $\iff t - \alpha$ — делитель), \Leftarrow следует из того, что все многочлены степени 1 неприводимы.
- (3) \Rightarrow (4) Пусть E/F — алгебраическое расширение, выберем $\theta \in E$, и найдём его минимальный многочлен. Он неприводим $\Rightarrow \deg f = 1$, то есть $\theta \in F$.
- (4) \Rightarrow (5) Тавтологично.
- (5) \Rightarrow (1) Рассмотрим $f \in F[t]$. $F_f = F \Rightarrow$ все корни f лежат в F . Так как f неприводим, то $\deg f = 1$. □

Определение 2.1.7 (Алгебраически замкнутое поле). Поле F , удовлетворяющее условиям из предыдущей леммы (лемма 2.1.6).

Лемма 2.1.7. Пусть K/F — алгебраическое расширение, и любой многочлен из $F[t]$ раскладывается на линейные множители в $K[t]$. Тогда K алгебраически замкнуто.

Доказательство. Пусть f — неприводимый в $K[t]$. Без потери общности f — унитарный: $f(t) = t^n + \alpha_{n-1}t^{n-1} + \dots + \alpha_0$. Построим поле $E := F[\alpha_0, \dots, \alpha_n]$, расширение E/F конечно.

f тем более неприводим в E , значит, можно рассмотреть поле $L := E[t]/(f)$, расширение L/E , а

стало быть и L/F тоже конечны.

$$\begin{array}{ccc}
 & K & L \\
 \text{алгебраично} \downarrow & & \nearrow \text{конечно} \\
 E & & \\
 \text{конечно} \downarrow & & \\
 & F &
 \end{array}$$

f имеет корень в L , назовём его β . В силу конечности β алгебраично над F , то есть $\exists g \in F[t] : g(\beta) = 0$. Согласно посылке леммы, g разложим на множители в $K[t]$, значит, имеется вложение $\phi : F_g \hookrightarrow K$ над E . Но $f(\beta) = 0 \Rightarrow f(\phi(\beta)) = \phi(f(\beta)) = \phi(0) = 0$, то есть f имеет корень в K . □

Интересный факт. Можно ослабить посылку: если K/F — алгебраическое расширение, и любой многочлен из $F[t]$ имеет корень в K , то K алгебраически замкнуто.

Лемма 2.1.8. Пусть L/F — расширение полей, причём L алгебраически замкнуто. Тогда $\text{Int}_L F$ тоже алгебраически замкнуто.

Доказательство. Рассмотрим $f \in F[t]$. В L он раскладывается на линейные множители $f(t) = (t - \alpha_1) \dots (t - \alpha_n)$, где $\alpha_i \in L$. Согласно (??) целого замыкания $\alpha_i \in \text{Int}_L F$. □

Пример. Рассмотрим расширение \mathbb{C}/\mathbb{Q} . Целые алгебраические числа $\mathbb{A} \stackrel{\text{def}}{=} \text{Int}_{\mathbb{C}} \mathbb{Q}$ — алгебраически замкнутое подполе в \mathbb{C} . Оно не совпадает с \mathbb{C} , так как \mathbb{C} континуально, а $\text{Int}_{\mathbb{C}} \mathbb{Q}$ счётно.

Определение 2.1.8 (Алгебраическое замыкание поля F). Алгебраическое расширение F , являющееся алгебраически замкнутым полем. Обозначается F^{alg} .

Теорема 2.1.6. У любого поля F существует алгебраическое замыкание.

Доказательство. Рассмотрим множество многочленов $F[t]$, как множество индексов, и введём множество переменных $X := \{x_f | f \in F[t]\}$. Далее рассмотрим кольцо многочленов от этих переменных $F[X]$, и профакторизуем его по идеалу $J := (f(x_f) | f \in F[t])$.

Лемма 2.1.9. *Этот идеал не совпадает со всем кольцом: $J \neq F[X]$.*

Доказательство леммы.

Пойдём от противного: $J = F[X] \Rightarrow 1 \in J$, то есть существует конечная линейная комбинация

$$g_1 f_1(x_{f_1}) + \dots + f_m f_m(x_{f_m}) = 1, \text{ где } f_i, g_i \in F[t] \quad (\Delta)$$

Корни конечного множества многочленов мы умеем присоединять: введём $f := f_1 \cdot \dots \cdot f_m$, в F_f у каждого из f_i есть корень, назовём его β_i . Теперь устроим гомоморфизм F -алгебр

$\phi : F[X] \rightarrow F_f, \begin{cases} x_{f_i} \mapsto \beta_i \\ x_g \mapsto 0 \end{cases}$, он определён согласно универсальному свойству кольца многочленов.

В образе (Δ) обращается в равенство $0 = 1$, но в F_f это, конечно, неверно. \square

Раз $J \not\subseteq F[X]$ не совпадает со всем кольцом, то можно взять максимальный идеал \mathfrak{m} , содержащий J , и не совпадающий со всем кольцом (лемма Цорна). Факторкольцо $E_1 := F[X]/\mathfrak{m}$ является полем, в котором образ переменной x_f — корень многочлена f .

К сожалению, не факт, что E_1 алгебраически замкнуто: (лемма 2.1.7) неприменима, так как неизвестно, алгебраично ли расширение E_1/F .

Обозначим $E_0 := F$, и устроим итерации, по E_i получая E_{i+1} согласно вышеописанной процедуре. Для цепочки вложений полей $E_0 \hookrightarrow E_1 \hookrightarrow E_2 \hookrightarrow \dots$ можно рассмотреть объединение с понятными операциями. Поле $\bar{F} := \bigcup_{i=0}^{\infty} E_i$ уже является алгебраически замкнутым полем (любой многочлен из $\bar{F}[t]$ имеет конечное количество коэффициентов, которые все лежат в каком-то E_N , а корень можно найти в E_{N+1}).

Теперь осталось положить $F^{\text{alg}} := \text{Int}_{\bar{F}} F$, оно алгебраически замкнуто, согласно (лемма 2.1.8). \square

Лекция X

22 апреля 2024 г.

Предложение 2.1.1. *Пусть E/F — алгебраическое расширение, и L/F — такое расширение, что $\forall f \in F[t]: f$ раскладывается на линейные множители в $L[t]$. Обозначим $K := \text{Int}_L F$. Тогда*

1. *Существует вложение $\phi : E \hookrightarrow L$ над F .*
2. *Для всякого вложения $\phi: \phi(E) \subset K$.*
3. *Если E алгебраически замкнуто, то $\phi(E) = K$.*

Доказательство.

1. Образует множество $\mathcal{X} := \left\{ (\tilde{F}, \phi) \middle| F \subset \tilde{F} \subset E, \phi : \tilde{F} \hookrightarrow L \right\}$. На \mathcal{X} введём частичный порядок: $(F', \phi') \preceq (F'', \phi'') \iff F' \subset F'' \text{ и } \phi'|_{F'} = \phi'$.

\mathcal{X} непусто, так как $(F, F \hookrightarrow L) \in \mathcal{X}$.

Убедимся, что здесь применима лемма Цорна: если $(F_\alpha, \phi_\alpha)_{\alpha \in A}$ — цепь, то $\tilde{F} := \bigcup_{\alpha \in A} F_\alpha$

вместе с $\tilde{\phi}$ — верхняя грань (где $\tilde{\phi}$ определено так: и $\forall x \in \tilde{F} : \tilde{\phi}(x) := \phi_\alpha(x)$ для произвольного α , такого, что $x \in F_\alpha$).

Тем самым, имеется максимальный элемент $(\tilde{F}, \tilde{\phi}) \in \mathcal{X}$. Предположим, что $\tilde{F} \neq E$, то есть $\exists \theta \in E \setminus \tilde{F}$. Пусть $f \in F[t]$ — минимальный многочлен θ в F , и $g \in \tilde{F}[t]$ — минимальный многочлен θ над \tilde{F} .

Отождествим \tilde{F} с его образом $\tilde{\phi}(\tilde{F}) \subset L$ (ϕ инъективно, как гомоморфизм полей).

В L многочлен f раскладывается на линейные множители. Так как $g \mid f$, то $g \in L[t]$ тоже раскладывается на линейные множители, то есть $\exists \alpha \in L : g(\alpha) = 0$. Согласно универсальному свойству простого расширения: $\tilde{F}[\theta] \cong \tilde{F}[t]/(g)$, то есть $\exists! \psi : \tilde{F}[\theta] \rightarrow \tilde{F}[\alpha]$ — гомоморфизм полей над \tilde{F} , такой, что $\psi(\theta) = \alpha$.

2. Предположим, что ϕ существует. Корень $f \in F[t]$ переходит в корень, поэтому ϕ сохраняет множество алгебраических элементов, откуда $\phi(E \subset K$.
3. Рассмотрим $\beta \in K$, это корень некоторого унитарного многочлена $f \in F[t]$. В E многочлен f раскладывается на линейные множители $f(t) = (t - \alpha_1) \cdot \dots \cdot (t - \alpha_n)$, где $\alpha_i \in E$. Применяя индуцированный $\phi : E[t] \rightarrow L[t]$ к данному разложению, получаем $f(t) = (t - \phi(\alpha_1)) \cdot \dots \cdot (t - \phi(\alpha_n))$. Подставляя β , получаем, нуль. Значит, $\beta = \phi(\alpha_i)$ для некоторого i . \square

Следствие 2.1.1. Любое алгебраическое расширение F вкладывается в алгебраическое замыкание F .

Следствие 2.1.2. Алгебраическое замыкание F вкладывается в любое алгебраически замкнутое поле, содержащее F .

Следствие 2.1.3. Алгебраическое замыкание единственно с точностью до не единственного изоморфизма.

2.1.3 Сепарабельность

Пусть F — поле, $f \in F[t]$.

Определение 2.1.9 (Сепарабельный многочлен f). f не имеет кратных корней в F^{alg} .

Так как кратные корни — это корни $\gcd(f, f')$, то условие сепарабельности эквивалентно условию $\gcd(f, f') = 1$.

Если $f = \prod_{i=1}^n f_i$, где f_i неприводимы, то f сепарабелен \iff все f_i различны и сепарабельны.

Неприводимый же многочлен на сепарабельность проверять легко: $\deg f' < \deg f$, поэтому при $\deg f > 0$: $\gcd(f, f') \neq 1 \iff f' = 0$ (что бывает только в конечной характеристике).

Теперь пусть E/F — алгебраическое расширение полей.

Определение 2.1.10 ($\alpha \in E$ сепарабелен над F). Минимальный многочлен α сепарабелен.

Определение 2.1.11 (Расширение E/F сепарабельно). $\forall \alpha \in E$: $\alpha \in E$ сепарабелен над F .

Интересный факт. $F = E^{\text{Aut}(E/F)} \iff E/F$ — сепарабельное расширение. Здесь $\text{Aut}(E/F)$ — автоморфизмы E , тождественные над F , и для $G \subset \text{Aut}(E/F)$: $E^G \stackrel{\text{def}}{=} \{x \in E \mid \forall g \in G : gx = x\}$ — множество точек, оставляемых под действием G на месте.

Примеры (Сепарабельные и несепарабельные расширения).

- Любое расширение поля характеристики нуль сепарабельно.
- Пусть $F := \mathbb{F}_p(t^p)$, $E := \mathbb{F}_p(t)$. Рассмотрим многочлен $x^p - t^p \in F[x]$. Он неприводим над F , так как даже свободный член неприводим, и видно, что все ассоциированные с t^p — не корни.

Но над E : $x^p - t^p = (x - t)^p$, то есть $x^p - t^p \in F[x]$ неприводим и несепарабелен. И действительно, $(x^p - t^p)' = px^{p-1} = 0$.

Определение 2.1.12 (Совершенное поле F). Любое алгебраическое расширение F сепарабельно.

Упражнение 2.1.1. Верно ли, что F совершенно \iff эндоморфизм Фробениуса $\text{Frob} : F \rightarrow F, x \mapsto x^p$ сюръективен?

Примеры.

- Если $\text{char } F = 0$, то F совершенно.
- Если $|F| < \infty$, то F совершенно.

Доказательство. Рассмотрим $\theta \in F^{\text{alg}}$. $|F[\theta]| = q^n$, где $q := |F|$. Тогда $\theta^{q^n-1} = 1$ (теорема Лагранжа для мультипликативной группы $F[\theta]^*$), то есть θ — корень $t^{q^n-1} - 1$.

Этот многочлен взаимно прост со своей производной: $(t^{q^n-1} - 1)' = (q^n - 1)t^{q^n-2} = -t^{q^n-2}$, и $\gcd(-t^{q^n-2}, t^{q^n-1} - 1) = 1$.

Минимальный многочлен θ делит $t^{q^n-1} - 1$, значит, он тоже не имеет кратных корней. \square

Лекция XI

29 апреля 2024 г.

Предложение 2.1.2. Пусть E/F — алгебраическое расширение полей. Следующие условия эквивалентны:

1. E/F несепабельно.
2. Минимальный многочлен некоторого $\theta \in E$ несепабелен над F .
3. $\exists f \in F[t]$ — неприводимый в $F[t]$, такой, что $f' = 0$, причём f имеет корень в E .
4. $\exists f \in F[t]$ — неприводимый в $F[t]$, такой, что f имеет кратный корень в E .
5. $\exists f \in F[t]$ — неприводимый в $F[t]$, такой, что $\exists g \in F[t] : f(t) = g(t^p)$, причём f имеет корень в E .

Доказательство. (1) \iff (2) \Rightarrow (3) \iff (4) \Rightarrow (5) очевидно (эквивалентность (3) \iff (4) соблюдена, так как для неприводимого многочлена $f : \gcd(f, f') \neq 1 \iff f' = 0$).

Докажем (5) \Rightarrow (2). Пусть $\theta \in E$ — корень f . Подставим: $f(\theta) = g(\theta^p) = 0$. Получили $(t - \theta^p) \mid g \Rightarrow (t - \theta)^p = t^p - \theta^p \mid f$. \square

На самом деле, данное предложение говорит, что кратность любого корня неприводимого несепабельного многочлена делится на p .

Упражнение 2.1.2. Сепарабельное расширение сепарабельного расширения сепарабельно.

Используя данное предложение, несложно доказать эквивалентность из (упражнение 2.1.1):

Доказательство. Если E/F несепабельно, то найдётся неприводимый многочлен $f = (\alpha_n t^{pn} + \alpha_{n-1} t^{p(n-1)} + \dots + \alpha_0) \in F[t]$. Но так как автоморфизм Фробениуса сюръективен, то $\forall \alpha_j \in F : \exists \beta_j \in F : \beta_j^p = \alpha_j$. Получаем

$$\alpha_n t^{pn} + \alpha_{n-1} t^{p(n-1)} + \dots + \alpha_0 = (\beta_n t^{pn} + \beta_{n-1} t^{p(n-1)} + \dots + \beta_0)^p$$

что противоречит неприводимости f . \square

Определение 2.1.13 (Расширение E/F нормально). Любой неприводимый многочлен из $F[t]$, имеющий корень в E , раскладывается на линейные множители в E

Пример. $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ не нормально, так как $t^3 - 2$ не раскладывается на линейные множители даже в \mathbb{R} .

Любое расширение несложно сделать нормальным, присоединив все корни всех неприводимых многочленов из $F[t]$, имеющих корни в E .

Определение 2.1.14 (Расширение Галуа). Конечное сепарабельное нормальное расширение.

Условие конечности иногда отсутствует, но мы другими заниматься не будем.

Определение 2.1.15 (Группа Галуа расширения Галуа E/F). Группа автоморфизмов E , тождественных на F : $\text{Gal}(E/F) \stackrel{\text{def}}{=} \text{Aut}(E/F)$.

Группа автоморфизмов расширения E/F имеет смысл и не для расширения Галуа, но там не используется запись Gal .

Теорема 2.1.7. Пусть имеются расширения K/F и E/F , и $f \in F[t]$. При этом K порождено некоторыми корнями многочлена f , а в E : f раскладывается на линейные множители. Пусть n — количество вложений $K \hookrightarrow E$ над F .

1. $0 < n \leq [K : F]$
2. Если f сепарабелен, то $n = [K : F]$.
3. Если f несепарабелен, свободен от квадратов в $F[t]$, и любой неприводимый в $F[t]$ сомножитель f имеет корень в K , то $n < [K : F]$.

Доказательство. Индукция по степени расширения $[K : F]$.

База: $[K : F] = 1 \iff K = F$.

Переход: разложим $f = f_1 \cdot \dots \cdot f_n$, где неприводимые $f_i \in F[t]$. $K \neq F \Rightarrow$ не все f_i имеют степень 1. Без потери общности f_1 имеет корень в $K \setminus F$. Если такой существует, то выберем f_1 , как несепарабельный многочлен, имеющий корень в K .

Зафиксируем какое-то вложение $F[t]/(f_1) \hookrightarrow K$, отождествим $F[t]/(f_1)$ со своим образом $\tilde{F} \leq K$. Используя универсальное свойство простого расширения, получаем, что количество вложений $\tilde{F} \hookrightarrow E$ (назовём его k) равно количеству корней f_1 в E .

Если f_1 сепарабелен, то в E он имеет $\deg f_1$ корней, иначе — строго меньше.

Пусть $\phi : \tilde{F} \hookrightarrow E$ — фиксированное вложение. Отождествим \tilde{F} и $\phi(\tilde{F})$. Расширение K/\tilde{F} порождено корнями f , он по-прежнему раскладывается на линейные множители в E .

$[K : \tilde{F}] \cdot [\tilde{F} : F] = [K : F] \Rightarrow [K : \tilde{F}] < [K : F]$. По индукционному предположению существует m вложений $K \hookrightarrow E$ над \tilde{F} , где $m \leq [K : \tilde{F}]$.

Так как столько вложений имеется для каждого ϕ , то $n = km \leq [\tilde{F} : F] \cdot [K : \tilde{F}] = [K : F]$. При этом, если f сепарабелен и свободен от квадратов, то несепарабельный f_1 , имеющий корень в K , найдётся, тогда $k < [\tilde{F} : F]$ и $n < [K : F]$. \square

Следствие 2.1.4. Пусть K/F и E/F — конечные расширения.

1. Количество вложений $K \hookrightarrow E$ над F не превосходит $[K : F]$.
2. Существует расширение L/E : имеется вложение $K \hookrightarrow L$ над F .
3. Если E/F — расширение Галуа, то количество вложений $K \hookrightarrow E$ над F равно либо $[K : F]$, либо 0.

Доказательство. Пусть $K = F[\alpha_1, \dots, \alpha_n]$, пусть f_1, \dots, f_n — минимальные многочлены $\alpha_1, \dots, \alpha_n$ соответственно.

Избавимся от ассоциированных, оставив только уникальные, и положим f равному их произведению.

Положим $L := E_f$. Теперь выполнена посылка (теорема 2.1.7), откуда количество вложений $K \hookrightarrow L$ над F не 0, но и не более $[K : F]$.

Если существует вложение $K \hookrightarrow E$ над F , то все f_i имеют корни в E и K/F сепарабельно. Тогда $\alpha_1, \dots, \alpha_n$ сепарабельны над F , то есть f сепарабелен над F . А из нормальности расширения

E/F все f_i раскладываются на линейные множители в E . Тем самым, $L = E$, и (теорема 2.1.7) завершает доказательство. \square

Следствие 2.1.5. Для расширения Галуа: $|\text{Gal}(E/F)| = [E : F]$.

Теорема 2.1.8 (Лемма Артина). Пусть E — поле, и $G \leq \text{Aut}(E)$, $|G| < \infty$. Обозначим $F := E^G \stackrel{\text{def}}{=} \{\alpha \in E \mid \forall g \in G : g\alpha = \alpha\}$.

Тогда $[E : F] = |G|$.

Доказательство. Достаточно доказать, что $[E : F] \leq |G|$, обратное неравенство следует из (следствие 2.1.4).

Пусть $G = \{\phi_1, \phi_2, \dots, \phi_n\}$, где $\phi_1 = 1_G = \text{id}_E$. Пусть $m > n$, $\alpha_1, \dots, \alpha_m \in E$, докажем, что $\alpha_1, \dots, \alpha_m$ линейно зависимы над F .

Заведём систему линейных уравнений $\left\{ \sum_{j=1}^m \phi_j(\alpha_i) x_i = 0 \right\}_{j=1}^n$ относительно переменных x_1, \dots, x_m .

В ней уравнений меньше, чем неизвестных, поэтому по теореме о размерности пересечения имеется ненулевое решение $\beta_1, \dots, \beta_m \in E$. Без потери общности $\beta_1 = 1$ (можно все β_i поделить на β_1).

Пусть в наборе β_1, \dots, β_m наименьшее количество ненулевых элементов. Если $\exists k : \beta_k \notin F$, то $\exists l : \phi_l(\beta_k) \neq \beta_k$. Вычитая решения, получаем противоречие. \square

Лекция XII

6 мая 2024 г.

Следствие 2.1.6. Для любой группы $G \leq \text{Aut}(E)$: $\text{Aut}(E/E^G) = G$.

Доказательство. Очевидно, $G \leq \text{Aut}(E/E^G)$. По лемме Артина $|G| = [E : E^G] \geq |\text{Aut}(E/E^G)| \geq |G|$, и равенство достигается только при $G = \text{Aut}(E/E^G)$ \square

Теорема 2.1.9 (Характеризация расширений Галуа). Пусть E/F — расширение полей. Следующие условия эквивалентны:

1. E/F — расширение Галуа.
2. E — поле разложения некоторого сепарабельного $f \in F[t]$.
3. $F = E^{\text{Aut}(E/F)}$ и $[E : F] < \infty$.
4. Для некоторой конечной $G \leq \text{Aut}(E)$: $F = E^G$.

Доказательство.

(1) \Rightarrow (2) Аналогично доказательству (следствие 2.1.4). Так как E/F — расширение Галуа, то оно порождено конечным множеством элементов: $E = F[\alpha_1, \dots, \alpha_n]$. Пусть $f_i \in F[t]$ — минимальный многочлен α_i , и пусть $f := f_{i_1} \cdot \dots \cdot f_{i_k}$, где перемножаются уникальные среди f_i .

f сепарабелен, как произведение взаимно простых сепарабельных многочленов, E порождено корнями f , и так как E/F нормально, то f разложим на линейные множители в E . Тем самым, $E = F_f$.

(2) \Rightarrow (3) Согласно (следствие 2.1.4), $|\text{Aut}(E/F)| = [E : F]$. Ясно, что $F \subset \tilde{F} := E^{\text{Aut}(E/F)}$. С другой стороны, по лемме Артина, $[E : \tilde{F}] = |\text{Aut}(E/F)|$, откуда $[\tilde{F} : F] = 1$.

(3) \Rightarrow (4) Согласно (теорема 2.1.7), $[E : F] < \infty \Rightarrow |\text{Aut}(E/F)| < \infty$, тем самым, $G := \text{Aut}(E/F)$ подойдёт.

- (4) \Rightarrow (1) По лемме Артина, $[E : F] = |G|$, тем самым, расширение конечно. Пусть $f \in F[t]$ — неприводимый, имеющий корень $\alpha \in E$. Рассмотрим орбиту α под действием G : $G\alpha = \{\alpha_1, \dots, \alpha_m\}$. Пусть $h(t) := (t - \alpha_1) \cdot \dots \cdot (t - \alpha_m) \in E[t]$. Раскрыв скобки (по теореме Виета)

$$h(t) = t^m - s_1(\alpha_1, \dots, \alpha_m) + s_2(\alpha_1, \dots, \alpha_m) - \dots + (-1)^m s_m(\alpha_1, \dots, \alpha_m)$$

где $s_k(\alpha_1, \dots, \alpha_m)$ — k -й основной симметрический многочлен, то есть сумма всевозможных произведений вида $\alpha_{i_1} \cdot \dots \cdot \alpha_{i_k}$ по всем кортежам $1 \leq i_1 < \dots < i_k \leq m$.

Таким образом, $\forall g \in G : \exists \sigma \in S_m : g(\alpha_i) = \alpha_{\sigma(i)}$. g переставляет α_i , тем самым, коэффициенты h лежат в $E^G = F$, иными словами, $h \in F[t]$. Но раз h раскладывается на различные линейные множители в $E[t]$, то минимальный многочлен α (который делит h) тоже раскладывается на различные линейные множители в $E[t]$. Так как $\alpha \in E$ был произвольным, то E/F по определению сепарабельно и нормально. \square

2.1.4 О сепарабельных расширениях

Следствие 2.1.7. *Расширение, порождённое конечным числом сепарабельных элементов, вкладывается в расширение Галуа (и, следовательно, сепарабельно).*

Доказательство. Аналогично доказательству (следствие 2.1.4). Так как E/F — расширение Галуа, то оно порождено конечным множеством элементов: $E = F[\alpha_1, \dots, \alpha_n]$. Пусть $f_i \in F[t]$ — минимальный многочлены α_i , и пусть $f := f_{i_1} \cdot \dots \cdot f_{i_k}$, где перемножаются уникальные среди f_i .

f сепарабелен, можно устроить вложение $E \hookrightarrow F_f$ (оно есть, например, согласно (следствие 2.1.4)), а F_f — расширение Галуа согласно (теорема 2.1.9). \square

Следствие 2.1.8. *Пусть K/F — расширение полей. Множество элементов K , сепарабельных над F , образует поле.*

Доказательство. $\forall \alpha, \beta \in K : F[\alpha, \beta]$ сепарабельно (следствие 2.1.7), значит, $\alpha + \beta, \alpha\beta$ и даже $\frac{\alpha}{\beta}$ (при $\beta \neq 0$) тоже сепарабельны. \square

Это поле называется *сепарабельным замыканием* F в K . Если опускают K , то подразумевается сепарабельное замыкание в $F^{\text{sep}} \subset F^{\text{alg}}$.

Определение 2.1.16 (Чисто несепарабельное расширение K/E). $\forall \alpha \in K \setminus E$: α не сепарабелен над E .

Следствие 2.1.9. *Любое алгебраическое расширение K/F раскладывается в башню сепарабельного расширения E/F и чисто несепарабельного K/E .*

Доказательство. Выберем за E сепарабельное замыкание F в K . Далее упражнение. \square

Следствие 2.1.10. *Пусть имеется башня расширений $E/K/F$, и E/F — расширение Галуа. Тогда E/K — расширение Галуа.*

Доказательство. Раз E/F — расширение Галуа, то $\exists f \in F[t] : E = F_f$, где f сепарабелен. Тогда $E = K_f$, значит, E/K — действительно расширение Галуа. \square

2.2 Соответствие Галуа

Теперь у нас всё готово, чтобы установить соответствие Галуа.

E/F — расширение Галуа, $G := \text{Gal}(E/F) = \text{Aut}(E/F)$. Пусть $\mathcal{F} := \{K \leq E \mid F \leq K \leq E\}$, и $\mathcal{G} := \{H \leq G\}$. Тогда имеется биекция $\mathcal{F} \leftrightarrow \mathcal{G}$: подполе $K \in \mathcal{F}$ сопоставляется $\text{Gal}(E/K) \leq G$. Обратно, подгруппе $H \in \mathcal{G}$ сопоставляется подполе E^H .

Теорема 2.2.1 (Соответствие Галуа). Указанные выше отображения $\mathcal{F} \leftrightarrow \mathcal{G}$ — взаимно обратные биекции, удовлетворяющие следующим свойствам:

- Монотонность по включению: $H \leq H' \leq G \Rightarrow E^{H'} \leq E^H$.
- При $H \leq H' \leq G : |H : H'| = [E^H : E^{H'}]$.
- $\forall \sigma \in G : \sigma(E^H) = E^{\sigma H \sigma^{-1}}$.
- E^H/F — расширение Галуа $\iff H \trianglelefteq G$. В этом случае $\text{Gal}(E^H/F) \cong G/H$.

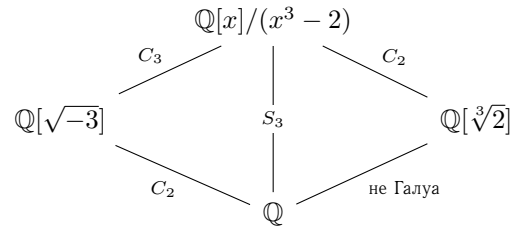
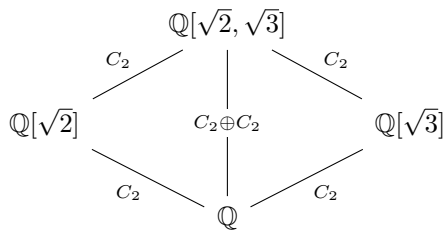
Доказательство.

- $\text{Gal}(E/E^H) = H$ — следствие из леммы Артина.
- $E^{\text{Gal}(E/K)} = K$ согласно (теорема 2.1.9). Согласно ей же, E/K — расширение Галуа.
- По теореме Лагранжа $|H' : H| = \frac{|G:H'|}{|G:H|} = \frac{[E:E^{H'}]}{[E:E^H]} = [E^{H'} : E^H]$.
- $\forall h \in H : \sigma h \sigma^{-1}(\sigma(\alpha)) = \sigma h(\alpha) = \sigma(\alpha) \Rightarrow \sigma(E^H) \leq E^{\sigma H \sigma^{-1}}$. Обратное включение получается заменой $\tilde{H} := \sigma H \sigma^{-1}$ и $\tilde{\sigma} := \sigma^{-1}$.
- $H \trianglelefteq G \iff \forall \sigma \in G : \sigma H \sigma^{-1} = H \iff \forall \sigma \in G : \sigma(E^H) = E^H$. Рассмотрим гомоморфизм $\theta : G \rightarrow \text{Aut}(E^H/F), \sigma \mapsto \sigma|_{E^H}$. Очевидно, $\text{Ker}(\theta) = H$. Покажем, что θ сюръективно. Пусть $\eta \in \text{Aut}(E^H/F)$, покажем, что $\eta \in \text{Im}(\theta)$.

Расширение E/F нормально, значит, $\exists f \in F[t] : E = F_f$. Тогда и подавно $(E^H)_f = E$. Так как $E = (E^H)_f \cong \eta(E^H)_f$, то по теореме о количестве вложений \exists хотя бы одно вложение $E \rightarrow E$ над η . Тем самым, $\text{Aut}(E^H/F) \cong G/H$. Теперь заметим, что $F = E^G = (E^H)^{G/H} \Rightarrow E^H/F$ — расширение Галуа, и $\text{Gal}(E^H/F) \cong G/H$.

Обратно: пусть E^H/F нормально, $\alpha \in E^H$ — корень некоторого многочлена $f \in F[t]$. Тогда $\forall \sigma \in G : \sigma(\alpha)$ — корень f , то есть $\sigma(E^H) = E^H$. С другой стороны, $\sigma(E^H) = E^{\sigma H \sigma^{-1}}$, и так как соответствие Галуа биективно, то $\forall \sigma \in G : \sigma H \sigma^{-1} = H$, то есть $H \trianglelefteq G$. \square

Теперь можно нарисовать некоторые картинки:



Лекция XIII

20 мая 2024 г.

Определение 2.2.1 (Решётка). Частично упорядоченное множество, в котором есть все конечные инфимумы (наибольший элемент, меньший данных) и супремумы (наименьший элемент, больший данных).

Соответствие Галуа устанавливает антиизоморфизм решёток подгрупп и подполей, где порядок индуцирован с включения.

Для K и L — подполей большого поля E — наименьшее поле, содержащее K и L , обозначают $K \cdot L$.

Предложение 2.2.1. Пусть E/F — расширение Галуа, $G := \text{Gal}(E/F)$. Выберем подгруппы $P, Q \leq G$, и соответствующие им поля $K := E^P, L := E^Q$, и рассмотрим следующую башню полей (поле выше — расширение поля ниже):



Если $K/(K \cap L)$ нормально, то и $(K \cdot L)/L$ нормально, причём $\text{Gal}(K \cdot L/L) \cong \text{Gal}(K/K \cap L)$.

Доказательство. Так как $K/K \cap L$ нормально, то $P \trianglelefteq \langle P \cup Q \rangle$. Тем самым, $\langle P \cup Q \rangle = PQ$, и $P \cap Q \trianglelefteq Q$, откуда из соответствия Галуа $K \cdot L/L$ нормально.

Согласно теореме Нётер об изоморфизме

$$\text{Gal}(KL/L) \cong \frac{Q}{Q \cap P} \cong \frac{PQ}{P} \cong \text{Gal}(K/K \cap L) \quad \square$$

Пусть $f \in F[t]$.

Определение 2.2.2 (Группа Галуа многочлена f). $\text{Gal}(f/F) \stackrel{\text{def}}{=} \text{Gal}(F_f/F)$. Если поле F не указано, то логично в качестве него брать наименьшее поле, содержащее коэффициенты многочлена. В характеристике нуль $F = \mathbb{Q}$ (коэффициенты многочлена f).

Пусть имеется расширение E/F , и $f \in F[t] \subset E[t]$. Из определения видно, что $E_f = E \cdot F_f = F_f$ содержит все корни f , а E_f порождено ими над E .

Таким образом, имеет место башня полей



Согласно (предложение 2.2.1), $\text{Gal}(E_f/E) \cong \text{Gal}(F_f/F \cap E) \leq \text{Gal}(F_f/F)$.

Определение 2.2.3 (Разрешимая группа G). Такая группа G , что существует субнормальный ряд с абелевыми факторами $1 = G_0 \trianglelefteq G_1 \dots \trianglelefteq G_n = G$ (факторы ряда — факторгруппы G_{i+1}/G_i).

Лемма 2.2.1. Группа разрешима \iff существует нормальный ряд с абелевыми факторами, то есть ряд $1 = G_0 \trianglelefteq G_1 \dots \trianglelefteq G_n$, где все $G_i \trianglelefteq G$.

Доказательство.

\Leftarrow . Очевидно.

\Rightarrow . Можно построить ряд по алгоритму $G_{i-1} := [G_i, G_i]$. \square

Определение 2.2.4 (Композиционный ряд). Неуплотняемый субнормальный ряд без повторений. Неуплотняемость означает, что любой фактор — простая (без нормальных подгрупп) группа.

В самом деле, если $H \trianglelefteq G_{i+1}/G_i$, то $\pi_{G_i}^{-1}(H)$ можно вставить в ряд между G_i и G_{i+1} .

Лемма 2.2.2. Любые два композиционных ряда эквивалентны. Любые два субнормальных ряда обладают эквивалентными уплотнениями. Факторы композиционного ряда изоморфны циклическим группам простого порядка.

Лемма 2.2.3. Пусть $|G| = p^n$. Тогда $\exists H \trianglelefteq G : |G : H| = p$.

Доказательство. Пусть $n \geq 1$. Центр $C \leq G$ p -группы нетривиален, значит, $\pi_C(G) = G/C$ имеет порядок строго меньше p^n . По индукции в ней есть подгруппа $\tilde{H} \trianglelefteq G/C$ индекса p , тогда $|G : \pi_C^{-1}(\tilde{H})| = p$. \square

Теорема 2.2.2 (ФТНА). $\mathbb{C} = \mathbb{R}[\sqrt{-3}]$ алгебраически замкнуто.

Доказательство. Рассмотрим конечное расширение E/\mathbb{C} , тогда расширение E/\mathbb{R} тоже конечно. Вложим его в нормальное расширение E'/\mathbb{C} .

$G := \text{Gal}(E'/\mathbb{R})$, пусть $|G| = 2^k \cdot m$, где m нечётно. Пусть P — силовская 2-подгруппа в G : $|G : P| = m$. Так как $[E' : \mathbb{R}] = 2^k \cdot m$ и $[E' : E'^P] = |P| = 2^k$, то $[E'^P : \mathbb{R}] = m$.

Рассмотрим $\alpha \in E'^P$, пусть $f \in \mathbb{R}[t]$ — минимальный многочлен α . Тогда $[\mathbb{R}[\alpha] : \mathbb{R}] = \deg f \mid m$, откуда $\deg f$ нечётна. Но f неприводим над \mathbb{R} , а он нечётной степени. Используя соображения непрерывности и полноты \mathbb{R} , получаем, что $\deg f = 1$, то есть $\alpha \in \mathbb{R}$. Тем самым, $E'^P = \mathbb{R}$, соответствие Галуа говорит, что $P = G$.

$\text{Gal}(E'/\mathbb{C}) \leq \text{Gal}(E'/\mathbb{R})$, откуда $\text{Gal}(E'/\mathbb{C})$ — тоже 2-группа. Согласно (лемма 2.2.3), найдётся $H \trianglelefteq \text{Gal}(E'/\mathbb{C})$ индекса 2.

Тогда $[E'^H : \mathbb{C}] = 2$, но у \mathbb{C} нет расширений степени 2 — любой квадратный многочлен над \mathbb{C} разложим в \mathbb{C} на линейные множители. Тем самым, $\text{Gal}(E'/\mathbb{C})$ тривиальна, откуда $E' = \mathbb{C}$, и у \mathbb{C} нет никаких конечных расширений. \square

Лекция XIV

21 мая 2024 г.

Теорема 2.2.3 (Дирихле, о линейной независимости характеров). Пусть H — группа, E — поле, и $\sigma_1, \dots, \sigma_n : H \rightarrow E^*$ — различные групповые гомоморфизмы. Утверждается, что $\sigma_1, \dots, \sigma_n$ линейно независимы над E в пространстве всех функций $H \rightarrow E$.

Доказательство. Предположим наличие линейной зависимости:

$$\forall h \in H : \sum_{i=1}^n \alpha_i \sigma_i(h) = 0, \text{ где } \alpha_i \in E \quad (\diamond)$$

Выберем самую короткую такую (с наименьшим n), в ней в частности все $\alpha_i \neq 0$.

Пусть $g \in H$ таков, что $\sigma_n(g) \neq \sigma_{n-1}(g)$. Запишем

$$\begin{cases} \sum_{i=1}^n \alpha_i \sigma_i(g) \sigma_i(h) = 0 \\ \sum_{i=1}^n \alpha_i \sigma_n(g) \sigma_i(h) = 0 \end{cases}$$

где первое получено подстановкой $h \leftarrow gh$ в (\diamond) , а второе — домножением (\diamond) на $\sigma_n(g)$. Вычитая, получаем линейную зависимость меньшей длины:

$$\sum_{i=1}^n \alpha_i (\sigma_i(g) - \sigma_n(g)) \sigma_i(h) = 0$$

При этом зависимость нетривиальна, так как $\alpha_{n-1}(\sigma_{n-1}(g) - \sigma_n(g)) \neq 0$. \square

Часто эту теорему применяют для $H = E^*$, $\sigma_i \in \text{Gal}(E/F)$: пусть E/F — расширение Галуа, пусть $n := [E : F]$, $\{\sigma_1, \dots, \sigma_n\} = \text{Gal}(E/F) \leq \text{End}(E/F) \stackrel{\text{def}}{=} \text{End}_F(E)$.

Тогда $\dim_E(\langle \text{Gal}_F(E) \rangle) = n$ — по теореме Дирихле (теорема 2.2.3) все эндоморфизмы вида $\sum_{i=1}^n \alpha_i \sigma_i$ различны. С другой стороны, $\dim_F(\text{End}_F(E)) = n^2$, так как $\dim_F(E) = n$, откуда $\langle \text{Gal}_F(E) \rangle = \text{End}_F(E)$, то есть $\sigma_1, \dots, \sigma_n$ — E -базис пространства $\text{End}_F(E)$.

Расширение называется тем же словом, что и его группа — так, бывают, *абелевы, циклические, разрешимые* расширения, и тому подобное.

Определение 2.2.5 ($\varepsilon \in F$ — первообразный корень n -й степени из 1). $\begin{cases} \varepsilon^n = 1 \\ \varepsilon^k \neq 1, & 0 < k < n \end{cases}$.

Если в поле есть первообразный корень степени n , то $\text{char } F \nmid n$: если $n = pm$, то $0 = \varepsilon^{pm} - 1 = (\varepsilon^m - 1)^p$, откуда ε — не первообразный.

Несложно видеть, что $\varepsilon^k = \varepsilon^m \iff k \equiv m \pmod{n}$, откуда $\varepsilon^0, \varepsilon, \dots, \varepsilon^{n-1}$ — корни n -й степени из единицы, и многочлен $t^n - 1$ раскладывается на линейные множители. Обозначим множество корней этого многочлена $\mu_n(F)$.

Лемма 2.2.4. Пусть E/F — расширение полей, и в базовом поле F есть первообразный корень степени n из 1. Следующие условия эквивалентны.

1. $E = F[\alpha]$, где $\alpha^n \in F$, и $\alpha^k \notin F$ при $0 < k < n$.
2. Расширение E/F циклическое расширение Галуа (то есть $\text{Gal}(E/F) \cong C_n$).

Доказательство.

(1) \Rightarrow (2) Многочлен $f(t) = t^n - \alpha^n \in F[t]$ имеет n различных корней $\{\alpha \varepsilon^k \mid 0 \leq k < n\}$, откуда $E = F_f$ для сепарабельного f , то есть E/F — расширение Галуа.

- Устроим отображение $\theta : \text{Gal}(E/F) \rightarrow E^*, \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$. Так как $\left(\frac{\sigma(\alpha)}{\alpha}\right)^n = \frac{\sigma(\alpha)^n}{\alpha^n} = \frac{\sigma(\alpha^n)}{\alpha^n} = \frac{\alpha^n}{\alpha^n} = 1$, то $\text{Im } \theta \subset \mu_n(F)$.
- Проверим, что это гомоморфизм групп.

$$\theta(\tau\sigma) = \frac{\tau\sigma(\alpha)}{\alpha} = \frac{\sigma(\tau(\alpha))}{\tau(\alpha)} \cdot \frac{\tau(\alpha)}{\alpha} \quad (\equiv)$$

Так как $\tau(\alpha)$ — корень f , то $\tau(\alpha) = \varepsilon^m \alpha$ для некоторого $m \in \mathbb{N}$. Сокращая на $\varepsilon^m \in F$, получаем

$$(\equiv) \frac{\sigma(\alpha)}{\alpha} \cdot \frac{\tau(\alpha)}{\alpha} = \theta(\sigma)\theta(\tau) = \theta(\tau)\theta(\sigma)$$

- Проверим сюръективность. Любая собственная подгруппа μ_n имеет вид μ_k , где $k \mid n$, и если $\exists k \in \mathbb{N} : \forall \sigma \in \text{Gal}(E/F) : \frac{\sigma(\alpha)^k}{\alpha^k} = 1$, то $\forall \sigma \in \text{Gal}(E/F) : \sigma(\alpha^k) = \alpha^k$, то есть $\alpha^k \in F$. Получаем, что $k \geq n$.
- С одной стороны, $|\text{Gal}(E/F)| \geq n$ из сюръективности, с другой стороны, $[E : F] \leq n$, откуда $|\text{Gal}(E/F)| = [E : F] = n$, и из количественных соображений θ — изоморфизм.

(2) \Rightarrow (1) Пусть σ — образующая группы Галуа ($\text{Gal}(E/F) = \{1, \sigma, \dots, \sigma^{n-1}\}$). По теореме Дирихле (теорема 2.2.3), $\sum_{k=0}^{n-1} \varepsilon^k \sigma^k \neq 0$, тем самым, $\exists \beta \in E : \alpha := \sum_{k=0}^{n-1} \varepsilon^k \sigma(\beta)^k \neq 0$.

- Посчитаем

$$\sigma(\alpha) = \sum_{k=0}^{n-1} \varepsilon^k \sigma(\beta)^{k+1} = \sum_{i=1}^n \varepsilon^{i-1} \sigma(\beta)^i = \varepsilon^{-1} \alpha$$

Тем самым, $\sigma(\alpha^k) = \sigma(\alpha)^k = (\varepsilon^{-1} \alpha)^k = \varepsilon^{-k} \alpha^k$. В частности, α^n неподвижен под действием $\text{Gal}(E/F)$, и $\alpha^n \in F$.

– Покажем линейную независимость $1, \alpha, \dots, \alpha^{n-1}$ над F , из количественных соображений будет следовать, что это базис E над F . Пусть $\sum_{k=0}^{n-1} \alpha^k x_k = 0$ для неких $x_k \in F$.

Применяя σ^j к данному равенству, получаем $\sum_{k=0}^{n-1} \varepsilon^{-kj} \alpha^k x_k = 0$. При $j = 0, \dots, n-1$ получаются n линейных уравнений с переменными $\alpha^k x_k$. Матрица коэффициентов системы $(\varepsilon^{-kj})_{j=0..n-1}^{k=0..n-1}$ невырождена, так как её определитель — определитель Вандермонда — не нуль. \square

Лемма 2.2.5. Пусть $E := F[\varepsilon]$, где ε — первообразный корень степени n . Тогда E/F — расширение Галуа, и $\text{Gal}(E/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ (в частности, расширение E/F абелево).

Доказательство. Так как $\mu_n = \langle \varepsilon \rangle$, то $t^n - 1$, раскладывается на линейные множители в $F[\varepsilon]$, то есть $F[\varepsilon] = F_{t^n-1}$. Всякий элемент $\sigma \in \text{Gal}(E/F)$ однозначно определён значением $\sigma(\varepsilon)$ (так как $E = F[\varepsilon]$), при этом так как преобразование σ обратимо, то $\sigma(\varepsilon)$ — тоже первообразный корень степени n из 1.

Устроим $\pi : \text{Gal}(E/F) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, сопоставляя элементу $\sigma \in \text{Gal}(E/F)$ такой показатель $k \in \mathbb{Z}/n\mathbb{Z}$, что $\sigma(\varepsilon) = \varepsilon^k$. Инъективность σ очевидна: $\sigma(\varepsilon) = \tau(\varepsilon) \Rightarrow \sigma = \tau$. Очевидно, это гомоморфизм моноидов, и так как образ обратимых элементов обратим, то $\pi : \text{Gal}(E/F) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ — гомоморфизм групп. \square

Определение 2.2.6 (Круговой многочлен степени n). $\Phi_n(t) \stackrel{\text{def}}{=} \prod_{\varepsilon} (t - \varepsilon)$, где ε пробегает все первообразные корни степени n из 1 по одному разу.

Так как любой корень степени n из 1 — первообразный степени $k \mid n$, то $\prod_{k \mid n} \Phi_k(t) = \prod_{\varepsilon^n=1} (t - \varepsilon) = t^n - 1$.

Интересный факт. Для любого поля с первообразным корнем степени n из единицы $\Phi_n \in \mathbb{Z}[t] \leq \mathbb{Q}[t]$, и там он неприводим, степени $\phi(n)$ (где ϕ — euler totient function).

Пусть $f \in F[t]$ — ненулевой многочлен.

Определение 2.2.7 (Уравнение $f = 0$ разрешимо в радикалах). Все корни f (лежащие в алгебраическом замыкании F) выражаются через элементы F при помощи арифметических операций и извлечений корня. Иными словами, существуют цепочка полей $F = F_0 \hookrightarrow F_1 \hookrightarrow \dots \hookrightarrow F_m$, где в F_m многочлен f раскладывается на линейные множители, и $F_i = F_{i-1}[\alpha_i]$, где $\beta := \alpha_i^k \in F_{i-1}$. В таком случае ещё пишут $F_i = F_{i-1}[\sqrt[n]{\beta_i}]$.

Теорема 2.2.4 (Абель — Руффини). Пусть F поле, $\text{char } F = 0$; ненулевой $f \in F[t]$. Следующие условия эквивалентны:

1. Уравнение $f = 0$ разрешимо в радикалах.
2. $\text{Gal}(F_f/F)$ разрешима.

Доказательство.

\Leftarrow . Сначала присоединим к F первообразный корень из 1 достаточно большой степени — подойдёт первообразный корень ε степени $(\deg f)!$. Положим $F_1 := F[\varepsilon]$. Иными словами, $F_1 := F_{t^{(\deg f)!}-1}$. Это расширение Галуа, так как $\text{char } F = 0$.

$\text{Gal}(f/F_1) \leq \text{Gal}(f/F)$, поэтому $G := \text{Gal}(f/F_1)$ тоже разрешима. По определению у неё существует субнормальный ряд, и **видимо так как G конечна** его можно уплотнить до композиционного $\{1\} = G_m \triangleleft G_{m-1} \triangleleft \dots \triangleleft G_1 = G$. Факторгруппы G_i/G_{i+1} — простые абелевы группы, то есть циклические, простого порядка. Положим $F_i := ((F_1)_f)^{G_i}$.

Согласно (лемма 2.2.4), F_i имеет вид $F_{i-1}[\alpha_i]$, что по определению означает разрешимость в радикалах.

\Rightarrow . По условию существует башня полей $F \hookrightarrow F_1 \hookrightarrow \dots \hookrightarrow F_m$, где f раскладывается на линейные множители в F_m , и $F_i = F_{i-1}[\alpha_i]$, где $\alpha_i^{k_i} \in F_{i-1}$. Для применения (лемма 2.2.4) недостаёт первообразного корня.

Добавим его: $F_{m+1} := (F_m)_{t^{k-1}}$, где $k := k_1 \cdot \dots \cdot k_m$. Далее хотим получить, что $\text{Gal}(f/F)$ разрешима. Понятно, что $F_f \subset F_m$, поэтому достаточно доказать, что $\text{Aut}(F_m/F)$ разрешима, или даже $\text{Aut}(F_{m+1}/F)$ разрешима — факторгруппа разрешимой группы разрешима. В доказательстве будет использоваться соответствие Галуа, для этого дополним F_{m+1}/F до нормального: пусть E/F нормально, и $F_{m+1} \subset E$ (например, E — поле разложения минимального многочлена, аннулирующего все элементы $\varepsilon, \alpha_1, \dots, \alpha_m$).

Пусть $\text{Gal}(E/F) = \{\sigma_1, \dots, \sigma_n\}$. Поле $\tilde{E} = F[\varepsilon, \sigma_i(\alpha_j)] \subset E$ тоже нормально над F , так как оно устойчиво под действием $\text{Gal}(E/F)$. А для этого поля есть хорошая цепочка (порождающие присоединяются по одному, все образы α_{j+1} добавляются после всех образов α_j):

$$F \subset F[\varepsilon] \subset F[\sigma_1(\alpha_1)] \subset F[\sigma_1(\alpha_1), \sigma_2(\alpha_1)] \subset \dots \subset \tilde{E}$$

Все промежуточные расширения абелевы (первое вкладывается в $(\mathbb{Z}/n\mathbb{Z})^*$ согласно (лемма 2.2.5), остальные циклические согласно (лемма 2.2.4)). Соответствие Галуа говорит, что этой башне полей соответствует субнормальный ряд группы $\text{Gal}(\tilde{E}/F)$ с абелевыми факторами, то есть $\text{Gal}(\tilde{E}/F)$ разрешима. Её факторгруппа $\text{Gal}(F_f/F)$ тоже разрешима. \square