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)**.** Такая диаграмма, что

$$A \underset{\iota_1}{\overset{\pi_1}{\leftrightarrows}} C \underset{\iota_2}{\overset{\pi_2}{\leftrightarrows}} B$$

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

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

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

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

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

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

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

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

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

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

Лемма 1.1.1. $\ker, \mathrm{coker}$ — *функторы* $\mathscr{A}rr\mathscr{A} \to \mathscr{A}rr\mathscr{A}$.

Доказательство. Достаточно доказать для ядер, для коядер двойственно.

Определим действие ker на морфизмах:

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

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

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

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

Интересный факт (Теорема Фрейда — Митчелла (Freyd — Mitchell)). Для любой малой абелевой категории $\mathscr{A}$: $\exists R \in \mathscr{R}ing$ (необязательно коммутативное кольцо с единицей) и строгий, полный, точный функтор $\mathscr{A} \to \mathscr{m}\mathscr{o}\mathscr{d}$-$R$.

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

$$\begin{array}{ccccccc} \mathrm{Ker}\, f & \xrightarrow{\ker f} & A & \xrightarrow{\quad f \quad} & B & \xrightarrow{\mathrm{coker}\, f} & \mathrm{CoKer}\, f \\ & & {\scriptstyle \mathrm{coker}\ker f}\downarrow & & \uparrow{\scriptstyle \ker\mathrm{coker} f} & & \\ & & \mathrm{CoKer}\ker f & \xrightarrow{\exists!} & \mathrm{Ker}\,\mathrm{coker}\, f & & \end{array}$$

Более того, в абелевой категории эта стрелка — изоморфизм.

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

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

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.

$\Leftarrow$. Очевидно.

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

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.

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).

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

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

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

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

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

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

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

Лекция II

19 февраля 2024 г.

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

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

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

Для всякого морфизма f коммутативна диаграмма в категории комплексов:

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

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.

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

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

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, но мы этого делать не будем. □

Ссылаемся на (лемма 1.1.2).

$$\cdots \longrightarrow A_{n+1} \xrightarrow{d^A_n} A_n \xrightarrow{d^A_{n-1}} A_{n-1} \longrightarrow \cdots$$

$$\cdots \longrightarrow B_{n+1} \xrightarrow{d^B_n} B_n \xrightarrow{d^B_{n-1}} B_{n-1} \longrightarrow \cdots$$

$$\cdots \longrightarrow A_{n+1} \oplus B_{n+1} \xrightarrow{d^{A\oplus B}_n} A_n \oplus B_n \xrightarrow{d^{A\oplus B}_{n-1}} A_{n-1} \oplus B_{n-1} \longrightarrow \cdots$$

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

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

1.3 Гомологии

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

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

Ниже мы по произвольному комплексу C строим новые комплексы.

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

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

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

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

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

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

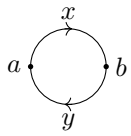
Построение H в терминах универсальных свойств. Так как $d[-1]\cdot d = 0$, то можно пропуститься через ядро: $\exists!\alpha : z\cdot\alpha = d$.

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. □

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

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

Примеры (Гомологии окружности).

- Рассмотрим окружность, как симплициальное множество: 

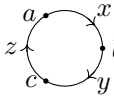
  Построим $C_0 = \mathbb{Z}a + \mathbb{Z}b$ — свободная абелева группа на $\{a, b\}$, $C_1 = \mathbb{Z}x + \mathbb{Z}y$ — тоже свободная абелева группа, но на образующих $\{x, y\}$. Вместо $\mathbb{Z}$ можно было взять любое другое кольцо.

  Все остальные элементы комплекса объявляются нулями.

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

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

  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: $AB + BC + CA$.*

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

Существует длинная точная последовательность гомологических групп

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

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. Сначала строим δ.

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

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

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

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

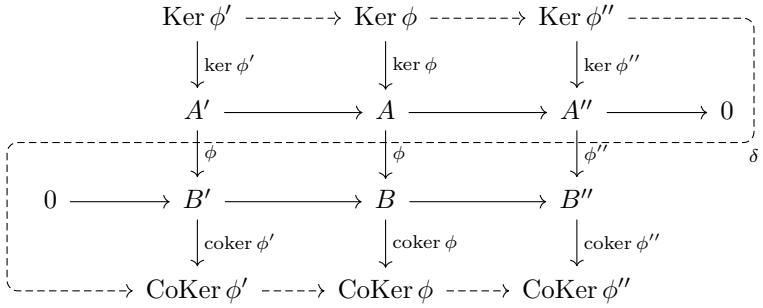
Лекция III

4 марта 2024 г.

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

Лемма 1.3.1 (О змее)**.** *Пусть даны два комплекса $A' \to A \to A'' \to 0$ 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).



Доказательство. Диаграммный поиск. □

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

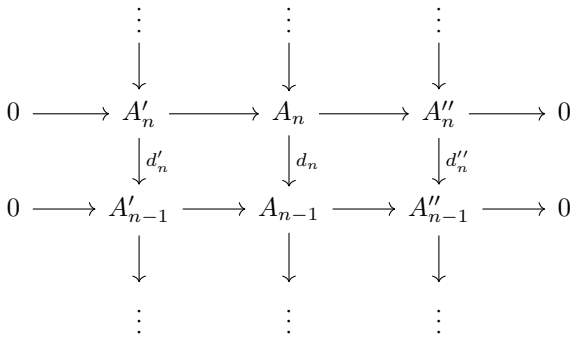
Существует длинная точная последовательность гомологических групп

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

где связующий морфизм δ будет построен в доказательстве.

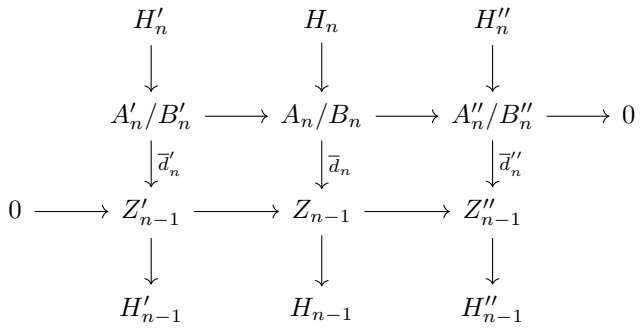
Более того, это всё функториально.

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



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.



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.

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: $\mathscr{F}(0) = 0, \mathscr{F}(\mathrm{coker}(\phi)) = \mathrm{coker}(\mathscr{F}(\phi))$.*
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», поэтому всякий аддитивный функтор сохраняет его.

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

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

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

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

Следствие 1.4.1. *Левый сопряжённый функтор точен справа.*

Доказательство. Он сохраняет копределы. □

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

К сожалению, в лемме о змее это не помогает в доказательстве того, что последовательность точна в члене $\mathrm{Ker}\,\phi$, 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

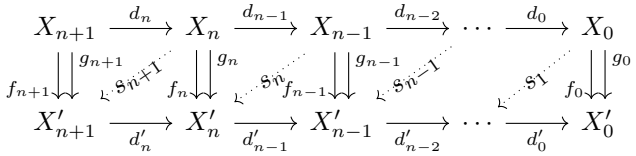
11 марта 2024 г.

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. □

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.



Пишут $f \simeq g$.

А почему это то же самое, что и гомотопность в топологии?

Теорема 1.4.1. Если два морфизма комплексов $f, g : X \to X'$ гомотопны, то $H(f) = H(g)$ (гомологии являются функтором, и действуют не только на комплексах, но и на морфизмах между ними).

Доказательство. Докажем, что $H(f - g) = 0$.

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

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, и $f \simeq g$ — морфизмы комплексов с объектами из $\mathscr{A}$, то (допуская вольность речи можно писать $\mathscr{F}(f)$) $\mathscr{F}(f) \simeq \mathscr{F}(g)$.

Факт 1.4.2. *Быть гомотопными — отношение эквивалентности.*

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

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

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)**.** $\mathrm{id}_X \simeq 0_X$.

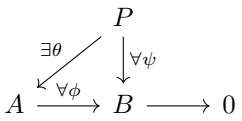
Замечание. Из (теорема 1.4.1) следует, что стягиваемый комплекс ацикличен.

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

1.5 Резольвенты

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

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



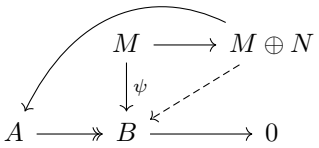
Факт 1.5.1. *В $\mathscr{Set}$ все множества — проективные объекты.*

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

Доказательство.

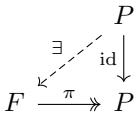
1. Свободный модуль проективен: пусть $\{p_\alpha\}$ — базис P. Определим $\theta(p_\alpha) = \psi(\phi^{-1}(p_\alpha))$, где прообраз выбран произвольно, и продолжим по линейности.

2. Прямое слагаемое проективного модуля проективно. Рассмотрим каноническое вложение $M \hookrightarrow M \oplus N$, где $M \oplus N$ — проективен.



   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).



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

Примеры.

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

Определение 1.5.2 (Проективная резольвента модуля M)**.** Ациклический 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.

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 Резольвенты. 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 $\rightsquigarrow$.

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

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

Раз $\mathscr{F}$ 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 (и ноль в верхней строчке вообще-то неважен), снизу — точный комплекс.

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

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

Доказательство.

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

  $Q_0 \to B$ сюръективно, значит, найдётся f_0, такое, что квадрат коммутативен.

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

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

  Хочется заполучить стрелку $P_{n+1} \to Q_{n+1}$, воспользовавшись проективностью P_{n+1}. Для этого надо найти сюръективное $Q_{n+1} \to ?$. Так как внизу — точная последовательность, то $Q_{n+1} \to \operatorname{Ker}(d^Q_{n-1})$ подойдёт: оно сюръективно, так как $P_{n+1} \to P_{n-1}$ нулевой, а квадрат $\begin{array}{ccc} P_n & \longrightarrow & P_{n-1} \\ \downarrow & & \downarrow \\ Q_n & \longrightarrow & Q_{n-1} \end{array}$ коммутативен. Тем самым, по определению проективного модуля $\exists f_{n+1}$.

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

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

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

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h_1} & \swarrow{\scriptstyle s_0} & \downarrow{\scriptstyle h_0} & \swarrow{\scriptstyle 0} & \downarrow{\scriptstyle 0} & \swarrow{\scriptstyle 0} & \\ \cdots & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \xrightarrow{d^Q_{-1}} & B & \longrightarrow & 0 \end{array}$$

s_0 строится по основному свойству проективного модуля P_0: ведь $h_0(P_0) \subset \operatorname{Ker}(d^Q_{-1}) = \operatorname{Im} d^Q_0$

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

$$\begin{array}{ccccccc} & & P_n & \xrightarrow{d^P_{n-1}} & P_{n-1} & \xrightarrow{d^P_{n-2}} & P_{n-2} \\ & \swarrow{\scriptstyle s_0} & \downarrow{\scriptstyle h_n} & \swarrow{\scriptstyle s_{n-1}} & \downarrow{\scriptstyle h_{n-1}} & \swarrow{\scriptstyle s_{n-2}} & \\ Q_{n+1} & \xrightarrow{d^Q_n} & Q_n & \xrightarrow{d^Q_{n-1}} & Q_{n-1} & & \end{array}$$

Хочется, чтобы выполнялось $h_n = d^Q_n s_n + s_{n-1} d^P_{n-1}$, эквивалентно $d^Q_n s_n = h_n - s_{n-1} d^P_{n-1}$.

Надо проверить, что образ правой части лежит в $\operatorname{Im}(d^Q_n)$, то есть $\operatorname{Ker}(d^Q_{n-1})$. Применим d^Q_{n-1}. Получим

$$d^Q_{n-1} h_n - d^Q_{n-1} s_{n-1} d^P_{n-1} = h_{n-1} d^P_{n-1} - (h_{n-1} - s_{n-2} d^P_{n-2}) d^P_{n-1} = 0$$

Тем самым, s_n действительно найдётся согласно свойству проективного модуля.

□

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

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

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

Таким образом, определение левого производного функтора L_n корректно.

С некоторой точки зрения «правильно» рассматривать категорию комплексов с точностью до гомотопической эквивалентности, назовём её $\mathscr{HoComp}(\mathscr{A})$: там объекты — $\operatorname{Obj}\mathscr{A}$, а группа морфизмов $\operatorname{Mor}_{\mathscr{HoComp}(\mathscr{A})}(P, Q) = \operatorname{Mor}(\mathscr{Comp}(\mathscr{A}))/\operatorname{Ho}(P, Q)$, 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. $L_0\mathscr{F}(A) = H_0(\mathscr{F}(P)) = \operatorname{CoKer}(\mathscr{F}(P_1) \to \mathscr{F}(P_0))$. Если функтор точен справа, то $\operatorname{CoKer}(\mathscr{F}(P_1) \to \mathscr{F}(P_0)) = \mathscr{F}(A)$.

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

- Обратно, если $L_0\mathscr{F} = \mathscr{F}$, то $\mathscr{F}$ сохраняет коядра, значит, точен справа. (По-хорошему, 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

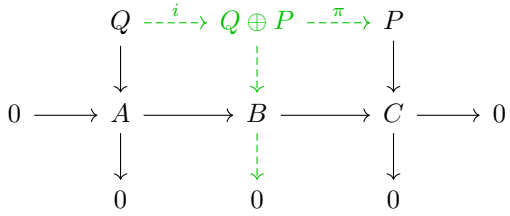
Зафиксируем некоторый функтор $\mathscr{F}$. Далее мы исследуем $L_n\mathscr{F}$, для упрощения записи будем писать $L_n \coloneqq L_n\mathscr{F}$.

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

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

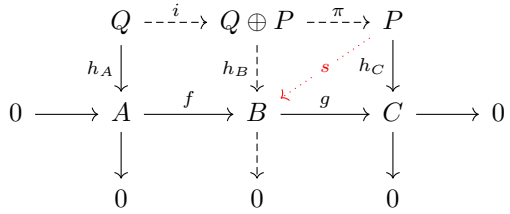
Для получения такой штуки было бы неплохо заполучить точную последовательность резольвент $P_A \to P_B \to P_C$, причём не абы какую, а сохраняющую свою точность под действием любого аддитивного функтора. Оказывается, это сделать несложно, и в этом нам поможет лемма о подкове.

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



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 $gs = h_C$.



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

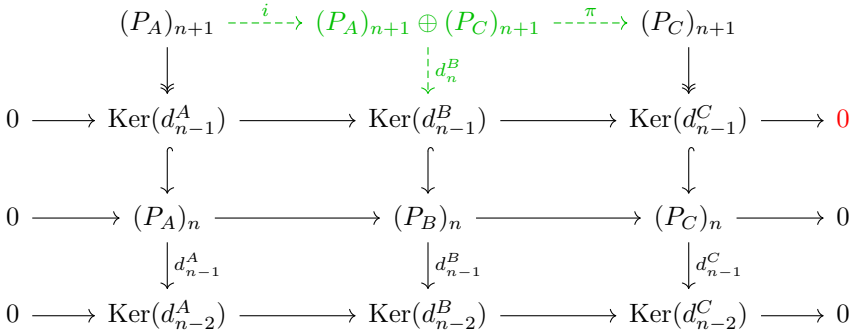
При таком определении правый квадрат будет коммутативен: $g(s(v)) = h_C(\pi(u, v)) \overset{?}{=} g(h_B(u, v)) = g(s(v))$, так как $gf = 0$.

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

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.

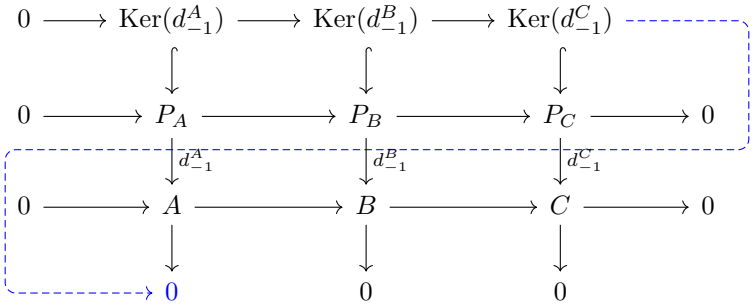
Доказательство. Возьмём произвольные резольвенты P_A, P_C. Резольвенту P_B будем строить пошагово, по индукции. $(P_B)_0 \coloneqq (P_A)_0 \oplus (P_C)_0$ строится прямым применением леммы о подкове.

Далее необходимо провести индукционный переход.



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.

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



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

Тем самым, 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. □

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. □

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

Лекция VI

25 марта 2024 г.

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 $\{\mathscr{F}_i\}_{i\in\mathbb{N}}$, 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 $\{L_i\mathscr{F}\}_{i\in\mathbb{N}}$ — 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:

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

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:

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

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, $M \in \mathscr{mod}\text{-}R, N \in R\text{-}\mathscr{mod}$, напомним, что тогда $M \otimes_R N \in \mathscr{Ab}$.

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

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 $0 \to M \xrightarrow{m\otimes r \mapsto m\otimes ar} M \to M \otimes R/aR \to 0$. Так как кольцо коммутативное, то тензорное произведение — $\mathscr{mod}\text{-}R$, 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 $\{x \in M | ax = 0\}$.

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

Идея доказательства.

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

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

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

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

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

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

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

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

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

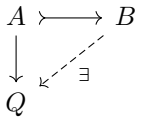
1.8 Производные функторы для Hom

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

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

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

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



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

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

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

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

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 $\mathrm{Ext}^i(M,N)$.

Построив 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)

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

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

Лекция VII

1 апреля 2024 г.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.9 Гомологии и когомологии групп

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

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

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

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, $\phi(1) \in A^G \stackrel{def}{=} \{a \in A | \forall g \in G : ga = a\}$ — *инварианты*. Значит, нулевые когомологии — инварианты.

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

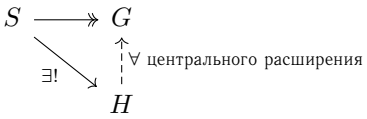
- $H^1(G, A) = \mathrm{Der}(G, A)$ — множество скрещённых гомоморфизмов.

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



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.

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

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

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

- 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 $F[t]$ — наименьшее подполе, 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 K является, например, $(1, \bar{t}, \dots, \bar{t}^{\deg(p)-1})$.

□

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

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

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

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

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

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

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

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

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

Теорема 2.1.1. Следующие условия равносильны

1. Расширение K/F конечно.
2. K/F — алгебраическое и конечнопорождённое.
3. $K = F[\alpha_1, \ldots, \alpha_n]$, 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 трансцендентности 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.

2.1.1 Алгебраическое замыкание одного поля в другом

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

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

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

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

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

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

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

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

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

1. todo
2. todo
3. todo

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

Теорема 2.1.2. Степень трансцендентности не зависит от выбора базиса.

Доказательство. Аналогично подобному факту из линейной алгебры. □

2.1.2 Поле разложения

Пусть F — поле, $f \in F[t]$.

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

Примеры.

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

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

Доказательство. Индукция по $\deg f$.

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

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

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

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

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

Пусть K/F и L/F — расширения полей. Тогда гомоморфизм $\phi : K \to L$ 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 2.1.4. Пусть K — поле, в котором $f \in F[t]$ раскладывается на линейные множители. Тогда K — поле разложения $f \iff K \cong F[\alpha_1, \ldots, \alpha_n]$, где α_i — корни f.

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

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

Лекция IX

16 апреля 2024 г.

Лемма 2.1.4. *Пусть K/F и L/F — конечные расширения, и $K \to L, L \to K$ — гомоморфизмы над F. Тогда $K \cong L$ (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 $\dim_F K = \dim_F L$. □

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

Доказательство. Так как F — векторное пространство над $\mathbb{F}_p$, то $F \overset{\mathbb{F}_p\text{-}\mathscr{V}ect}{\cong} \mathbb{F}_p^n$ для некоторого $n \in \mathbb{N}$. □

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

Доказательство.

- Обозначим $q \coloneqq p^n \in \mathbb{N}$. 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, $F \coloneqq (\mathbb{F}_p)_f$ 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 и умножения:

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

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

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

  С другой стороны, X содержит все корни $t^q - t$, а F — поле разложения $t^q - t$, значит, имеется и гомоморфизм $F \to X$. $X/\mathbb{F}_p$ и $F/\mathbb{F}_p$ конечны, откуда (лемма 2.1.4) $X = F$.
- Пусть E — произвольное поле порядка p^n. Его характеристика равна p, значит, в него вкладывается $\mathbb{F}_p$. $|E^*| = q - 1$, значит по теореме Лагранжа (о порядке элемента в группе) $\forall x \in E : x^{q-1} = 1$. Тем самым, f раскладывается на линейные множители и в E, откуда опять же имеется вложение $F \hookrightarrow E$. Но $|F| = |E| = q$, значит, $F \cong E$. □

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

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

Доказательство. Тривиально.

(1) $\Rightarrow$ (2) Тавтологично.

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

(3) $\Rightarrow$ (4) Пусть E/F — алгебраическое расширение, выберем $\theta \in E$, и найдём его минимальный многочлен. Он неприводим $\Rightarrow \deg f = 1$, то есть $\theta \in F$.

(4) $\Rightarrow$ (5) Тавтологично.

(5) $\Rightarrow$ (1) Рассмотрим $f \in F[t]$. $F_f = F \Rightarrow$ все корни f лежат в F. Так как f неприводим, то $\deg f = 1$.

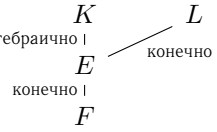
□

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

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

Доказательство. Пусть f – неприводимый в $K[t]$. Без потери общности f — 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.



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

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

Лемма 2.1.8. *Пусть L/F — расширение полей, причём L алгебраически замкнуто. Тогда* $\mathrm{Int}_L F$ *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 $\alpha_i \in L$. Согласно (**??**) целого замыкания $\alpha_i \in \mathrm{Int}_L F$. □

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

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

Теорема 2.1.6. У любого поля F существует алгебраическое замыкание.

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

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

Доказательство леммы.

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

$$g_1 f_1(x_{f_1}) + \cdots + f_m f_m(x_{f_m}) = 1, \text{ где } f_i, g_i \in F[t] \qquad (\triangle)$$

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. □

Раз $J \trianglelefteqslant F[X]$ 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 2.1.7) неприменима, так как неизвестно, алгебраично ли расширение E_1/F.

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 $F^{\text{alg}} \coloneqq \text{Int}_{\overline{F}} F$, оно алгебраически замкнуто, согласно (лемма 2.1.8). □

Лекция X

22 апреля 2024 г.

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

2. Предположим, что ϕ существует. Корень $f \in F[t]$ переходит в корень, поэтому ϕ сохраняет множество алгебраических элементов, откуда $\phi(E \subset K$.

3. Рассмотрим $\beta \in K$, это корень некоторого 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. □

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

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

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

2.1.3 Сепарабельность

Пусть F — поле, $f \in F[t]$.

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

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

Если $f = \prod\limits_{i=1}^{n} f_i$, 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 2.1.10 ($\alpha \in E$ сепарабелен над F)**.** Минимальный многочлен α сепарабелен.

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

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

Примеры (Сепарабельные и несепарабельные расширения).

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

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

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

Упражнение 2.1.1. *Верно ли, что F совершенно $\iff$ эндоморфизм Фробениуса* $\mathrm{Frob} : F \to F, x \mapsto x^p$ *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. □

Лекция XI

29 апреля 2024 г.

Предложение 2.1.2. *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 $(t - \theta^p) \mid g \Rightarrow (t - \theta)^p = t^p - \theta^p \mid f$. □

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

Упражнение 2.1.2. *Сепарабельное расширение сепарабельного расширения сепарабельно.*

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

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

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

что противоречит неприводимости f. □

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

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

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

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

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

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

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

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

1. $0 < n \leqslant [K : F]$
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: $[K : F] = 1 \iff K = F$.

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 имеют степень 1. Без потери общности f_1 имеет корень в $K \setminus F$. Если такой существует, то выберем f_1, как несепарабельный многочлен, имеющий корень в K.

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

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

Пусть $\phi : \widetilde{F} \hookrightarrow E$ — 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 2.1.4. *Пусть K/F и E/F — конечные расширения.*

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

Доказательство. Пусть $K = F[\alpha_1, \ldots, \alpha_n]$, 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 2.1.7), откуда количество вложений $K \hookrightarrow L$ над F не 0, но и не более $[K : F]$.

Если существует вложение $K \hookrightarrow E$ над F, то все f_i имеют корни в E и K/F сепарабельно. Тогда $\alpha_1, \ldots, \alpha_n$ 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 2.1.7) завершает доказательство. □

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

Теорема 2.1.8 (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 2.1.4).

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.

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 $\beta_1, \ldots, \beta_m \in E$. Без потери общности $\beta_1 = 1$ (можно все β_i поделить на β_1).

Пусть в наборе $\beta_1, \ldots, \beta_m$ наименьшее количество ненулевых элементов. Если $\exists k : \beta_k \notin F$, то $\exists l : \phi_l(\beta_k) \neq \beta_k$. Вычитая решения, получаем противоречие. □

Лекция XII

6 мая 2024 г.

Следствие 2.1.6. *Для любой группы* $G \leqslant \operatorname{Aut}(E)$*:* $\operatorname{Aut}(E/E^G) = G$.

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

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

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

Доказательство.

(1) ⇒ (2) Аналогично доказательству (следствие 2.1.4). Так как E/F — расширение Галуа, то оно порождено конечным множеством элементов: $E = F[\alpha_1, \ldots, \alpha_n]$. Пусть $f_i \in F[t]$ — 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, как произведение взаимно простых сепарабельных многочленов, E порождено корнями f, и так как E/F нормально, то f разложим на линейные множители в E. Тем самым, $E = F_f$.

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

(3) ⇒ (4) Согласно (теорема 2.1.7), $[E : F] < \infty \Rightarrow |\operatorname{Aut}(E/F)| < \infty$, тем самым, $G \coloneqq \operatorname{Aut}(E/F)$ 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)

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

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 $1 \leqslant i_1 < \cdots < i_k \leqslant m$.

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

2.1.4 О сепарабельных расширениях

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

Доказательство. Аналогично доказательству (следствие 2.1.4). Так как E/F — расширение Галуа, то оно порождено конечным множеством элементов: $E = F[\alpha_1,\ldots,\alpha_n]$. 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 2.1.4)), а F_f — расширение Галуа согласно (теорема 2.1.9). □

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

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

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

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

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

Доказательство. Выберем за E сепарабельное замыкание F в K. Дальше упражнение. □

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

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

2.2 Соответствие Галуа

Теперь у нас всё готово, чтобы установить соответствие Галуа.

E/F — расширение Галуа, $G \coloneqq \mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$. Пусть $\mathcal{F} \coloneqq \{K \mid F \leqslant K \leqslant E\}$, 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 2.2.1 (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 $\mathrm{Gal}(E^H/F) \cong G/H$.

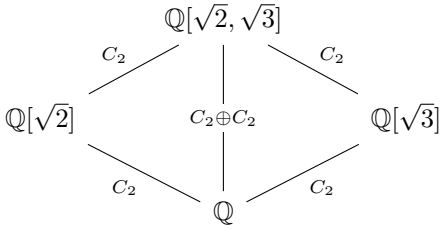
Доказательство.

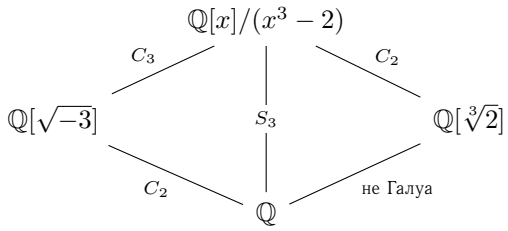
- $\mathrm{Gal}(E/E^H) = H$ — следствие из леммы Артина.
- $E^{\mathrm{Gal}(E/K)} = K$ согласно (теорема 2.1.9). Согласно ей же, E/K — расширение Галуа.
- По теореме Лагранжа $|H' : H| = \frac{|G:H'|}{|G:H|} = \frac{\left[E:E^H\right]}{\left[E:E^{H'}\right]} = \left[E^{H'} : E^H\right]$.
- $\forall h \in H : \sigma h \sigma^{-1}(\sigma(\alpha)) = \sigma h(\alpha) = \sigma(\alpha) \Rightarrow \sigma(E^H) \leqslant E^{\sigma H \sigma^{-1}}$. Обратное включение получается заменой $\widetilde{H} \coloneqq \sigma H \sigma^{-1}$ и $\widetilde{\sigma} \coloneqq \sigma^{-1}$.
- $H \trianglelefteqslant G \iff \forall \sigma \in G : \sigma H \sigma^{-1} = H \iff \forall \sigma \in G : \sigma(E^H) = E^H$. 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. 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:





Лекция XIII

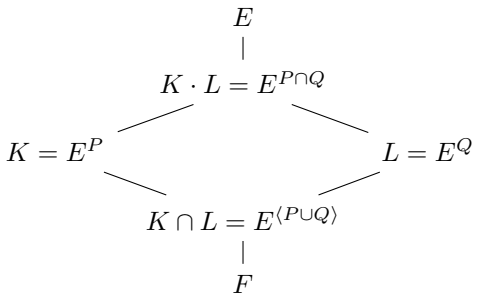
20 мая 2024 г.

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

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

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

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



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

Согласно теореме Нётер об изоморфизме

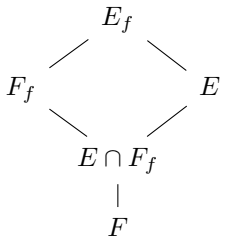
$$\mathrm{Gal}(KL/L) \cong \frac{Q}{Q \cap P} \cong \frac{PQ}{P} \cong \mathrm{Gal}(K/K \cap L) \qquad \square$$

Пусть $f \in F[t]$.

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

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

Таким образом, имеет место башня полей



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

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

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

Доказательство.

$\Leftarrow$. Очевидно.

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

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

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

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

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

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 2.2.2 (FTHA)**.** $\mathbb{C} = \mathbb{R}\left[\sqrt{-3}\right]$ алгебраически замкнуто.

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

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

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

$\mathrm{Gal}(E'/\mathbb{C}) \leqslant \mathrm{Gal}(E'/\mathbb{R})$, откуда $\mathrm{Gal}(E'/\mathbb{C})$ — тоже 2-группа. Согласно (лемма 2.2.3), 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 у $\mathbb{C}$ нет никаких конечных расширений. □

Лекция XIV

21 мая 2024 г.

Теорема 2.2.3 (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:

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

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 ($\circlearrowleft$), а второе — домножением ($\circlearrowleft$) 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 $n \coloneqq [E:F]$, $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Gal}(E/F) \leqslant \mathrm{End}(E/F) \overset{def}{=} \mathrm{End}_F(E)$.

Тогда $\dim_E(\langle \mathrm{Gal}_F(E)\rangle) = n$ — по теореме Дирихле (теорема 2.2.3) 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 $\mathrm{End}_F(E)$.

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

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

Если в поле есть первообразный корень степени n, то $\mathrm{char}\, F \nmid n$: 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 2.2.4. *Пусть E/F — расширение полей, и в базовом поле F есть первообразный корень степени n из 1. Следующие условия эквивалентны.*

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

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 $\mathrm{Im}\,\theta \subset \mu_n(F)$.
- Проверим, что это гомоморфизм групп.

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

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

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

- 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 2.2.3), $\sum\limits_{k=0}^{n-1} \varepsilon^k\sigma^k \neq 0$, 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 2.2.5. *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 преобразование σ обратимо, 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 2.2.6 (Круговой многочлен степени n)**.** $\Phi_n(t) \stackrel{def}{=} \prod\limits_{\varepsilon}(t - \varepsilon)$, 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 $\prod\limits_{k \mid n} \Phi_k(t) = \prod\limits_{\varepsilon^n=1} (t-\varepsilon) = t^n - 1$.

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).

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

Определение 2.2.7 (Уравнение $f = 0$ разрешимо в радикалах)**.** Все корни f (лежащие в алгебраическом замыкании F) выражаются через элементы F при помощи арифметических операций и извлечений корня. Иными словами, существуют цепочка полей $F = F_0 \hookrightarrow F_1 \hookrightarrow \cdots \hookrightarrow F_m$, 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 $F_i = F_{i-1}\left[\sqrt[n]{\beta_i}\right]$.

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

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

$\mathrm{Gal}(f/F_1) \leqslant \mathrm{Gal}(f/F)$, поэтому $G \coloneqq \mathrm{Gal}(f/F_1)$ тоже разрешима. По определению у неё существует субнормальный ряд, и видимо так как G конечна его можно уплотнить до композиционного $\{1\} = G_m \trianglelefteqslant G_{m-1} \trianglelefteqslant \ldots \trianglelefteqslant G_1 = G$. 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 2.2.4), F_i имеет вид $F_{i-1}[\alpha_i]$, что по определению означает разрешимость в радикалах.

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

Добавим его: $F_{m+1} \coloneqq (F_m)_{t^k-1}$, где $k \coloneqq k_1 \cdot \ldots \cdot k_m$. Далее хотим получить, что $\mathrm{Gal}(f/F)$ разрешима. Понятно, что $F_f \subset F_m$, поэтому достаточно доказать, что $\mathrm{Aut}(F_m/F)$ разрешима, или даже $\mathrm{Aut}(F_{m+1}/F)$ 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 $\mathrm{Gal}(E/F) = \{\sigma_1, \ldots, \sigma_n\}$. Поле $\widetilde{E} = F[\varepsilon, \sigma_i(\alpha_j)] \subset E$ тоже нормально над F, так как оно устойчиво под действием $\mathrm{Gal}(E/F)$. А для этого поля есть хорошая цепочка (порождающие присоединяются по одному, все образы α_{j+1} добавляются после всех образов α_j):

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

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