Алгебра. Неофициальный конспект

Лектор: Алексей Владимирович Степанов
Конспектировал Леонид Данилевич

IV семестр, весна 2024 г.

Оглавление

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 $\mathscr{A}$)**.** $\forall A, B \in \mathscr{A} : \mathrm{Mor}_{\mathscr{A}}(A, B)$ образует абелеву группу, и везде, где определена, выполнена дистрибутивность:

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

Определение 1.1.2 (Бипроизведение $A, B \in \mathscr{A}$)**.** Такая диаграмма $A \underset{i_1}{\overset{\pi_1}{\leftrightarrows}} C \underset{i_2}{\overset{\pi_2}{\rightleftarrows}} B$, что

1. $\pi_1 i_1 = \mathrm{id}_A$.
2. $\pi_2 i_2 = \mathrm{id}_B$.
3. $i_2\pi_2 + i_1\pi_1 = \mathrm{id}_C$.
4. $\pi_2 i_1 = 0$.
5. $\pi_1 i_2 = 0$.

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

$$\mathrm{Mor}_{\mathscr{Arr}\mathscr{C}}(\phi, \psi) = \{(\alpha, \beta) | \alpha : \mathrm{source}(\phi) \to \mathrm{source}(\psi), \beta : \mathrm{target}(\phi) \to \mathrm{target}(\psi), \beta\phi = \psi\alpha\}$$

то есть множество коммутативных диаграмм следующего вида:

$$\begin{tikzcd} \bullet \arrow[r, "\phi"] \arrow[d, "\alpha"] & \bullet \arrow[d, "\beta"] \\ \bullet \arrow[r, "\psi"] & \bullet \end{tikzcd}$$

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

Лемма 1.1.1. $\ker, \operatorname{coker}$ — *функторы* $\mathscr{Arr}\mathscr{A} \to \mathscr{Arr}\mathscr{A}$ *(то есть лемма утверждает, что можно определить действие не только на объектах, но и на морфизмах).*

Доказательство. Достаточно доказать для ядер, для коядер двойственно.

Определим действие ker на морфизмах. Пусть (α, β) — морфизм между $f, f' \in \mathscr{Arr}\mathscr{A}$:

$$\begin{tikzcd} \operatorname{Ker} f \arrow[r, "\ker f"] \arrow[d, dashed, "\exists! \phi"] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[d, "\beta"] \\ \operatorname{Ker} f' \arrow[r, "\ker f'"] & A' \arrow[r, "f'"] & B' \end{tikzcd}$$

Тогда $f \cdot \ker f = 0$, откуда $\beta \cdot f \cdot \ker f = 0$, а из коммутативности $f' \cdot \alpha \cdot \ker f = 0$. 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 $\mathscr{A}$: $\exists R \in \mathscr{Ring}$ (необязательно коммутативное кольцо с единицей) и строгий, полный, точный функтор $\mathscr{A} \to \mathscr{mod}\text{-}R$.

Иными словами, всякую абелеву категорию можно себе мыслить, как *полную подкатегорию* в категории $\mathscr{mod}\text{-}R$ (то есть категорию $\mathscr{C}$, в которой $\operatorname{Obj}\mathscr{C} \subset \operatorname{Obj}\mathscr{mod}\text{-}R$, и $\forall A, B \in \operatorname{Obj}\mathscr{C}$: $\operatorname{Mor}_{\mathscr{C}}(A, B) = \operatorname{Mor}_{\mathscr{mod}\text{-}R}(A, B)$) для некоторого кольца R. Неформально это означает, что все факты, которые можно доказать для категории модулей, будут верны и для данной абелевой категории. Мы часто будем использовать теорему Фрейда — Митчелла, чтобы доказать какой-то факт про все абелевы категории, используя конкретность категории модулей.

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

$$\begin{tikzcd} \operatorname{Ker} f \arrow[r, "\ker f"] & A \arrow[rr, "f"] \arrow[d, "\operatorname{coker}\ker f"'] & & B \arrow[r, "\operatorname{coker} f"] & \operatorname{CoKer} f \\ & \operatorname{CoKer}\ker f \arrow[rr, dashed, "\exists!"] & & \operatorname{Ker}\operatorname{coker} f \arrow[u, "\ker\operatorname{coker} f"'] & \end{tikzcd}$$

Более того, в абелевой категории эта стрелка — изоморфизм.

Доказательство. Само построение пунктирной стрелки легко получается из универсальных свойств ядра и коядра, а доказательство того, что это — изо — непростое.

Из теоремы Фрейда — Митчелла это очевидно: для $f : A \to B$: с одной стороны, $\operatorname{CoKer}\ker f =$ $A/\operatorname{Im}(\ker f) = A/\operatorname{Ker} f$, а с другой стороны $\operatorname{Ker}\operatorname{coker} f = \operatorname{Ker}(\operatorname{coker} f) = \operatorname{Im}(A)$, и, конечно, $\operatorname{Im}(A) \cong A/\operatorname{Ker}(f)$.

Также это можно обосновать, исходя из эпи-моно разложения, полученного на прошлой лекции. Там было построено, что $f = \varepsilon \cdot \ker\operatorname{coker} f$ (для какого-то эпиморфизма ε) — эпи-моно разложение.

Двойственно $f = \mu \cdot \operatorname{coker}\ker f$ (для какого-то мономорфизма μ) — тоже эпи-моно разложение, и дальше можно воспользоваться функториальностью эпи-моно разложения:

$$\begin{tikzcd}
\bullet \arrow[r, "\varepsilon"] \arrow[d, leftrightarrow, "\mathrm{id}"'] & \bullet \arrow[r, "\ker\operatorname{coker} f"] \arrow[d, dashed, shift left, "\zeta"] & \bullet \arrow[d, leftrightarrow, "\mathrm{id}"] \\
\bullet \arrow[r, "\operatorname{coker}\ker f"] & \bullet \arrow[u, dashed, shift left, "\xi"] \arrow[r, "\mu"] & \bullet
\end{tikzcd}$$

В его силу найдутся такие стрелки ξ и ζ, что все квадраты коммутативны. Значит, ξ подходит в качестве пунктирной стрелки в утверждении предложения. При этом ξ — изо, так как $\xi\zeta = \mathrm{id}$ (из коммутативности квадратов $\xi \cdot \operatorname{coker}\ker f = \varepsilon$ и $\zeta \cdot \xi \cdot \operatorname{coker}\ker f = \zeta \cdot \varepsilon = \operatorname{coker}\ker f$, но $\operatorname{coker}\ker f$ — эпиморфизм, поэтому $\zeta \cdot \xi = \mathrm{id}$) и $\zeta\xi = \mathrm{id}$ (аналогично) $\square$

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

- *$\mathscr{C}$ является абелевой.*
- – *$0_{\mathscr{A}} \in \mathscr{C}$, здесь, как обычно, $0_{\mathscr{A}}$ — нулевой объект категории $\mathscr{A}$.*
  – *$\mathscr{C}$ содержит бипроизведение любых двух своих объектов.*
  – *Ядра и коядра (взятые в $\mathscr{A}$) любых морфизмов из $\mathscr{C}$ лежат в $\mathscr{C}$.*

Доказательство.

$\Leftarrow$. Достаточно проверить все свойства определения абелевой категории. Они все сразу следуют, в частности, любой мономорфизм μ в $\mathscr{C}$ нормален, так как он является ядром $\operatorname{coker}\mu$ (что следует либо из леммы, доказанной при построении эпи-моно разложения, либо из теоремы Фрейда — Митчелла).

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

1.2 Компле́ксы

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

Определение 1.2.1 (Компле́кс)**.** 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 $(\mathbb{Z}, \geqslant)$ (полученной из частично упорядоченного множества) в $\mathscr{A}$ (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: в абстрактной категории объекты не сравнимы на $\subset$.

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

Так же, как видно из определения, в данной категории должны быть счётные бипроизведения (прямые суммы), иначе градуированного объекта может не быть.

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.

1.2.1 Морфизмы комплексов

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

$$\begin{tikzcd} A_{n+1} \arrow[r, "d_n^A"] \arrow[d, "f"] & A_n \arrow[d, "f"] \\ B_{n+1} \arrow[r, "d_n^B"] & B_n \end{tikzcd}$$

На языке абелевых категорий, надо рассматривать не одно отображение f, так как отношение $f(A_n) \subset B_n$ не выражается, а серию морфизмов $\{f_n : A_n \to B_n\}_{n\in\mathbb{Z}}$.

Для всякого морфизма f коммутативна диаграмма в категории комплексов:

$$\begin{tikzcd} A[1] \arrow[r, "d^A"] \arrow[d, "{f[1]}"] & A \arrow[d, "f"] \\ B[1] \arrow[r, "d^B"] & B \end{tikzcd}$$

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

Теорема 1.2.1. Категория комплексов абелева.

Доказательство.

> **Лемма 1.2.1.** *Если $\mathscr{C}$ — малая категория, $\mathscr{A}$ — абелева, то* $\mathrm{Func}(\mathscr{C}, \mathscr{A})$ *— тоже абелева категория.*
>
> *Доказательство леммы.*
>
> Морфизмы в данной категории — естественные преобразования между функторами, и их сложение устроено поточечно: $\forall \eta, \zeta : \mathscr{F} \to \mathscr{G}, \forall A \in \mathscr{A} : (\eta + \zeta)_A = \eta_A + \zeta_A$.
>
> Нулевой объект — функтор $\mathbb{0}$, сопоставляющий каждому объекту $0_{\mathscr{A}}$, и каждой стрелке — нуль-стрелку.
>
> Для двух функторов $\mathscr{F}, \mathscr{G}$ имеется их бипроизведение: $(\mathscr{F} \oplus \mathscr{G})(C) = \mathscr{F}(C) \oplus \mathscr{G}(C)$.
>
> Если $\eta \in \mathrm{Mor}_{\mathrm{Func}(\mathscr{C},\mathscr{A})}(\mathscr{F}, \mathscr{G})$ (то есть η — естественное преобразование $\mathscr{F} \to \mathscr{G}$), то $(\mathrm{Ker}\,\eta)(C) = \mathrm{Ker}(\eta_C)$.
>
> ker определяется аналогично лемме (лемма 1.1.1). Аналогично с коядрами.
>
> Далее по-хорошему надо проверить, что выполняются все универсальные свойства, и что любой мономорфизм нормален, но мы этого делать не будем. □

Ссылаемся на (лемма 1.1.2), рассматривая категорию комплексов, как полную подкатегорию в категории функторов. Нулевой объект — комплекс, состоящий из нулей — в категории комплексов имеется. Бипроизведением комплексов $A_\bullet$ и $B_\bullet$ является комплекс $(A \oplus B)_\bullet$, у которого $(A \oplus B)_n = A_n \oplus B_n$, и $d_n^{A\oplus B} = d_n^A \oplus d_n^B$:

$$\cdots \longrightarrow A_{n+1} \xrightarrow{d_n^A} A_n \xrightarrow{d_{n-1}^A} A_{n-1} \longrightarrow \cdots$$

$$\cdots \longrightarrow B_{n+1} \xrightarrow{d_n^B} B_n \xrightarrow{d_{n-1}^B} B_{n-1} \longrightarrow \cdots$$

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

Если $d_{n-1}^A \cdot d_n^A = 0$, и $d_{n-1}^B \cdot d_n^B = 0$, то (из теоремы Митчелла уж точно очевидно) $d_{n-1}^{A\oplus B} \cdot d_n^{A\oplus B} = 0$.

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

1.3 Гомологии

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

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_n"] \arrow[d, "d_n"] & C_n \arrow[r] \arrow[d, "d_{n-1}"] & \cdots \\
\cdots \arrow[r] & C_n \arrow[r, "d_{n-1}"] & C_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

Ниже мы по произвольному комплексу C строим новые комплексы.

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

В конкретной категории в n-й компоненте комплекса циклов лежит подмодуль C_n, при взятии дифференциала обращающийся в нуль: $Z(C)_n = \operatorname{Ker} d[-1]_n = \operatorname{Ker} d_{n-1} \subset C_n$.

Определение 1.3.2 (Границы)**.** Комплекс $B = B(C) \overset{def}{=} \operatorname{Im} d$.

В конкретной категории в n-й компоненте комплекса границ лежит подмодуль C_n, являющийся образом дифференциала: $B(C)_n = \operatorname{Im} d_n \subset C_n$.

Определения циклов и границ имеют смысл и для абстрактных абелевых категорий. В них, *образ* — это ядро коядра: $\operatorname{Im}\phi \overset{def}{=} \operatorname{Ker}(\operatorname{coker}\phi)$. В абелевой категории канонически $\operatorname{Im}\phi \cong \operatorname{CoIm}\phi \overset{def}{=} \operatorname{CoKer}(\ker\phi)$, так что образ можно определять и так.

На языке конкретных категорий, так как $d^2 = 0$, то $B_n \subset Z_n$, и можно определить фактормодуль $H_n \coloneqq Z_n/B_n$ — *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.

Построение H в терминах универсальных свойств. Пусть C — произвольный комплекс, $Z = Z(C)$, $B = B(C)$. Изобразим следующую диаграмму в категории комплексов, где $z : Z(C) \to C$ вкладывает ядра, а $\operatorname{coker} z = b : C[1] \to B$ — факторизация по этому вложению:

$$\begin{tikzcd}
Z[1] \arrow[r, "z{[1]}"] & C[1] \arrow[r, "d"] \arrow[d, "b"'] \arrow[dr, dashed, "\alpha"] & C \arrow[r, "d{[-1]}"] & C[-1] \\
 & B \arrow[r, dotted, "\beta"'] & Z \arrow[u, "z"'] \arrow[r, dotted, "\operatorname{coker}\beta"'] & H \arrow[r, dotted] & 0
\end{tikzcd}$$

Так как $d[-1] \cdot d = 0$, то можно пропуститься 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 пропуститься через коядро, то есть $\exists! \beta : \beta b = \alpha$. Далее H определяется, как коядро β. □

Взятие циклов, границ и гомологий функториально (то есть циклы, границы и даже гомологии являются функторами, бьющими из категории комплексов в неё же). Например, для морфизма комплексов образуется соответствующий морфизм комплексов их гомологий. Это сразу следует из функториальности взятия ядер и коядер.

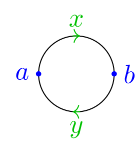
Следствие 1.3.1. *В комплексах Z, B, H нулевые дифференциалы.*

Доказательство. Из диаграммы следует, что в комплексе Z нулевые дифференциалы. Это неудивительно — Z, как комплекс ядер, имеет дифференциалы, получаемые ограничением d_n, на при ограничении d_n на своё ядро получается нуль:

$$\begin{tikzcd}
\cdots \arrow[r] & \operatorname{Ker}(d_n) \arrow[r] \arrow[d] & \operatorname{Ker}(d_{n-1}) \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_n"] & C_n \arrow[r] & \cdots
\end{tikzcd}$$

B состоит из подмодулей в Z, H — из фактормодулей, понятно, что там дифференциалы тоже нулевые. □

1.3.1 Гомологии окружности

- Рассмотрим окружность, как симплициальное множество, склеенное из двух нульмерных клеток-точек $\{a, b\}$, и двух одномерных клеток-отрезков $\{x, y\}$: 

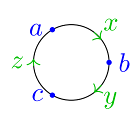
  Построим $C_0 = \mathbb{Z}a + \mathbb{Z}b$ — свободная абелева группа на $\{a, b\}$, $C_1 = \mathbb{Z}x + \mathbb{Z}y$ — тоже свободная абелева группа, но на образующих $\{x, y\}$. Вместо $\mathbb{Z}$ можно было взять любое другое кольцо.

  Получили так называемый *симплициальный комплекс* для данного разбиения окружности на клетки (все остальные элементы комплекса объявляются нулями):

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

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

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

- Теперь триангулируем окружность по-другому: 

 $\begin{cases} d_1(x) = b - a, \\ d_1(y) = c - b, \\ d_1(z) = a - c \end{cases}$.

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

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: $AB + BC + CA$.*

1.3.2 Длинная точная последовательность гомологий

Напомним, что комплекс называется *точным*, если не просто $d_n \cdot d_{n+1} = 0$, но и сразу $\mathrm{Im}(d_{n+1}) = \mathrm{Ker}(d_n)$. Часто встречаются *короткие точные последовательности* — последовательности вида $0 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 0$. Точность в члене A означает, что i — моно, точность в члене C означает, что π — эпи, а в члене B — что $\mathrm{Im}(i) = \mathrm{Ker}(\pi)$, то есть (в элементах) $\forall x \in B : \pi(x) = 0 \iff x \in \mathrm{Im}(i)$.

Теорема 1.3.1 (Длинная точная последовательность гомологий)**.** Пусть имеется точная последовательность комплексов $0 \to A' \xrightarrow{i} A \xrightarrow{\pi} A'' \to 0$.

Тогда существует длинная точная последовательность гомологических групп

$$\cdots \longrightarrow H' \xrightarrow{\ i\ } H \xrightarrow{\ \pi\ } H'' \xrightarrow{\ \delta\ } H'[-1] \xrightarrow{i[-1]} H[-1] \longrightarrow \cdots$$

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. Для $z \in Z''_n$, обозначим за $[z]$ класс z в H''_n.

$$\begin{tikzcd}
0 \arrow[r] & A'_n \arrow[r, "i_n"] \arrow[d, "d'_n"'] & A_n \arrow[r, "\pi_n"] \arrow[d, "d_n"] & A''_n \arrow[r] \arrow[d, "d''_n"] & 0 \\
0 \arrow[r] & A'_{n-1} \arrow[r, "i_{n-1}"] & A_{n-1} \arrow[r, "\pi_{n-1}"] & A''_{n-1} \arrow[r] & 0
\end{tikzcd}$$

Рассуждения ниже обычно называют *диаграммный поиск*. Кажется, это невозможно ни записывать, ни читать, но для полной картины пусть будет.

- Для начала построим $\delta : H''_n \to H'_{n-1}$.
  - Выберем $z \in \mathrm{Ker}(d''_n)$, пусть $y \in \pi_n^{-1}(z)$ — произвольный прообраз. $\bar{y} \coloneqq d_n(y)$ лежит в ядре π_{n-1} из коммутативности правого квадрата. Из точности нижней строки $\exists \bar{x} \in i_{n-1}^{-1}(\bar{y})$ (и он единственен, так как i_{n-1} — моно), положим $\delta([z]) \coloneqq [\bar{x}]$.
  - Убедимся, что определение не зависит от выбора $y \in \pi_n^{-1}(z)$. Для этого рассмотрим другой $y' \in \pi_n^{-1}(z)$. Так как $\pi_n(y - y') = 0$, то из точности верхней строки $\exists x \in i_n^{-1}(y-y')$. Из коммутативности левого квадрата: $d'_n(x) = i_{n-1}^{-1}(d_n(y-y')) = i_{n-1}^{-1}(d_n(y)) - i_{n-1}^{-1}(d_n(y'))$, то есть $\bar{x}$ определён с точностью до $\mathrm{Im}(d'_n)$, а его класс эквивалентности в гомологиях — однозначно.
  - Очевидно, что δ линеен: его можно задать формулой $i_{n-1}^{-1}(d(\pi_n^{-1}(\_)))$, где берётся любой прообраз. Для всякого R-линейного $f : x_1 \in f^{-1}(y_1), x_2 \in f^{-1}(y_2) \Rightarrow \forall \alpha, \beta \in R : \alpha x_1 + \beta y_1 \in f^{-1}(\alpha x_2 + \beta y_2)$, то есть прообразы можно выбирать линейно.
- Убедимся, что полученная длинная точная последовательность гомологических групп точна. Здесь используются определённые при построении δ элементы $y \in A_n$ и $\bar{y} \in A_{n-1}, \bar{x} \in A'_{n-1}$.
  - $\forall z \in \mathrm{Ker}(d''_n) : \delta([z]) = 0 \iff \bar{y} = 0 \iff y \in \mathrm{Ker}(d_n)$. Отсюда $\delta([z]) = 0 \iff z \in \pi_n(\mathrm{Ker}(d_n))$, что означает точность в члене H''_n.
  - С одной стороны, $\forall \bar{x} \in \mathrm{Ker}(d'_{n-1}) : i_{n-1}(\bar{x}) \in \mathrm{Im}(d_n) \Rightarrow \exists y \in A_n : i_{n-1}(\bar{x}) = d_n(y) \Rightarrow \bar{x} = \delta([\pi_n(y)])$ (δ определена, так как $\pi_n(y) \in \mathrm{Ker}(d''_n)$ — из коммутативности правого квадрата: $d''_n(\pi_n(y)) = \pi_{n-1}(\bar{y})$, а из точности нижней строки это нуль). С другой стороны, $\forall z \in \mathrm{Ker}(d''_n) : i_{n-1}(\delta([z])) = d_n(y) \in \mathrm{Im}(d_n)$. Это означает точность в члене H'_{n-1}.
  - С одной стороны, $\forall \bar{x} \in \mathrm{Ker}(\mathrm{d}'_{n-1}) : \pi_{n-1}(i_{n-1}(\bar{x})) = 0$ из точности нижней строки. С другой стороны, $\forall \bar{y} \in \mathrm{Ker}(d_{n-1})$: если $\pi_{n-1}(\bar{y}) \in \mathrm{Im}(d''_n)$, то из сюръективности π: $\exists y \in A_n : d''_n(\pi_n(z)) = \pi_{n-1}(\bar{y})$. Обозначим $\Delta \coloneqq \bar{y} - d_n(y)$, так как $\pi_{n-1}(\Delta) = 0$, то $\Delta \in \mathrm{Im}(i_{n-1})$. Тем самым, $[\bar{y}] = [\Delta]$ лежит в образе H''_{n-1}, и последовательность точна в члене H_n.

- Функториальность идёт без доказательства. □

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 точных комплекса $A' \to A \to A'' \to 0$ и $0 \to B' \to B \to B''$, 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).

$$\begin{tikzcd}
 & \operatorname{Ker}\phi' \arrow[r, dashed] \arrow[d, "\ker\phi'"] & \operatorname{Ker}\phi \arrow[r, dashed] \arrow[d, "\ker\phi"] & \operatorname{Ker}\phi'' \arrow[d, "\ker\phi''"] \arrow[dddll, dashed, "\delta"] & \\
 & A' \arrow[r] \arrow[d, "\phi"] & A \arrow[r] \arrow[d, "\phi"] & A'' \arrow[r] \arrow[d, "\phi''"] & 0 \\
0 \arrow[r] & B' \arrow[r] \arrow[d, "\operatorname{coker}\phi'"] & B \arrow[r] \arrow[d, "\operatorname{coker}\phi"] & B'' \arrow[d, "\operatorname{coker}\phi''"] & \\
 & \operatorname{CoKer}\phi' \arrow[r, dashed] & \operatorname{CoKer}\phi \arrow[r, dashed] & \operatorname{CoKer}\phi'' &
\end{tikzcd}$$

Доказательство. Доказательство очень похоже на доказательство существования длинной точной последовательности гомологий.

Можно опять сказать, что это диаграммный поиск, и повторить доказательство, но проще вывести из доказательства (теорема 1.3.1). Для этого достаточно рассмотреть комплексы $C_\bullet \coloneqq \left[\ldots \to 0 \to A \xrightarrow{\phi} B \to 0 \to \ldots\right]$, и соответствующие $C'_\bullet$ и $C''_\bullet$ (где вместо A и B подставлены A' и B' либо A'' и B'' соответственно). После этого доказательство (теорема 1.3.1) строит искомую длинную точную последовательность, так как $H(C_\bullet) = [\ldots \to 0 \to \operatorname{Ker}(\phi) \to \operatorname{CoKer}(\phi) \to 0 \to \ldots]$. При этом априори лемма о змее чуть сильнее, так как она не использует, что $A' \to A$ — моно, а $B \to B'$ — эпи, но можно проследить, что доказательство (теорема 1.3.1) в нужных членах это тоже не использует. □

Теорема 1.3.2 (Длинная точная последовательность гомологий на бис)**.** Пусть имеется точная последовательность комплексов $0 \to A' \xrightarrow{i} A \xrightarrow{\pi} A'' \to 0$.

Существует длинная точная последовательность гомологических групп

$$\cdots \longrightarrow H' \xrightarrow{i} H \xrightarrow{\pi} H'' \xrightarrow{\delta} H'[-1] \xrightarrow{i[-1]} H[-1] \longrightarrow \cdots$$

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)

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & A'_n \arrow[r] \arrow[d, "d'_n"] & A_n \arrow[r] \arrow[d, "d_n"] & A''_n \arrow[r] \arrow[d, "d''_n"] & 0 \\
0 \arrow[r] & A'_{n-1} \arrow[r] \arrow[d] & A_{n-1} \arrow[r] \arrow[d] & A''_{n-1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

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:

$$\begin{tikzcd}
 & H'_n \arrow[d] & H_n \arrow[d] & H''_n \arrow[d] & \\
 & A'_n/B'_n \arrow[r] \arrow[d, "\overline{d}'_n"] & A_n/B_n \arrow[r] \arrow[d, "\overline{d}_n"] & A''_n/B''_n \arrow[r] \arrow[d, "\overline{d}''_n"] & 0 \\
0 \arrow[r] & Z'_{n-1} \arrow[r] \arrow[d] & Z_{n-1} \arrow[r] \arrow[d] & Z''_{n-1} \arrow[d] & \\
 & H'_{n-1} & H_{n-1} & H''_{n-1} &
\end{tikzcd}$$

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 $\widetilde{d}_n : A_n/B_n \to A_{n-1}$. Так как A — комплекс, то $\widetilde{d}_n(A_n/B_n) \subset Z_{n-1}$, можно сузить codomain, получая $\overline{d}_n$. По определению $H_n = Z_n/B_n$, поэтому действительно $H_n = \mathrm{Ker}(d_n)$. В свою очередь, $H_{n-1} = Z_{n-1}/B_{n-1}$, и это действительно $\mathrm{CoKer}(d_n)$.

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

Применяя лемму о змее, получаем утверждение теоремы. □

1.4 Функторы между абелевыми категориями

Пусть $\mathscr{A}, \mathscr{B}$ — абелевы категории.

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

1.4.1 Точные и полуточные функторы

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

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

Лемма 1.4.1. *Пусть $\mathscr{F}$ — аддитивный функтор. Следующие условия эквивалентны:*

1. $\mathscr{F}$ точен справа.

2. $\mathscr{F}$ сохраняет нуль и коядра: $\mathscr{F}(0) = 0, \mathscr{F}(\operatorname{coker}(\phi)) = \operatorname{coker}(\mathscr{F}(\phi))$.

3. $\mathscr{F}$ 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» (его определение не использует никакие универсальные свойства, только накладываются некоторые условия на стрелки, которые аддитивные функторы сохраняют), поэтому всякий аддитивный функтор сохраняет его. Предложение из предыдущего семестра о том, что существование инициального объекта и всех копроизведений влечёт существование всех копределов завершает доказательство.

(2) $\Rightarrow$ (1) Короткая точная последовательность $A' \overset{\phi}{\to} A \overset{\psi}{\to} A'' \to 0$ характеризуется свойствами $\psi = \operatorname{coker}\phi, 0 = \operatorname{coker}\psi$.

(1) $\Rightarrow$ (2) Рассмотрим произвольный $\phi : A' \to A$. У него есть эпи-моно разложение $\phi = \mu\varepsilon$ (μ — моно, ε — эпи), и $\operatorname{coker}(\mu\varepsilon) = \operatorname{coker}(\mu)$, так как ε — эпиморфизм. Значит, без потери общности ϕ — мономорфизм.

Тогда последовательность $0 \to A' \overset{\phi}{\to} A \overset{\operatorname{coker}\phi}{\to} \operatorname{CoKer}\phi \to 0$ точна, и так как $\mathscr{F}$ — точен справа, то $\mathscr{F}(\operatorname{coker}\phi) = \operatorname{coker}(\mathscr{F}(\phi))$.

Также точный справа функтор сохраняет нуль: $0 \to A \overset{\mathrm{id}}{\to} A \to 0 \to 0$ переходит в $\mathscr{F}(A) \overset{\mathrm{id}}{\to} \mathscr{F}(A) \to \mathscr{F}(0) \to 0$. □

Следствие 1.4.1. *Левый сопряжённый функтор (к любому другому функтору) точен справа.*

Доказательство. Он сохраняет копределы. □

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

Коядро, как конечный копредел, сохраняет коядра, значит, коядро — точный справа функтор. Двойственно, ядро — точный слева функтор — сохраняет ядра, значит, точный слева функтор.

Это можно понять и без высокой науки, но проверять точность в категории стрелок непросто, так как она не является конкретной категорией, и не вложена в $\mathcal{mod}\text{-}R$. Видимо, удобнее всего проверять второй пункт из (лемма 1.4.1), и он вырождается в следующую диаграмму:

$$\begin{tikzcd}
A \arrow[r, dashed, "\phi"] \arrow[d, "\ker f"'] \arrow[dr, phantom, "I"] & B \arrow[r, dashed, "\psi"] \arrow[d, dashed, "\ker g"] \arrow[dr, phantom, "III"] & C \arrow[d, "\ker h"] \\
D \arrow[r, "\ker \alpha"] \arrow[d, dashed, "f"'] \arrow[dr, phantom, "II"] & E \arrow[r, "\alpha"] \arrow[d, dashed, "g"] \arrow[dr, phantom, "IV"] & F \arrow[d, "h"] \\
G \arrow[r, "\ker \beta"] & H \arrow[r, "\beta"] & I
\end{tikzcd}$$

Применяя к морфизму (α, β) функтор $\ker$, свойственный категории стрелок, мы получим морфизм (ψ, α). Если же рассмотреть морфизм (α, β), как морфизм в произвольной абелевой категории, то его ядром будет $(\ker\alpha, \ker\beta)$. К ядру также можно применить функтор $\ker$, свойственный категории стрелок, получая морфизм $(\phi, \ker\alpha)$.

Чтобы проверить, что функтор ядра сохраняет ядра, надо убедиться, что $\phi = \ker\psi$. Используя коммутативность I, и то, что $\ker\alpha \cdot \ker f$ — мономорфизм, получаем, что ϕ — тоже мономорфизм. Проверим точность в члене B, рассмотрев $x \in B$, такой, что $\psi(x) = 0$.

- Во-первых, $\ker h(\psi(x)) = 0 \overset{\mathit{III}\text{ коммутативен}}{\Rightarrow} \alpha(\ker g(x)) = 0 \overset{\text{точность в } E}{\Rightarrow} \exists y \in D : \ker\alpha(y) = \ker g(x)$.
- Во-вторых, из коммутативности II: $\ker\beta(f(y)) = 0, \overset{\ker\beta\text{ — моно}}{\Rightarrow} f(y) = 0 \overset{\text{точность в } D}{\Rightarrow} \exists z \in A : \ker f(z) = y$.
- И наконец, $\ker g(\phi(z)) = \ker g(x) \overset{\ker g\text{ — моно}}{\Rightarrow} \phi(z) = x$.

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

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.*

Доказательство. Условия как раз означают, что короткая точная последовательность отображается в короткую точную последовательность. □

1.4.2 Гомотопность морфизмов комплексов

Пусть имеются комплексы $X_\bullet$ и $X'_\bullet$, и между ними морфизмы f, g.

Определение 1.4.2 (Морфизмы f и g гомотопны)**.** Существует семейство морфизмов $s_k : X_{k-1} \to X'_k$, таких, что $f_n - g_n = d'_n s_{n+1} + s_n d_{n-1}$. При этом диаграмма ниже **не обязана** быть коммутативной.

$$\begin{tikzcd}
X_{n+1} \arrow[r, "d_n"] \arrow[d, shift right, "f_{n+1}"'] \arrow[d, shift left, "g_{n+1}"] & X_n \arrow[r, "d_{n-1}"] \arrow[d, shift right, "f_n"'] \arrow[d, shift left, "g_n"] \arrow[dl, dotted, "s_{n+1}"'] & X_{n-1} \arrow[r, "d_{n-2}"] \arrow[d, shift right, "f_{n-1}"'] \arrow[d, shift left, "g_{n-1}"] \arrow[dl, dotted, "s_n"'] & \cdots \arrow[r, "d_0"] \arrow[dl, dotted, "s_{n-1}"'] & X_0 \arrow[d, shift right, "f_0"'] \arrow[d, shift left, "g_0"] \arrow[dl, dotted, "s_1"'] \\
X'_{n+1} \arrow[r, "d'_n"'] & X'_n \arrow[r, "d'_{n-1}"'] & X'_{n-1} \arrow[r, "d'_{n-2}"'] & \cdots \arrow[r, "d'_0"'] & X'_0
\end{tikzcd}$$

Пишут $f \simeq g$.

А почему вот такие диагональные стрелки — это то же самое, что и гомотопность в топологии?

Теорема 1.4.1. Если два морфизма комплексов $f, g : X \to X'$ гомотопны, то $H(f) = H(g)$ (здесь функтор гомологий применён не к объектам-комплексам, а к морфизмам комплексов).

Доказательство. Гомологии — аддитивный функтор, докажем, что $H(f - g) = 0$.

Рассмотрим $\overline{x} \in H_n(X)$. У него имеется прообраз $x \in Z_n(X)$.

Заметим, что $H(f_n - g_n)(\overline{x}) = \overline{(f_n - g_n)(x)} = \overline{d'_n(s_{n+1}(x))} + \overline{s_n(d_{n-1}(x))}$. Первое слагаемое равно нулю, так как $d'_n(\cdots) \in B_n(X')$, а второе — так как $x \in \operatorname{Ker} d_{n-1}$. □

Замечание. Если $\mathscr{F} : \mathscr{A} \to \mathscr{A}$ — аддитивный функтор, то ему соответствует функтор $\mathscr{Comp}(\mathscr{F})$, действующий на комплексах с элементами из $\mathscr{A}$ поэлементным применением к объектам и морфизмам функтора $\mathscr{F}$. Допуская вольность речи, можно обозначать этот функтор тоже $\mathscr{F}$. Используя эту вольность речи, можно отметить, что если $f \simeq g$ — гомотопные морфизмы комплексов с объектами из $\mathscr{A}$, то $\mathscr{F}(f) \simeq \mathscr{F}(g)$.

Факт 1.4.2. *Для морфизмов комплексов «быть гомотопными» — отношение эквивалентности.*

Доказательство. Рефлексивность: $\forall n : s_n = 0$. Симметричность: $s_n \coloneqq -s_n$. Транзитивность:

$$\begin{cases} f_n - g_n = d'_n s_{n+1} + s_n d_{n-1} \\ g_n - h_n = d'_n r_{n+1} + r_n d_{n-1} \end{cases} \Rightarrow f_n - h_n = d'_n(s_{n+1} + r_{n+1}) + (s_n + r_n) d_{n-1} \qquad \square$$

Определение 1.4.3 (Два комплекса X и X' гомотопически эквивалентны)**.** Существуют морфизмы комплексов $f : X \to X'$ и $g : X' \to X$, такие, что $fg \simeq \mathrm{id}_{X'}$ и $gf \simeq \mathrm{id}_X$. Данные морфизмы f и g называют *гомотопическими эквивалентностями*.

Факт 1.4.3. *Если X и X' гомотопически эквивалентны, то $H(X) \cong H(X')$.*

Определение 1.4.4 (Квазиизоморфизм $f : X \to X'$)**.** Морфизм f, такой, что $H(f)$ — изоморфизм.

Факт 1.4.4. *Гомотопическая эквивалентность — квазиизоморфизм.*

Определение 1.4.5 (Комплекс X ацикличен)**.** X точен, то есть $H(X) = 0$.

Определение 1.4.6 (Комплекс X стягиваем)**.** $\mathrm{id}_X \simeq 0_X$.

Замечание. Из (теорема 1.4.1) следует, что стягиваемый комплекс ацикличен.

Обратное, вообще говоря, неверно. Стягиваемый комплекс сохраняется под действием функторов, а ацикличный — может и не сохраниться.

1.5 Проективные резольвенты

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

Определение 1.5.1 (Объект P проективен)**.** $\forall \phi : A \to B$: ϕ — эпи $\Rightarrow \forall \psi : P \to B$: $\exists \theta : P \to A$, такое, что диаграмма коммутирует. При этом θ должно быть какое-то, не факт, что оно единственно.

$$\begin{tikzcd} & P \arrow[dl, dotted, "\exists\theta"'] \arrow[d, dashed, "\forall\psi"] & \\ A \arrow[r, "\forall\phi"] & B \arrow[r] & 0 \end{tikzcd}$$

Факт 1.5.1. *В $\mathscr{Set}$ все множества — проективные объекты.*

Теорема 1.5.1. Пусть $\mathscr{A} = R\text{-}\mathscr{mod}$. 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.

$$\begin{tikzcd} & M \arrow[r] \arrow[d, "\psi"] & M \oplus N \arrow[dl, dashed] \arrow[dll, bend right] \\ A \arrow[r, two heads] & B \arrow[r] & 0 \end{tikzcd}$$

   Определим $M \oplus N \to B, (m, n) \mapsto \psi(m)$. Так как $M \oplus N$ проективен, то найдётся $M \oplus N \to A$, и композиция $M \to M \oplus N \to A$ 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).

$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists"'] \arrow[d, "\mathrm{id}"] \\ F \arrow[r, two heads, "\pi"] & P \end{tikzcd}$$

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

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 над кольцом $\mathbb{Z}/6\mathbb{Z}$.
- Можно предъявить проективный модуль, исходя из топологического факта о том, что шар нельзя причесать. А как?

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

В будущем докажем, что любые две проективные резольвенты гомотопически эквивалентны (следствие 1.6.1).

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

Если в нашей категории $\mathscr{A}$ 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 Левый производный функтор

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

$$\begin{tikzcd} \cdots \arrow[r, rightsquigarrow] & P_1 \arrow[r, rightsquigarrow] & P_0 \arrow[r] \arrow[d, rightsquigarrow] & 0 \\ \cdots \arrow[r] & 0 \arrow[r] & A \arrow[r, rightsquigarrow] & 0 \end{tikzcd}$$

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

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

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

Теорема 1.6.1. Пусть P_i проективные, сверху комплекс (ноль в верхней строчке стоит для красоты, он там неважен), снизу — точный комплекс, и дан морфизм f.

$$\begin{tikzcd} \cdots \arrow[r] & P_1 \arrow[r] \arrow[d, dashed] & P_0 \arrow[r] \arrow[d, dashed] & A \arrow[r] \arrow[d, dashed, "f"] & 0 \\ \cdots \arrow[r] & Q_1 \arrow[r] & Q_0 \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

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

Доказательство.

- – Сначала построим $f_i : P_i \to Q_i$.

  $Q_0 \to B$ сюръективно, значит, так как P_0 проективен, то найдётся $f_0 : P_0 \to Q_0$, такое, что квадрат коммутативен.

  – Далее по индукции: пусть построены $f_0, \dots, f_n$.

$$\begin{tikzcd} P_{n+1} \arrow[r, "d_n^P"] \arrow[d, dashed, "f_{n+1}"] & P_n \arrow[r, "d_{n-1}^P"] \arrow[d, "f_n"] & P_{n-1} \arrow[d, "f_{n-1}"] \\ Q_{n+1} \arrow[r, "d_n^Q"] & Q_n \arrow[r, "d_{n-1}^Q"] & Q_{n-1} \end{tikzcd}$$

  Хочется заполучить стрелку $P_{n+1} \to Q_{n+1}$, воспользовавшись проективностью P_{n+1}. Для этого надо найти сюръективное отображение из Q_{n+1}.

  Так как внизу — точная последовательность, то $d_n^Q : Q_{n+1} \to \operatorname{Ker}(d_{n-1}^Q)$ подойдёт: во-первых, $\operatorname{Im}(d_n^Q) = \operatorname{Ker}(d_{n-1}^Q)$ из точности $Q_\bullet$, а во-вторых, $\operatorname{Im}(f_n \circ d_n^P) \subset \operatorname{Ker}(d_n^Q)$ — чтобы это увидеть, надо применить d_n^Q и воспользоваться коммутативностью правого квадрата, и тем, что P — комплекс. Тем самым, по определению проективного модуля $\exists f_{n+1} : P_{n+1} \to Q_{n+1}$.

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

$$\begin{tikzcd} \cdots \arrow[r] & P_1 \arrow[r] \arrow[d, shift right, "f_1"'] \arrow[d, shift left, "g_1"] & P_0 \arrow[r] \arrow[d, shift right, "f_0"'] \arrow[d, shift left, "g_0"] & A \arrow[r] \arrow[d, dashed, "f"] & 0 \\ \cdots \arrow[r] & Q_1 \arrow[r] & Q_0 \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

  Распишем разность: пусть $h_i \coloneqq f_i - g_i$. Построим гомотопию $h \simeq 0$. Понятно, что $A \to Q_0$ надо взять нулевым.

$$\begin{tikzcd} \cdots \arrow[r] & P_1 \arrow[r] \arrow[d, dashed, "h_1"] & P_0 \arrow[r] \arrow[d, dashed, "h_0"] \arrow[dl, dashed, "s_0"'] & A \arrow[r] \arrow[d, dashed, "0"] \arrow[dl, dashed, "0"'] & 0 \arrow[dl, dashed, "0"'] \\ \cdots \arrow[r] & Q_1 \arrow[r] & Q_0 \arrow[r, "d_{-1}^Q"] & B \arrow[r] & 0 \end{tikzcd}$$

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

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

$$\begin{tikzcd} & P_n \arrow[r, "d_{n-1}^P"] \arrow[d, dashed, "h_n"] \arrow[dl, dashed, "s_n"'] & P_{n-1} \arrow[r, "d_{n-2}^P"] \arrow[d, dashed, "h_{n-1}"] \arrow[dl, "s_{n-1}"'] & P_{n-2} \arrow[dl, "s_{n-2}"'] \\ Q_{n+1} \arrow[r, "d_n^Q"] & Q_n \arrow[r, "d_{n-1}^Q"] & Q_{n-1} & \end{tikzcd}$$

  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 $\mathrm{Im}(d_n^Q)$, то есть $\mathrm{Ker}(d_{n-1}^Q)$. 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.*

Доказательство. Пусть P, Q — две резольвенты объекта A. В силу (теорема 1.6.1), можно построить морфизмы этих резольвент $f : P \to Q$ и $g : Q \to P$.

$$\begin{array}{ccc} P & \longrightarrow & A \\ {\scriptstyle g}\uparrow\downarrow{\scriptstyle f} & & \updownarrow{\scriptstyle \mathrm{id}} \\ Q & \longrightarrow & A \end{array} \qquad \begin{array}{ccc} P & \longrightarrow & A \\ {\scriptstyle \mathrm{id}}\downarrow\downarrow{\scriptstyle gf} & & \updownarrow{\scriptstyle \mathrm{id}} \\ P & \longrightarrow & A \end{array}$$

Получается, что $gf : P \to P$ — эндоморфизм P, как резольвенты A. С другой стороны, id_P — тоже эндоморфизм P, как резольвенты A, и опять применяя (теорема 1.6.1), получаем, что $gf \simeq \mathrm{id}_P$. Аналогично $fg \simeq \mathrm{id}_Q$. □

Таким образом, определение левого производного функтора $L_n\mathscr{F}(A) \stackrel{def}{=} H_n\mathscr{F}(P)$ корректно.

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

Примеры (Что такое L_0 от точного справа функтора).

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

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

  точна. $L_0\mathscr{F}(A) = H_0(\mathscr{F}(P)) = \mathrm{CoKer}(\mathscr{F}(P_1) \to \mathscr{F}(P_0))$. Получается $\mathrm{CoKer}(\mathscr{F}(P_1) \to \mathscr{F}(P_0)) = \mathscr{F}(A)$, то есть $L_0\mathscr{F} = \mathscr{F}$.

- Обратно, если $L_0\mathscr{F} = \mathscr{F}$, то $\mathscr{F}$ сохраняет коядра, значит, точен справа. Вообще-то, сохраняются только коядра морфизмов проективных объектов, почему этого достаточно? (Похорошему, надо ещё проверить, что $L_0\mathscr{F}$ действует на морфизмах так же, но это банально).

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

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

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

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

1.6.1 Длинная точная последовательность левых производных функторов

Зафиксируем некоторый функтор $\mathscr{F}$. Далее мы исследуем $L_n\mathscr{F}$, для упрощения записи будем писать $L_n \coloneqq L_n\mathscr{F}$.

Пусть имеется короткая точная последовательность $0 \to A \to B \to C \to 0$ в $\mathscr{A}$. Построим длинную точную последовательность производных функторов, выглядящую так:

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

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

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

$$\begin{tikzcd}
 & Q \arrow[r, dashed, "i"] \arrow[d] & Q \oplus P \arrow[r, dashed, "\pi"] \arrow[d, dashed] & P \arrow[d] & \\
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d, dashed] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

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 $gs = h_C$.

$$\begin{tikzcd}
 & Q \arrow[r, dashed, "i"] \arrow[d, "h_A"'] & Q \oplus P \arrow[r, dashed, "\pi"] \arrow[d, dashed, "h_B"'] & P \arrow[d, "h_C"'] \arrow[dl, dotted, "s"'] & \\
0 \arrow[r] & A \arrow[r, "f"] \arrow[d] & B \arrow[r, "g"] \arrow[d, dashed] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

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 $gh_B(0,v) = h_C(v) = gs(v)$. Тем самым, подойдёт $h_B(u,v) \coloneqq f(h_A(u)) + s(v)$.

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

Также несложно убедиться, что построенный морфизм h_B — эпи, видимо, это делается в тупую при помощи диаграммного поиска:

Рассмотрим $b \in B$, пусть $c \coloneqq g(c)$ и $\bar{b} \coloneqq \pi^{-1}\left(h_C^{-1}(c)\right)$ — произвольный прообраз. Из коммутативности правого квадрата $h_B\left(\bar{b}\right)$ и b под действием g уходят в $g(b)$, откуда $g\left(b - h_B\left(\bar{b}\right)\right) = 0$. Из точности нижней строки $\exists a \in A : f(a) = b - h_B\left(\bar{b}\right)$, а из эпиморфности $h_A : \exists \bar{a} \in Q : h_A\left(\bar{a}\right) = a$. Тем самым, $h_B\left(i(\bar{a}) + \bar{b}\right) = b$. □

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

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

Далее необходимо провести индукционный переход.

$$\begin{tikzcd}
 & (P_A)_{n+1} \arrow[r, dashed, "i"] \arrow[d, two heads] & (P_A)_{n+1} \oplus (P_C)_{n+1} \arrow[r, dashed, "\pi"] \arrow[d, dashed, "d_n^B"] & (P_C)_{n+1} \arrow[d, two heads] & \\
0 \arrow[r] & \operatorname{Ker}(d_{n-1}^A) \arrow[r] \arrow[d, hook] & \operatorname{Ker}(d_{n-1}^B) \arrow[r] \arrow[d, hook] & \operatorname{Ker}(d_{n-1}^C) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & (P_A)_n \arrow[r] \arrow[d, two heads, "d_{n-1}^A"] & (P_B)_n \arrow[r] \arrow[d, two heads, "d_{n-1}^B"] & (P_C)_n \arrow[r] \arrow[d, two heads, "d_{n-1}^C"] & 0 \\
0 \arrow[r] & \operatorname{Ker}(d_{n-2}^A) \arrow[r] & \operatorname{Ker}(d_{n-2}^B) \arrow[r] & \operatorname{Ker}(d_{n-2}^C) \arrow[r] & 0
\end{tikzcd}$$

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

При $n = 1$ это верно в силу леммы о змее:

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}(d_{-1}^A) \arrow[r] \arrow[d, hook] & \operatorname{Ker}(d_{-1}^B) \arrow[r] \arrow[d, hook] & \operatorname{Ker}(d_{-1}^C) \arrow[d, hook] \arrow[dddll, dashed, rounded corners] & \\
0 \arrow[r] & P_A \arrow[r] \arrow[d, "d_{-1}^A"] & P_B \arrow[r] \arrow[d, "d_{-1}^B"] & P_C \arrow[r] \arrow[d, "d_{-1}^C"] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Если же $n > 1$, то воспользуемся тем, что $(P_B)_n = (P_A)_n \oplus (P_C)_n$. Это, в частности, значит, что у ретракции $\pi_n : (P_B)_n \to (P_C)_n$ имеется односторонняя обратная — сечение $s_n : (P_C)_n \to (P_B)_n$, такая, что $\pi_n \cdot s_n = \mathrm{id}_{(P_C)_n}$. Ввиду функториальности ядра односторонняя обратная будет иметься и у отображения ядер $\operatorname{Ker}(d_{n-1}^B) \to \operatorname{Ker}(d_{n-1}^C)$, что значит, что это эпиморфизм.

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

Точность $0 \to P_A \to P_B \to P_C$ 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* $0 \to A \to B \to C \to 0$ *имеет место длинная точная последовательность*

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

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

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

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

Лекция VI

25 марта 2024 г.

1.6.2 Связанные последовательности функторов

Рассмотрим формальное обобщение производных функторов.

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

Определение 1.6.1 ((Левая) связанная последовательность функторов)**.** Такая последовательность функторов $\{\mathscr{F}_i\}_{i\in\mathbb{N}_0}$, что для любой точной последовательности $0 \to A \to B \to C \to 0$ существует функториальная длинная точная последовательность

$$\cdots \to \mathscr{F}_1(A) \to \mathscr{F}_1(B) \to \mathscr{F}_1(C) \to \mathscr{F}_0(A) \to \mathscr{F}_0(B) \to \mathscr{F}_0(C)$$

Пример. Последовательность $\{L_i\mathscr{F}\}_{i\in\mathbb{N}_0}$ — связанная последовательность функторов.

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

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

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

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

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

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

$$0 \to M \to P \to A \to 0$$

Так как последовательности функторов — связаны — то имеется длинная точная последовательность, нарисуем её кусок:

$$\begin{tikzcd}
0 = \mathscr{F}_1(P) \arrow[r] & \mathscr{F}_1(A) \arrow[r] \arrow[d, dashed, leftrightarrow] & \mathscr{F}_0(M) \arrow[r] \arrow[d, leftrightarrow] & \mathscr{F}_0(P) \arrow[d, leftrightarrow] \\
0 = \mathscr{G}_1(P) \arrow[r] & \mathscr{G}_1(A) \arrow[r] & \mathscr{G}_0(M) \arrow[r] & \mathscr{G}_0(P)
\end{tikzcd}$$

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

Теперь займёмся индукционным переходом:

$$\begin{tikzcd}
0 = \mathscr{F}_i(P) \arrow[r] & \mathscr{F}_i(A) \arrow[r] \arrow[d, dashed, leftrightarrow] & \mathscr{F}_{i-1}(M) \arrow[r] \arrow[d, leftrightarrow] & \mathscr{F}_{i-1}(P) = 0 \\
0 = \mathscr{G}_i(P) \arrow[r] & \mathscr{G}_i(A) \arrow[r] & \mathscr{G}_{i-1}(M) \arrow[r] & \mathscr{G}_{i-1}(P) = 0
\end{tikzcd}$$

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

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

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

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

1.7 Производные функторы для $\otimes$

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

Изучим производные функторов тензорного произведения (функтор тензорного произведения точен справа, так как он — левый сопряжённый к Hom (что верно в силу естественного изоморфизма $\mathrm{Hom}(A \otimes B, C) \cong \mathrm{Hom}(A, \mathrm{Hom}(B, C))$)).

Обозначим $\mathrm{LTor}_i(M, \_) \overset{def}{=} L_i(M \otimes \_)$, $\mathrm{RTor}_i(\_, N) \overset{def}{=} L_i(\_ \otimes N)$.

Примеры.

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

  Тензорно домножая на M, мы получаем $0 \to M \overset{m\otimes r \mapsto m \otimes ar}{\longrightarrow} M \to M \otimes R/aR \to 0$. Так как кольцо коммутативное, то тензорное произведение — $\mathcal{mod}\text{-}R$, 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 $\{x \in M | ax = 0\}$.

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

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

Идея доказательства. Пусть имеются резольвенты $[\ldots \to P_1 \to P_0 \to M]$ и $[\ldots \to Q_1 \to Q_0 \to N]$, нарисуем следующую коммутативную диаграмму:

$$
\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
\cdots \arrow[r] & P_1 \otimes Q_1 \arrow[r] \arrow[d] & P_0 \otimes Q_1 \arrow[r] \arrow[d] & M \otimes Q_1 \arrow[r] \arrow[d] & 0 \\
\cdots \arrow[r] & P_1 \otimes Q_0 \arrow[r] \arrow[d] & P_0 \otimes Q_0 \arrow[r] \arrow[d] & M \otimes Q_0 \arrow[r] \arrow[d] & 0 \\
\cdots \arrow[r] & P_1 \otimes N \arrow[r] \arrow[d] & P_0 \otimes N \arrow[r] \arrow[d] & M \otimes N & \\
 & 0 & 0 & &
\end{tikzcd}
$$

Тензорное домножение на свободный объект — точный справа функтор — из дистрибутивности тензорного произведения. Тензорное домножение на проективный объект (прямое слагаемое свободного) — 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 $\mathsf{Tot}(M, N)_n \coloneqq \bigoplus_{i=0}^{n} P_i \otimes Q_{n-i}$, и теперь надо определить дифференциал D. Необходимо, чтобы выполнялось требование $D^2 = 0$, поэтому абы какой не подойдёт.

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

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

Теперь определим полный дифференциал $D_n \coloneqq \bigoplus\limits_{p+q=n} D_{p,q} : \mathsf{Tot}(M, N)_n \to \mathsf{Tot}(M, N)_{n-1}$.

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.

Таких функторов два: имеются ковариантный $\mathrm{Hom}(M, \_)$, и контравариантный $\mathrm{Hom}(\_, N)$.

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

1.8.1 Инъективные резольвенты

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

$$\begin{tikzcd} A \arrow[r, tail] \arrow[d] & B \arrow[dl, dashed, "\exists"] \\ Q & \end{tikzcd}$$

Интересный факт. Инъективный модуль — то же самое, что и делимый модуль, то есть $\forall r \in R \setminus \{0\}, q \in M : \exists x \in M : rx = q$. Скорее всего, это верно только над PID.

В одну сторону доказательство очевидно — чтобы убедиться, что инъективный модуль является делимым, надо в качестве A взять кольцо R, а в качестве B — поле частных R.

В категории $\mathscr{C}$, где *достаточно много инъективных объектов* (то есть $\forall C \in \mathscr{C} : \exists$ проективный Q вместе с вложением $C \hookrightarrow Q$), двойственно проективной, строится инъективная резольвента, в которой коядро предыдущего морфизма вкладывается в следующий инъективный модуль:

$$0 \to N \to Q_0 \to Q_1 \to Q_2 \to \cdots$$

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

$$0 \to \mathrm{Hom}(M, Q_0) \to \mathrm{Hom}(M, Q_1) \to \cdots$$

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

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

1.8.2 О расширениях модулей и Ext^1

Название Ext происходит от extensions, элементы Ext^1 находятся в биекции с классами коротких точных последовательностей $0 \to M \to ? \to N \to 0$ (теорема 1.8.1). В качестве среднего члена всегда подойдёт $M \oplus N$, но, может быть, и ещё что-то, и за это отвечает Ext^1.

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

Лекция VII

1 апреля 2024 г.

Пусть $M, N \in \mathcal{mod}\text{-}R$.

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

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

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

Доказательство. Рассмотрим расширение $0 \to M \to X \to N \to 0$. Запишем кусок длинной точной последовательности правых производных функторов для $\operatorname{Hom}(\_, M)$ и данной короткой точной последовательности, заменяя Ext^0 на Hom:

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

Построим $x \in \operatorname{Ext}^1(N, M)$, как образ $\mathrm{id} \in \operatorname{Hom}(M, M)$.

Построим стрелку обратно, накрыв N проективным объектом, и взяв ядро: $0 \to A \to P \to N \to 0$. Для $\operatorname{Hom}(\_, M)$ и этой короткой точной последовательности можно тоже записать кусок длинной точной последовательности правых производных функторов:

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

Так как домножение на проективный модуль — точный функтор, то $\operatorname{Ext}^1(P, M) = 0$. Значит, $\operatorname{Ext}^1(N, M) \twoheadleftarrow \operatorname{Hom}(A, M)$ — эпиморфизм. Сопоставим элементу $x \in \operatorname{Ext}^1(N, M)$ его какой-то прообраз $\beta \in \operatorname{Hom}(A, M)$. Теперь пусть X — пушаут диаграммы $M \xleftarrow{\beta} A \to P$.

Построим следующую диаграмму, получая отображение $X \to N$ из универсального свойства пушаута, применённого к $P \to N$ и нулевому $M \to N$.

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\beta"] & P \arrow[r] \arrow[d] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M \arrow[r] & X \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

Можно показать, что нижняя последовательность — короткая точная, и мы определим её, как образ элемента $x \in \operatorname{Ext}^1(N, M)$.

Далее можно проверить, что в одну сторону эти отображения взаимно обратны — построим по диаграмме выше, как по паре коротких точных последовательностей, последовательность правых производных функторов, и в силу функториальности между ними будут следующие морфизмы:

$$\begin{tikzcd}
0 = \operatorname{Ext}^1(P, M) & \operatorname{Ext}^1(N, M) \arrow[l] & \operatorname{Hom}(A, M) \arrow[l] & \operatorname{Hom}(P, M) \arrow[l] & \operatorname{Hom}(N, M) \arrow[l] \\
 & \operatorname{Ext}^1(N, M) \arrow[u, equal, "?"] & \operatorname{Hom}(M, M) \arrow[l] \arrow[u, "_\cdot\beta"] & \operatorname{Hom}(X, M) \arrow[l] \arrow[u] & \operatorname{Hom}(N, M) \arrow[l] \arrow[u, equal]
\end{tikzcd}$$

Если я правильно понимаю, то стрелка, помеченная ? — тождественное отображение просто-напросто из функториальности длинной точной последовательности, и того, что функторы сохраняют id.

Элементу $x \in \operatorname{Ext}^1(N, M)$ сопоставляется $\beta \in \operatorname{Hom}(A, M)$, полученная проходом против стрелки влево. Можно заметить, что образ id под действием $\_ \cdot \beta$ тоже равен β, так что из коммутативности левого квадрата, если сопоставить x короткую точную последовательность, а потом обратно, то получится снова x.

Надо ещё проверить, что обратное отображение не зависит от выбора β, и что композиция в другую сторону тоже тождественна, но это вряд ли будет когда-нибудь написано. □

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

Запишем проективную резольвенту по первому аргументу.

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

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

  Граничные гомоморфизмы определены так: $d_n(g_0,\ldots,g_n) = \sum\limits_{i=0}^{n}(-1)^i(g_0,\ldots,\widehat{g}_i,\ldots,g_n)$. 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 $I_G = \mathrm{Ker}(\phi)$, здесь $\phi : \mathbb{Z}[G] \to \mathbb{Z}$ — $\mathbb{Z}$-линейный гомоморфизм аугментации, определённый на базисе $g \mapsto 1$. Иными словами, $I_G = \langle g-1 | g\in G\rangle = \left\{ \sum\limits_{g\in G}\alpha_h\cdot g \,\middle|\, \sum\limits_{g\in G}\alpha_g = 0\right\}$, 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. $H^0(G,A) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},A)$. Всякому гомоморфизму $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},A)$ можно $\phi(1)$. Из G-линейности $\forall g\in G : \phi(1) = \phi(g\cdot 1) = g\cdot\phi(1)$, значит, $\phi(1) \in A^G \overset{def}{=} \{a\in A | \forall g\in G : ga = a\}$ — *инварианты*. Значит, нулевые когомологии — инварианты.
- $H_1(G,\mathbb{Z}) = G^{\mathrm{ab}} \overset{def}{=} G/[G,G]$.
- $H^1(G,A) = \mathrm{Der}(G,A)$ — множество скрещённых гомоморфизмов.

  Скрещенный гомоморфизм — это такое отображение $\phi : G\to A$, которое обладает свойством $\phi(gh) = g\cdot\phi(h)+\phi(g)$.
- $H_2(G,\mathbb{Z}) =?$ Предположим, что имеется точная последовательность групп $0\to R\to F\to G\to 1$, то есть $G\cong F/R$.

  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 $\mathrm{Ker}(\pi) \in C(S)$, и

  $$\begin{tikzcd} S \arrow[r, two heads] \arrow[dr, "\exists!"'] & G \\ & H \arrow[u, dashed, "\forall \text{ центрального расширения}"'] \end{tikzcd}$$

  В этом случае $H_2(G,\mathbb{Z}) = \mathrm{Ker}\,\pi$. Например, в случае $G = SL_n(F) : S = \mathrm{St}_n(F)$ — *группа Стейнберга*. Ядро $\mathrm{St}_n(F) \twoheadrightarrow SL_n(F)$ — это $K_{2,n}(F) = H_2(G,\mathbb{Z})$. Для $n \geqslant 5$ 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 $\dim_F K \overset{def}{=} [K : F]$ — *степень расширения*.

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

2.1.1 Лемма о простых расширениях. Алгебраические и трансцендентные элементы

Лемма 2.1.1 (О простых расширениях)**.** *Либо $F(\alpha) \cong F(t)$ — поле дробно-рациональных функций, оно же поле частных $F[t]$, 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 $\phi : F[t] \to F(\alpha), t \mapsto \alpha$.

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

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

- Иначе, так как многочлены — PID — то $\operatorname{Ker} \phi = p \cdot F[t]$, и $\operatorname{Im} \phi \cong F[t]/(p)$. 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 $\operatorname{Im} \phi \cong F[t]/(p)$ — уже поле. Базисом $F[t]/(p)$ над F является, например, $\left(1, \bar{t}, \ldots, \bar{t}^{\deg(p)-1}\right)$. □

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 унитальности минимального многочлена.

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

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

Лемма 2.1.2. *Пусть имеется композиция (ещё говорят* башня*) 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. □

2.1.2 Конечные и алгебраические расширения

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

Теорема 2.1.1. Пусть K/F — расширение полей. Следующие условия равносильны:

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

Доказательство.

(3) ⇒ (1) Индукция по n.

База: $n = 0 \Rightarrow K = F$.

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

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

Доказательство леммы.

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

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

(2) ⇒ (3) Тавтологично.

2.1.3 Алгебраическое замыкание одного поля в другом

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

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

2.1.4 Базис трансцендентности

Пусть $X \subset K$ — произвольное подмножество, где по-прежнему K/F — расширение полей.

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)**.** $\langle X \rangle \overset{def}{=} \operatorname{Int}_K F(X)$ (где, как обычно, $F(X)$ — наименьшее подполе в K, содержащее F и 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 $F(t)$: одноэлементное множество $\{t\}$ — 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 подскажем, как они выглядят?

Теорема 2.1.2. Степень трансцендентности не зависит от выбора базиса.

Доказательство. Аналогично подобному факту из линейной алгебры. □

2.2 Построение полей

2.2.1 Поле разложения

Пусть F — поле, $f \in F[t]$.

Определение 2.2.1 (Поле разложения f над F)**.** Расширение 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.

- $F = \mathbb{R}, f(t) = t^2 + 1$. В этом случае $F_f \cong \mathbb{C}$.
- $F = \mathbb{Q}, f(t) = t^3 - 2$. В этом случае $\mathbb{Q}\left(\sqrt[3]{2}\right)$ — 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 $\sqrt{-3}$, так как $\left(\frac{-1 \pm \sqrt{-3}}{2}\right)^3 = 1$. Тем самым, поле разложения $\mathbb{Q}_f \cong \mathbb{Q}\left[\sqrt[3]{2}, \sqrt{-3}\right]$.

Теорема 2.2.1. 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 $E \coloneqq F[t]/(p)$. В E: $\alpha \coloneqq \overline{t} = t + (p)$ — корень p.

Также в E: $f(t) = (t - \alpha) \cdot h(t)$ для некоторого $h : \deg h = \deg f - 1$. Положим $F_f \coloneqq E_h$, 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 $F[t]$ — UFD, и раз уж f раскладывается на линейные множители в K, то p и подавно.

При этом h раскладывается в K на линейные множители, по индукции E_h вкладывается в K. $\square$

Пусть K/F и L/F — расширения полей. Тогда гомоморфизм $\phi : K \to L$ 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 2.2.2. Пусть K — поле, в котором $f \in F[t]$ раскладывается на линейные множители. Тогда K — поле разложения $f \iff K \cong F[\alpha_1, \ldots, \alpha_n]$, где α_i — все корни f ($\deg f = n$).

Доказательство.

- $\Leftarrow$. Построенное в (теорема 2.2.1) поле разложения действительно порождено корнями f.
- $\Rightarrow$. В поле разложения f по определению лежат все корни f. Более того, раз в $F[\alpha_1, \ldots, \alpha_n]$ многочлен f разложим на линейные множители, то имеется гомоморфизм $K \to F[\alpha_1, \ldots, \alpha_n]$. Он сюръективен (в образе лежит F, так как гомоморфизм — над F, и в образе лежат корни α_i, так как в них отправятся корни многочлена f) и инъективен (любой гомоморфизм полей инъективен). $\square$

Лекция IX

16 апреля 2024 г.

Лемма 2.2.1. *Пусть K/F и L/F — конечные расширения, и $K \to L, L \to K$ — гомоморфизмы над F. Тогда $K \cong L$ (и оба отображения — изоморфизмы).*

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

2.2.2 Конечные поля

Пусть F — конечное поле ($|F| < \infty$). В поле есть единница, 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 2.2.2. *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 $F \overset{\mathbb{F}_p\text{-}\mathscr{V}ect}{\cong} \mathbb{F}_p^n$ для некоторого $n \in \mathbb{N}$. $\square$

Теорема 2.2.3. 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 $X \coloneqq \{x \in F | x^q - x = 0\} \subset F$. Заметим, что X замкнуто относительно сложения, умножения и взятия обратного:

$$\begin{cases} x^q = x \\ y^q = y \end{cases} \Rightarrow \begin{cases} (xy)^q = xy \\ (x+y)^q = x^q + y^q = x + y \\ \left(\frac{1}{x}\right)^q = \frac{1}{x^q} = \frac{1}{x} \end{cases}$$

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

  Тем самым, $X \leqslant F$ — подполе в F. Из замкнутости X относительно сложения $\mathbb{F}_p \subset X$, так как всякий элемент в $\mathbb{F}_p$ — сумма единиц.

  С другой стороны, X содержит все корни $t^q - t$, а F — поле разложения $t^q - t$, значит, имеется и гомоморфизм $F \to X$. $X/\mathbb{F}_p$ и $F/\mathbb{F}_p$ конечны, откуда (лемма 2.2.1) $X = F$.

- 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, $F \cong E$. □

2.2.3 Алгебраическая замкнутость поля и алгебраическое замыкание

Лемма 2.2.3. *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. $\forall f \in F[t] \setminus F$: *($f$ неприводим* $\iff \deg f = 1$).
4. *Любое алгебраическое расширение F совпадает с F.*
5. *Любое конечное расширение F совпадает с F.*

Доказательство. Тривиально.

(1) ⇒ (2) Тавтологично.

(2) ⇒ (3) ⇒ следует из теоремы Безу (α корень $\iff$ $t - \alpha$ — делитель), ⇐ следует из того, что все многочлены степени 1 неприводимы.

(3) ⇒ (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) ⇒ (5) Тавтологично.

(5) ⇒ (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 2.2.2 (Алгебраически замкнутое поле)**.** Поле F, удовлетворяющее условиям из предыдущей леммы (лемма 2.2.3).

Лемма 2.2.4. *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 — унитальный: $f(t) = t^n + \alpha_{n_1} t^{n-1} + \cdots + \alpha_0$. Построим поле $E \coloneqq F[\alpha_0, \ldots, \alpha_n]$, расширение E/F конечно.

f тем более неприводим в E, значит, можно рассмотреть поле $L \coloneqq E[t]/(f)$, расширение L/E, а стало быть и L/F тоже конечны.
$$\begin{tikzcd} K \arrow[d, dash, "\text{алгебраично}"'] & L \arrow[dl, dash, "\text{конечно}"] \\ E \arrow[d, dash, "\text{конечно}"'] & \\ F & \end{tikzcd}$$

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. $\square$

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 2.2.5. *Пусть L/F — расширение полей, причём L алгебраически замкнуто. Тогда $\operatorname{Int}_L F$ тоже алгебраически замкнуто.*

Доказательство. Рассмотрим $f \in F[t]$. В L он раскладывается на линейные множители $f(t) = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n)$, где $\alpha_i \in L$. По определению алгебраического замыкания F в L, $\alpha_i \in \operatorname{Int}_L F$. Применяя (лемма 2.2.4), получаем, что $\operatorname{Int}_L F$ алгебраически замкнуто. $\square$

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

Определение 2.2.3 (Алгебраическое замыкание поля F)**.** Алгебраическое расширение F, являющееся алгебраически замкнутым полем. Обозначается F^{alg}.

Теорема 2.2.4. У любого поля F существует алгебраическое замыкание.

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

> **Лемма 2.2.6.** *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
> $$g_1 f_1(x_{f_1}) + \cdots + f_m f_m(x_{f_m}) = 1, \text{ где } f_i, g_i \in F[t] \qquad (\triangle)$$
> Корни конечного множества многочленов мы умеем присоединять: введём $f \coloneqq f_1 \cdot \ldots \cdot f_m$, в F_f у каждого из f_i есть корень, назовём его β_i. Теперь устроим гомоморфизм F-алгебр $\phi : F[X] \to F_f, \begin{cases} x_{f_i} \mapsto \beta_i \\ x_g \mapsto 0 \end{cases}$, он определён согласно универсальному свойству кольца многочленов.
>
> В образе $(\triangle)$ обращается в равенство $0 = 1$, но в F_f это, конечно, неверно. $\square$

Раз $J \trianglelefteq F[X]$ не совпадает со всем кольцом, то можно взять максимальный идеал $\mathfrak{m}$, содержащий J, и не совпадающий со всем кольцом (лемма Цорна). Факторкольцо $E_1 \coloneqq F[X]/\mathfrak{m}$ является полем, в котором образ переменной x_f — корень многочлена f.

К сожалению, не факт, что E_1 алгебраически замкнуто, (лемма 2.2.4) неприменима, так как неизвестно, что всякий многочлен из $F[t]$ раскладывается в $E_1[t]$ на линейные множители.

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

Теперь осталось положить $F^{\text{alg}} \coloneqq \operatorname{Int}_{\overline{F}} F$, оно алгебраически замкнуто, согласно (лемма 2.2.5). $\square$

Лекция X

22 апреля 2024 г.

Предложение 2.2.1. *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 $K \coloneqq \operatorname{Int}_L F$. Тогда*

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

Доказательство.

1. Образуем множество $\mathscr{X} \coloneqq \left\{(\widetilde{F}, \phi) \middle| F \subset \widetilde{F} \subset E, \phi : \widetilde{F} \hookrightarrow L\right\}$. На $\mathscr{X}$ введём частичный порядок: $(F', \phi') \preceq (F'', \phi'') \iff F' \subset F''$ и $\phi''\big|_{F'} = \phi'$.

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

   Убедимся, что здесь применима лемма Цорна: если $(F_\alpha, \phi_\alpha)_{\alpha \in A}$ — цепь, то $\widetilde{F} \coloneqq \bigcup\limits_{\alpha \in A} F_\alpha$ вместе с $\widetilde{\phi}$ — верхняя грань (где $\widetilde{\phi}$ определено так: и $\forall x \in \widetilde{F} : \widetilde{\phi}(x) \coloneqq \phi_\alpha(x)$ для произвольного α, такого, что $x \in F_\alpha$).

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

   Отождествим $\widetilde{F}$ с его образом $\widetilde{\phi}(\widetilde{F}) \subset L$ (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: $\widetilde{F}[\theta] \cong \widetilde{F}[t]/(g)$, то есть $\exists! \psi : \widetilde{F}[\theta] \to \widetilde{F}[\alpha]$ — гомоморфизм полей над $\widetilde{F}$, такой, что $\psi(\theta) = \alpha$. Пара $(\widetilde{F}[\theta], \psi)$ строго больше пары $(\widetilde{F}, \widetilde{\phi})$, противоречие. Тем самым, $\widetilde{F} = E$, и имеется полностью определённое $E \to L$.

2. 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 унитального многочлена $f \in F[t]$. В E многочлен f раскладывается на линейные множители $f(t) = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n)$, где $\alpha_i \in E$. Применяя индуцированный $\phi : E[t] \to L[t]$ к данному разложению, получаем $f(t) = (t - \phi(\alpha_1)) \cdot \ldots \cdot (t - \phi(\alpha_n))$. Подставляя β, получаем, нуль. Значит, $\beta = \phi(\alpha_i)$ для некоторого i. $\square$

Следствие 2.2.1. *Любое алгебраическое расширение F вкладывается в алгебраическое замыкание F.*

Следствие 2.2.2. *Алгебраическое замыкание F вкладывается в любое алгебраически замкнутое поле, содержащее F.*

Следствие 2.2.3. *Алгебраическое замыкание единственно с точностью до* ***не единственного*** *изоморфизма.*

2.3 Сепарабельность

Пусть F — поле, $f \in F[t]$.

Определение 2.3.1 (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 $f = \prod\limits_{i=1}^{n} f_i$, 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 2.3.2 ($\alpha \in E$ сепарабелен над F)**.** Минимальный многочлен α сепарабелен.

Определение 2.3.3 (Расширение E/F сепарабельно)**.** $\forall \alpha \in E$: $\alpha \in E$ сепарабелен над F.

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

Примеры (Сепарабельные и несепарабельные расширения).

- Любое расширение поля характеристики нуль сепарабельно.
- Пусть $E \coloneqq \mathbb{F}_p(t)$, $F \coloneqq \mathbb{F}_p(t^p)$ (подполе в E, содержащее только степени t, кратные p). Рассмотрим многочлен $x^p - t^p \in F[x]$. Над $E : x^p - t^p = (x-t)^p$, то есть он раскладывается на кратные линейные множители. Но над F многочлен неприводим, так как легко перечислить все его делители в $E[t]$, и убедиться, что в F они не лежат.

  Получается, $x^p - t^p \in F[x]$ неприводим и несепарабелен. И действительно, $(x^p - t^p)' = px^{p-1} = 0$.

Определение 2.3.4 (Совершенное поле F)**.** Любое алгебраическое расширение F сепарабельно.

Упражнение 2.3.1. *Верно ли, что F совершенно $\iff$ эндоморфизм Фробениуса* $\mathrm{Frob} : F \to F, x \mapsto x^p$ *сюръективен?*

Примеры.

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

  Доказательство. Рассмотрим $\theta \in F^{\mathrm{alg}}$. $|F[\theta]| = q^n$, где $q \coloneqq |F|$. 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: $\left(t^{q^n-1} - 1\right)' = (q^n - 1)t^{q^n-2} = -t^{q^n-2}$, 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 2.3.1. *Пусть E/F — алгебраическое расширение полей. Следующие условия эквивалентны:*

1. *E/F несепарабельно.*
2. *Минимальный многочлен некоторого $\theta \in E$ несепарабелен 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* 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 несепарабельного многочлена делится на p. Используя его, несложно доказать эквивалентность из (упражнение 2.3.1):

Доказательство. Если E/F несепарабельно, 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. $\square$

Упражнение 2.3.2. *Сепарабельное расширение сепарабельного расширения сепарабельно.*

2.4 Расширения Галуа

Определение 2.4.1 (Расширение E/F нормально)**.** Любой неприводимый многочлен из $F[t]$, имеющий корень в E, раскладывается на линейные множители в E

Пример. $\mathbb{Q}\left[\sqrt[3]{2}\right]/\mathbb{Q}$ 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 2.4.2 (Расширение Галуа)**.** Конечное сепарабельное нормальное расширение.

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

Определение 2.4.3 (Группа Галуа расширения Галуа E/F)**.** Группа автоморфизмов E, тождественных на F: $\mathrm{Gal}(E/F) \overset{def}{=} \mathrm{Aut}(E/F)$.

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

2.4.1 Теорема о количестве вложений

Теорема 2.4.1. 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. $0 < n \leqslant [K : F]$
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: $[K : F] = 1 \iff K = F$. Все три пункта очевидны.

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

Зафиксируем какое-то вложение $F[t]/(f_1) \hookrightarrow K$, отождествим $F[t]/(f_1)$ со своим образом $\widetilde{F} \leqslant K$. Используя универсальное свойство простого расширения, получаем, что количество вложений $\widetilde{F} \hookrightarrow E$ (назовём это количество 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 $\phi : \widetilde{F} \hookrightarrow E$ — фиксированное вложение. Отождествим $\widetilde{F}$ и $\phi(\widetilde{F})$. Расширение $K/\widetilde{F}$ порождено корнями f, он по-прежнему раскладывается на линейные множители в E.

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

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

Следствие 2.4.1. *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 $K = F[\alpha_1, \ldots, \alpha_n]$, пусть $f_1, \ldots, f_n$ — минимальные многочлены $\alpha_1, \ldots, \alpha_n$ соответственно.

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

Положим $L \coloneqq E_f$. Теперь выполнена посылка (теорема 2.4.1), 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. Если дополнительно E/F — расширение Галуа, то и подрасширение E/F — сепарабельно. Тогда $\alpha_1, \ldots, \alpha_n$ 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 2.4.1) завершает доказательство. □

Следствие 2.4.2. *Для расширения Галуа:* $|\operatorname{Gal}(E/F)| = [E : F]$.

2.4.2 Лемма Артина

Теорема 2.4.2 (Лемма Артина)**.** Пусть E — поле, и $G \leqslant \operatorname{Aut}(E)$, $|G| < \infty$. Обозначим $F \coloneqq E^G \overset{def}{=} \{\alpha \in E | \forall g \in G : g\alpha = \alpha\}$.

Тогда $[E : F] = |G|$.

Доказательство. Достаточно доказать, что $[E : F] \leqslant |G|$, обратное неравенство следует из (следствие 2.4.1).

Пусть $G = \{\phi_1, \phi_2, \ldots, \phi_n\}$, где $\phi_1 = 1_G = \mathrm{id}_E$. Пусть $m > n, \alpha_1, \ldots, \alpha_m \in E$, докажем, что $\alpha_1, \ldots, \alpha_m$ линейно зависимы над F, то есть что имеет место линейная зависимость $\sum\limits_{i=1}^{m} \alpha_i x_i = 0$.

Заведём систему линейных уравнений $\left\{\sum\limits_{i=1}^{m} \phi_j(\alpha_i)x_i = 0\right\}_{j=1}^{n}$ относительно переменных $x_1, \ldots, x_m$. В ней уравнений меньше, чем неизвестных, поэтому по теореме о размерности пересечения имеется ненулевое решение $\beta_1, \ldots, \beta_m \in E$. Дальше надо доказать, что найдётся решение, где все $\beta_i \in F$.

Выберем набор $\beta_1, \ldots, \beta_m$ с наименьшим количеством ненулевых элементов. Пусть $\beta_i \neq 0$ для некоторого i, отнормируем решение, поделив на β_i. Теперь $\beta_i = 1$. Утверждается, что все $\beta_i \in F$.

От противного: если $\exists k : \beta_k \notin F$, то $\exists l : \phi_l(\beta_k) \neq \beta_k$. Тогда не только $\beta_1, \ldots, \beta_m$ — решение, но и $\phi_l(\beta_1), \ldots, \phi_l(\beta_m)$ — тоже решение, причём их поэлементная разность имеет меньшее количество ненулевых элементов. Получаем противоречие. $\square$

Лекция XII

6 мая 2024 г.

Следствие 2.4.3. *Для любой группы* $G \leqslant \mathrm{Aut}(E)$*:* $\mathrm{Aut}(E/E^G) = G$.

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

2.4.3 Теорема о характеризации расширений Галуа

Теорема 2.4.3 (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. $F = E^{\mathrm{Aut}(E/F)}$ и $[E : F] < \infty$.
4. Для некоторой конечной $G \leqslant \mathrm{Aut}(E)$: $F = E^G$.

Доказательство.

$(1) \Rightarrow (2)$ Аналогично доказательству (следствие 2.4.1). Так как E/F — расширение Галуа, то оно порождено конечным множеством элементов: $E = F[\alpha_1, \ldots, \alpha_n]$. Пусть $f_i \in F[t]$ — минимальные многочлены α_i, и пусть $f \coloneqq f_{i_1} \cdot \ldots \cdot f_{i_k}$, 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. Согласно (теорема 2.2.2), $E = F_f$.

$(2) \Rightarrow (3)$ Согласно (следствие 2.4.1), $|\mathrm{Aut}(E/F)| = [E : F]$. Ясно, что $F \subset \widetilde{F} \coloneqq E^{\mathrm{Aut}(E/F)}$. С другой стороны, по лемме Артина, $[E : \widetilde{F}] = |\mathrm{Aut}(E/F)|$, откуда $[\widetilde{F} : F] = 1$.

$(3) \Rightarrow (4)$ Согласно (теорема 2.4.1), $[E : F] < \infty \Rightarrow |\mathrm{Aut}(E/F)| < \infty$, тем самым, $G \coloneqq \mathrm{Aut}(E/F)$ 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: $G\alpha = \{\alpha_1, \ldots, \alpha_m\}$. Пусть $h(t) \coloneqq (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_m) \in E[t]$. Раскрыв скобки (по теореме Виета)

$$h(t) = t^m - s_1(\alpha_1, \ldots, \alpha_m)t^{m-1} + s_2(\alpha_1, \ldots, \alpha_m)t^{m-2} + \cdots + (-1)^m s_m(\alpha_1, \ldots, \alpha_m)$$

где $s_k(\alpha_1, \ldots, \alpha_m)$ — k-й основной симметрический многочлен, то есть сумма всевозможных произведений вида $\alpha_{i_1} \cdot \ldots \cdot \alpha_{i_k}$ по всем кортежам $1 \leqslant i_1 < \cdots < i_k \leqslant m$. Эти коэффициенты инвариантны под действием G, значит, они лежат в F. Под действием G коэффициенты h остаются на месте, а корни h переходят в корни.

Таким образом, $\forall g \in G : \exists \sigma \in S_m : g(\alpha_i) = \alpha_{\sigma(i)}$. 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. $\square$

2.4.4 Характеризация сепарабельных расширений

Следствие 2.4.4. *Расширение E/F, порождённое конечным числом сепарабельных элементов, вкладывается в расширение Галуа (и, следовательно, сепарабельно).*

Доказательство. Аналогично доказательству (следствие 2.4.1). Пусть $E = F[\alpha_1, \ldots, \alpha_n]$, где α_i сепарабельны. Пусть $f_i \in F[t]$ — минимальный многочлены α_i, и пусть $f \coloneqq f_{i_1} \cdot \ldots \cdot f_{i_k}$, где перемножаются уникальные среди f_i.

f сепарабелен, можно устроить вложение $E \hookrightarrow F_f$ (оно есть, например, согласно (следствие 2.4.1)), а F_f — расширение Галуа согласно (теорема 2.4.3). $\square$

Следствие 2.4.5. *Пусть K/F — расширение полей. Множество элементов K, сепарабельных над F, образует поле.*

Доказательство. $\forall \alpha, \beta \in K : F[\alpha, \beta]$ сепарабельно (следствие 2.4.4), 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 2.4.4 (Чисто несепарабельное расширение K/E)**.** $\forall \alpha \in K \setminus E$: α не сепарабелен над E.

Следствие 2.4.6. *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. Дальше надо проверить, что элементы в K, несепарабельные над F, остались несепарабельными над E, упражнение читателю. $\square$

2.5 Соответствие Галуа

Следствие 2.5.1. *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. $\square$

Теперь у нас всё готово, чтобы установить соответствие Галуа.

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

Теорема 2.5.1 (Соответствие Галуа)**.** Указанные выше отображения $\mathcal{F} \leftrightarrow \mathcal{G}$ — взаимно обратные биекции, удовлетворяющие следующим свойствам:

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

Доказательство.

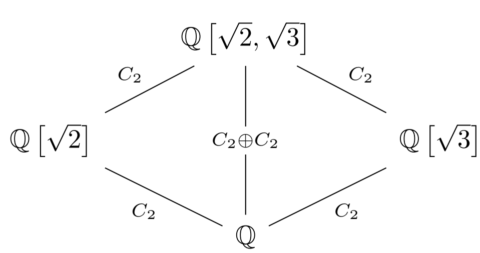
- $\mathrm{Gal}(E/E^H) = H$ — следствие из леммы Артина (следствие 2.4.3).
- $E^{\mathrm{Gal}(E/K)} = K$ согласно теореме о характеризации расширений Галуа (теорема 2.4.3). E/K — расширение Галуа согласно ей же (точнее, (следствие 2.5.1)).
- Монотонность по включению очевидна.
- По лемме Артина $\forall H' \leqslant H \leqslant G : |H : H'| = \frac{|H|}{|H'|} = \frac{\left[E:E^H\right]}{\left[E:E^{H'}\right]} = \left[E^{H'} : E^H\right]$.
- Запишем цепочку равносильностей $\alpha \in E^H \iff \forall h \in H : h(\alpha) = \alpha \iff \forall h \in H : \sigma h \sigma^{-1}(\sigma\alpha) = \sigma\alpha \iff \sigma\alpha \in E^{\sigma H \sigma^{-1}}$.
- $H \trianglelefteqslant G \iff \forall \sigma \in G : \sigma H \sigma^{-1} = H \iff \forall \sigma \in G : \sigma(E^H) = E^H$. Рассмотрим гомоморфизм $\theta : G \to \mathrm{Aut}(E^H/F), \sigma \mapsto \sigma\big|_{E^H}$. Очевидно, $\mathrm{Ker}(\theta) = H$. Покажем, что θ сюръективно. Пусть $\eta \in \mathrm{Aut}(E^H/F)$, покажем, что $\eta \in \mathrm{Im}(\theta)$.

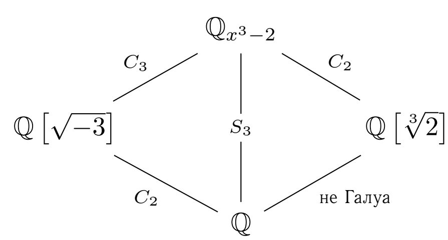
  Расширение E/F нормально, значит, $\exists f \in F[t] : E = F_f$. Тогда и подавно $(E^H)_f = E$. Так как $E = (E^H)_f \cong \eta(E^H)_f$, то по теореме о количестве вложений $\exists$ хотя бы одно вложение $E \to E$ над η (то есть продолжение η, как отображения полей). Итого θ сюръективно.

  Тем самым, $\mathrm{Aut}(E^H/F) \cong G/H$. Теперь заметим, что $F = E^G = (E^H)^{G/H} \Rightarrow E^H/F$ — расширение Галуа, и $\mathrm{Gal}(E^H/F) \cong G/H$.

  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 $H \trianglelefteqslant G$. ☐

Теперь можно нарисовать некоторые картинки:





Здесь одно поле находится над другим, если верхнее — расширение нижнего. Их обычно соединяют просто чертой, а не стрелкой, и на черте написана группа Галуа расширения.

Лекция XIII

20 мая 2024 г.

Определение 2.5.1 (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.

Пусть K и L — подполя большого поля E. Наименьшее подполе в E, содержащее и K, и L, обозначают $K \cdot L$.

Предложение 2.5.1. *Пусть E/F — расширение Галуа, $G \coloneqq \mathrm{Gal}(E/F)$. Выберем подгруппы $P, Q \leqslant G$, и соответствующие им поля $K \coloneqq E^P, L \coloneqq E^Q$, и рассмотрим следующую башню* *полей:*

$$\begin{tikzcd}[arrows=dash]
& E \arrow[d] & \\
& K \cdot L = E^{P \cap Q} \arrow[dl] \arrow[dr] & \\
K = E^P \arrow[dr] & & L = E^Q \arrow[dl] \\
& K \cap L = E^{\langle P \cup Q \rangle} \arrow[d] & \\
& F &
\end{tikzcd}$$

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

Доказательство. Так как $K/K \cap L$ нормально, то $P \trianglelefteq \langle P \cup Q \rangle$. Тем самым, $\langle P \cup Q \rangle = PQ \overset{def}{=} \{pq | p \in P, q \in Q\}$, и $P \cap Q \trianglelefteq Q$, откуда из соответствия Галуа $K \cdot L/L$ нормально.

Согласно теореме Нётер об изоморфизме

$$\mathrm{Gal}(K \cdot L/L) \cong \frac{Q}{Q \cap P} \cong \frac{PQ}{P} \cong \mathrm{Gal}(K/K \cap L) \qquad \square$$

Пусть $f \in F[t]$ — сепарабельный.

Определение 2.5.2 (Группа Галуа многочлена f)**.** $\mathrm{Gal}(f/F) \overset{def}{=} \mathrm{Gal}(F_f/F)$. Если поле F не указано, то логично в качестве него брать наименьшее поле, содержащее коэффициенты многочлена. В частности характеристике нуль выбирается $F := \mathbb{Q}$ (коэффициенты многочлена f).

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

Таким образом, имеет место башня полей

$$\begin{tikzcd}[arrows=dash]
& E_f \arrow[dl] \arrow[dr] & \\
F_f \arrow[dr] & & E \arrow[dl] \\
& E \cap F_f \arrow[d] & \\
& F &
\end{tikzcd}$$

Согласно (предложение 2.5.1), $\mathrm{Gal}(E_f/E) \cong \mathrm{Gal}(F_f/E \cap F_f) \leqslant \mathrm{Gal}(F_f/F)$.

2.6 Применения теории Галуа

2.6.1 Разрешимые группы и субнормальные ряды

Определение 2.6.1 (Разрешимая группа G)**.** Такая группа G, что существует субнормальный ряд с абелевыми *факторами* $1 = G_0 \trianglelefteq G_1 \ldots \trianglelefteq G_n = G$ (факторы ряда — факторгруппы G_{i+1}/G_i).

Лемма 2.6.1. *Группа разрешима $\iff$ существует нормальный ряд с абелевыми факторами, то есть ряд $1 = G_0 \trianglelefteq G_1 \ldots \trianglelefteq G_n$, где все $G_i \trianglelefteq G$.*

Доказательство.

- $\Leftarrow$. Очевидно.
- $\Rightarrow$. Согласно посылке, у группы G есть субнормальный ряд с абелевыми факторами $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$. Построим ряд по алгоритму $\widetilde{G}_{i-1} := \left[\widetilde{G}_i, \widetilde{G}_i\right]$.

Лемма 2.6.2. *Если $H \trianglelefteqslant G$, то $[H, H] \trianglelefteqslant G$.*

Доказательство леммы.

На образующих: $\forall h_1, h_2 \in H : {}^g[h_1, h_2] = [{}^g h_1, {}^g h_2] \in [H, H]$. □

Согласно лемме, это будет нормальный ряд с абелевыми факторами.

Теперь убедимся, что $[G_{i+1}, G_{i+1}] \leqslant G_i$. Профакторизуем обе части предполагаемого выключения по G_i. Слева будет $[G_{i+1}, G_{i+1}]/G_i = [G_{i+1}/G_i, G_{i+1}/G_i] = \{1\}$, так как фактор абелев. Тем самым, включение выполнено.

По индукции легко видеть, что $\widetilde{G}_i \leqslant G_i$, откуда нормальный ряд $\widetilde{G}_n \trianglerighteqslant \widetilde{G}_{n-1} \trianglerighteqslant \ldots$ обрывается на шаге с номером не больше n. □

Определение 2.6.2 (Композиционный ряд)**.** Неуплотняемый субнормальный ряд без повторений. Неуплотняемость означает, что любой фактор — простая (без нормальных подгрупп) группа.

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

Лемма 2.6.3. *Любые два композиционных ряда эквивалентны. Любые два субнормальных ряда обладают эквивалентными уплотнениями. Факторы композиционного ряда изоморфны циклическим группам простого порядка.*

Доказательство. Аналогично теореме Жордана — Гёльдера. □

2.6.2 Основная теорема алгебры

Лемма 2.6.4. *Пусть $|G| = p^n$. Тогда $\exists H \leqslant G : |G : H| = p$.*

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

Теорема 2.6.1 (FTHA)**.** $\mathbb{C} = \mathbb{R}\left[\sqrt{-1}\right]$ алгебраически замкнуто.

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

$G \coloneqq \mathrm{Gal}(E'/\mathbb{R})$, 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 $\left[E' : E'^P\right] = |P| = 2^k$, то $\left[E'^P : \mathbb{R}\right] = m$.

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 полноты $\mathbb{R}$ и непрерывности ($\lim\limits_{x \to -\infty} f(x) = -\infty$ и $\lim\limits_{x \to +\infty} f(x) = +\infty$), получаем, что у f есть корень. Значит, $\deg f = 1$, то есть $\alpha \in \mathbb{R}$. Тем самым, $E'^P = \mathbb{R}$, соответствие Галуа говорит, что $P = G$.

$\mathrm{Gal}(E'/\mathbb{C}) \leqslant \mathrm{Gal}(E'/\mathbb{R})$, откуда $\mathrm{Gal}(E'/\mathbb{C})$ — тоже 2-группа. Согласно (лемма 2.6.4), найдётся $H \leqslant \mathrm{Gal}(E'/\mathbb{C})$ 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, $\mathrm{Gal}(E'/\mathbb{C})$ тривиальна, откуда $E' = \mathbb{C}$, и получается, что у $\mathbb{C}$ нет никаких конечных расширений. □

Лекция XIV

21 мая 2024 г.

2.6.3 Теорема Абеля — Руффини о разрешимости в радикалах

Теорема Дирихле о независимости характеров. Группа Галуа, как базис $\mathrm{End}(E/F)$

Теорема 2.6.2 (Дирихле, о линейной независимости характеров)**.** Пусть H — группа, E — поле, и $\sigma_1, \ldots, \sigma_n : H \to E^*$ — различные групповые гомоморфизмы. Утверждается, что $\sigma_1, \ldots, \sigma_n$ линейно независимы над E в пространстве всех функций $H \to E$.

Доказательство. Предположим наличие линейной зависимости:

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

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

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

где первое получено подстановкой $h \leftarrow gh$ в ($\bigcirc$), а второе — домножением ($\bigcirc$) 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 $\alpha_{n-1}(\sigma_{n-1}(g) - \sigma_n(g)) \neq 0$. □

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

Тогда $\dim_E(\langle \mathrm{Gal}_F(E) \rangle) = n$ — по теореме Дирихле (теорема 2.6.2) все эндоморфизмы вида $\sum\limits_{i=1}^{n} \alpha_i \sigma_i$ различны. С другой стороны, $\dim_F(\mathrm{End}_F(E)) = n^2$, так как $\dim_F(E) = n$, откуда $\langle \mathrm{Gal}_F(E) \rangle = \mathrm{End}_F(E)$, то есть $\sigma_1, \ldots, \sigma_n$ — E-базис пространства $\mathrm{End}_F(E)$.

Первообразный корень и круговой многочлен

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

Определение 2.6.3 ($\varepsilon \in F$ — первообразный корень n-й степени из 1)**.** $\begin{cases} \varepsilon^n = 1 \\ \varepsilon^k \neq 1, \quad 0 < k < n \end{cases}$.

Если в поле есть первообразный корень степени n, то $p \coloneqq \operatorname{char} F \nmid n$: 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 $\varepsilon^0, \varepsilon, \ldots, \varepsilon^{n-1}$ — корни n-й степени из единицы, и многочлен $t^n - 1$ раскладывается на линейные множители. Обозначим множество корней этого многочлена $\mu_n(F)$.

Лемма 2.6.5. *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. E/F — *циклическое расширение Галуа (то есть* $\mathrm{Gal}(E/F) \cong C_n$*).*

Доказательство.

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

- Устроим отображение $\theta : \mathrm{Gal}(E/F) \to E^*, \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$. 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 $\operatorname{Im}\theta \subset \mu_n(F)$.
- Проверим, что это гомоморфизм групп.

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

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

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

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

(2) $\Rightarrow$ (1) Пусть σ — образующая группы Галуа ($\mathrm{Gal}(E/F) = \{1, \sigma, \ldots, \sigma^{n-1}\}$). По теореме Дирихле (теорема 2.6.2), $\sum\limits_{k=0}^{n-1} \varepsilon^k\sigma^k \neq 0$, тем самым, $\exists \beta \in E : \alpha \coloneqq \sum\limits_{k=0}^{n-1} \varepsilon^k\sigma(\beta)^k \neq 0$.

- 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 $\mathrm{Gal}(E/F)$, и $\alpha^n \in F$.

- Покажем линейную независимость $1, \alpha, \ldots, \alpha^{n-1}$ над F, из количественных соображений будет следовать, что это базис E над F. Пусть $\sum\limits_{k=0}^{n-1} \alpha^k x_k = 0$ для неких $x_k \in F$. Применяя σ^j к данному равенству, получаем $\sum\limits_{k=0}^{n-1} \varepsilon^{-kj}\alpha^k x_k = 0$. При $j = 0, \ldots, n-1$ 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. □

Лемма 2.6.6. *Пусть $E \coloneqq F[\varepsilon]$, где ε — первообразный корень степени n. Тогда E/F — расширение Галуа, и $\mathrm{Gal}(E/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ (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 $\sigma \in \mathrm{Gal}(E/F)$ однозначно определён значением $\sigma(\varepsilon)$ (так как $E = F[\varepsilon]$), при этом так как σ оставляет F на месте, то $\sigma(\varepsilon)$ — тоже первообразный корень степени n из 1.

Устроим $\pi : \mathrm{Gal}(E/F) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, сопоставляя элементу $\sigma \in \mathrm{Gal}(E/F)$ 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 $\pi : \mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^*$ — гомоморфизм групп. □

Определение 2.6.4 (Круговой многочлен степени n)**.** $\Phi_n(t) \overset{def}{=} \prod\limits_{\varepsilon}(t - \varepsilon)$, 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 $\Phi_n \in \mathbb{Z}[t] \leqslant \mathbb{Q}[t]$, и там он неприводим, степени $\phi(n)$ (где ϕ — euler totient function).

Теорема Абеля — Руффини

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

Определение 2.6.5 (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 $\beta \coloneqq \alpha_i^k \in F_{i-1}$. В таком случае ещё пишут $F_i = F_{i-1}\left[\sqrt[m]{\beta_i}\right]$.

Теорема 2.6.3 (Абель — Руффини)**.** Пусть F поле, $\operatorname{char} F = 0$; ненулевой $f \in F[t]$. Следующие условия эквивалентны:

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

Доказательство.

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

В силу рассуждения после (определение 2.5.2), $\operatorname{Gal}(f/F_1) \leqslant \operatorname{Gal}(f/F)$, поэтому $G \coloneqq \operatorname{Gal}(f/F_1)$ тоже разрешима. По определению у неё существует субнормальный ряд, и так как G конечна, то его можно уплотнить до композиционного $\{1\} = G_m \trianglelefteqslant G_{m-1} \trianglelefteqslant \ldots \trianglelefteqslant G_1 = G$. Факторгруппы G_i/G_{i+1} — простые абелевы группы, то есть циклические, простого порядка. Положим $F_i \coloneqq ((F_1)_f)^{G_i}$.

Согласно (лемма 2.6.5), 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 2.6.5) недостаёт первообразного корня.

Добавим его: $F_{m+1} \coloneqq (F_m)_{t^k-1}$, где $k \coloneqq k_1 \cdot \ldots \cdot k_m$. Далее хотим получить, что $\operatorname{Gal}(f/F)$ разрешима. Понятно, что $F_f \subset F_m$, поэтому достаточно доказать, что $\operatorname{Aut}(F_m/F)$ разрешима, или даже $\operatorname{Aut}(F_{m+1}/F)$ 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 $\varepsilon, \alpha_1, \ldots, \alpha_m$).

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

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

Все промежуточные расширения абелевы (первое вкладывается в $(\mathbb{Z}/n\mathbb{Z})^*$ согласно (лемма 2.6.6), остальные циклические согласно (лемма 2.6.5)). Соответствие Галуа говорит, что этой башне полей соответствует субнормальный ряд группы $\operatorname{Gal}(\widetilde{E}/F)$ с абелевыми факторами, то есть $\operatorname{Gal}(\widetilde{E}/F)$ разрешима. Её факторгруппа $\operatorname{Gal}(F_f/F)$ тоже разрешима. $\square$