Теория колец

МГУ имени М. В. Ломоносова, Москва

весна 2023

Версия от 27 апреля 2023г.

1 Ассоциативные кольца. Модули. Простые модули и кольца.

Лекция 1. Ассоциативные кольца. Идеалы. Гомоморфизмы.

Определение 1.1. *Ассоциативное кольцо с единицей* — это множество R с заданными на нём операциями сложения «+» и умножения « $\cdot$ » так, что

1. R — абелева группа по сложению,
2. R — моноид (полугруппа с единицей 1) по умножению,
3. выполнены две аксиомы дистрибутивности:

$$\forall a, b, c \in R\colon\ c(a+b) = ca + cb \ \ \&\ \ (a+b)c = ac + bc.$$

В нашем курсе слово «кольцо» всегда будет означать ассоциативное кольцо с единицей.

Определение 1.2. Пусть подмножество S кольца R содержит его единицу и само является кольцом относительно тех же операций. Тогда S будем называть *подкольцом* R. [1]

Определение 1.3. Элементы a, b кольца R *коммутируют (перестановочны)*, если $ab = ba$. Элемент $z \in R$ называется *центральным*, если он перестановочен с любым

[1] Другими словами, возможно корректное ограничение на S сигнатуры $(+, \cdot, 0, 1)$ исходного кольца.

элементом кольца R. *Центром* $Z(R)$ кольца называют множество всех его центральных элементов

$$Z(R) = \{z \in R \mid \forall r \in R\colon\ rz = zr\}.$$

Если в кольце R любые два элемента перестановочны, т.е. $Z(R) = R$, то R называют *коммутативным*.

Определение 1.4. Элемент r кольца R *обратим справа*, если существует *правый обратный* к нему элемент, т.е. такой $s \in R$, что $rs = 1$. Аналогично определяется обратимость слева. *Обратимый* элемент r — это элемент, обратимый и справа, и слева; тогда его левый и правый обратный единственны и совпадают, поэтому в этом случае говорят о *(двустороннем) обратном* r^{-1}.

Доказательство корректности. Если $sr = rt = 1$, то $t = (sr)t = srt = s(rt) = s$. □

Позже будет приведен пример кольца с элементами r, s таких, что $rs = 1 \neq sr$.

Определение 1.5. *Тело* — кольцо с $1 \neq 0$, в котором всякий ненулевой элемент обратим. *Поле* — коммутативное тело.

Пример 1.6.

1. Кольцо целых чисел $\mathbb{Z}$. В нём обратимы только ± 1.
2. Примеры полей: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_{p^k}$, рациональные функции от нескольких переменных над полем.
3. Пусть в $H = \mathbb{R}^4$ фиксирован произвольный базис $\{1, i, j, k\}$. Введём умножение на элементах базиса: $i^2 = j^2 = k^2 = ijk = -1$, $a \cdot 1 = 1 \cdot a = a$ для всех $a \in \{i, j, k\}$. Продолжим умножение на всё H по линейности; получится *тело кватернионов* $\mathbb{H}$. Это пример тела, не являющегося полем.
4. *Кольцо $n \times n$-матриц* $M_n(R)$ над кольцом R с операциями $(A + B)_{ij} = (A)_{ij} + (B)_{ij}$, $(A \cdot B)_{ij} = \sum\limits_{k=1}^{n} (A)_{ik}(B)_{kj}$. Единица кольца — единичная матрица E, для которой $(E)_{ij} = \delta_{ij}$ — символ Кронекера. Отметим, что $M_n(M_k(R)) = M_{nk}(R)$.

Определение 1.7. Построим *кольцо формальных степенных рядов* $R[[t]]$. Рассмотрим множество $\{(r_i)_{i=0}^{\infty} \mid r_i \in R\}$ всех бесконечных последовательностей элементов кольца R и определим операции

$$(r_i)_{i=0}^{\infty} + (s_i)_{i=0}^{\infty} = (r_i + s_i)_{i=0}^{\infty}, \quad (r_i)_{i=0}^{\infty} \cdot (s_i)_{i=0}^{\infty} = \left(\sum_{i=0}^{j} r_i s_{j-i}\right)_{j=0}^{\infty}.$$

В этом случае удобно обозначить $(r_i)_{i=0}^{\infty} = \sum\limits_{i=0}^{\infty} r_i t^i$. В частности, элементы R коммутируют с t. Подкольцо в $R[[t]]$, состоящее из всех рядов, в которых лишь конечное число коэффициентов отлично от нуля, называется *кольцом многочленов* от одной переменной $R[t]$.

Замечание 1.8. В алгебре обычно рассматривают суммы только конечного числа слагаемых. В $R[[t]]$ осмысленна запись $(1-t)^{-1} = S = \sum\limits_{i=0}^{\infty} t^i$, поскольку знак суммирования в правой части — это часть определения элемента S. Запись $(1-t)^{-1} = \sum\limits_{i=0}^{\infty} s_i$, где $s_i = t^i \in R[[t]]$, смысла не имеет.

Определение 1.9. *Прямое произведение* $R \times S$ двух колец R, S — множество пар вида (r, s), в котором сложение и умножение производятся покомпонентно. В общем случае, если $\{R_\lambda\}_{\lambda\in\Lambda}$ — произвольное семейство колец, индексированное множеством Λ, то прямое произведение колец этого семейства определяется как множество функций

$$\prod_{\lambda\in\Lambda} R_\lambda = \left\{ f\colon \Lambda \to \bigsqcup_{\lambda\in\Lambda} R_\lambda \mid f(\lambda) \in R_\lambda \right\}$$

с поточечными операциями сложения и умножения. Функцию f часто удобно записывать в виде $f = \prod\limits_{\lambda\in\Lambda} r_\lambda$, где $r_\lambda = f(\lambda)$.

Определение 1.10. *Групповое кольцо* RG группы G — множество формальных сумм $\sum\limits_{g\in G} r_g g$, где лишь конечное число коэффициентов r_g отлично от нуля. Умножение элементов производится в соответствии со структурами кольца и группы. Оно задаётся на произведениях $r_g g \cdot s_h h = r_g s_h gh$ и продолжается на всё RG с сохранением дистрибутивности. Единица кольца — это $1_R 1_G$.

Определение 1.11. Подножество $I \subseteq R$ называется *правым идеалом* кольца R, если

1. I — подгруппа в R по сложению,
2. I замкнуто относительно умножения на элементы R справа:

$$\forall u \in I,\ \forall r \in R\colon\ ur \in I.$$

Аналогично определяется *левый идеал*. *Двусторонний идеал* I, или просто *идеал*, — это подмножество кольца, которое одновременно является и левым, и правым идеалом. Обозначение — $I \lhd R$.

Определение 1.12. Односторонний или двусторонний идеал I назовём *нетривиальным*, если $I \neq \{0\}, R$. Будем говорить, что I *собственный*, если $I \neq R$.

Обратим внимание на простой, но полезный факт: односторонний или двусторонний идеал собственный тогда и только тогда, когда он не содержит 1.

Правый идеал собственный тогда и только тогда, когда он не содержит обратимых справа элементов кольца. Действительно, если элемент u правого идеала I обладает правым обратным $r \in R$, то $1 = ur \in I$.

Пример 1.13.

1. Подмножество матриц с нулевой i-й строкой является правым идеалом в $M_n(R)$, но не левым.

2. Подмножество матриц с нулевым j-м столбцом является левым идеалом в $M_n(R)$, но не правым.

3. В коммутативном кольце любой односторонний идеал является двусторонним.

4. В теле есть только тривиальные односторонние и двусторонние идеалы.

5. В прямом произведении колец $\prod_{\lambda\in\Lambda} R_\lambda$ определен идеал, состоящий из всех функций, которые отличны от нуля лишь в конечном числе точек. Этот идеал называют *прямой суммой колец* $\bigoplus_{\lambda\in\Lambda} R_\lambda$, он собственный тогда и только тогда, когда множество Λ бесконечно.

Определение 1.14. Пусть $M \subseteq R$ — непустое подмножество, не обязательно конечное или счётное. *Правый идеал, порождённый множеством* M, определяется как множество всех возможных правых линейных комбинаций элементов из M с коэффициентами из R

$$MR = \left\{ \sum_{i=1}^{n} m_i r_i \;\middle|\; m_i \in M,\ r_i \in R,\ n \in \mathbb{N} \right\} \subseteq R.$$

Левый идеал RM определяется аналогично. *Идеал, порождённый множеством* M, определяется как

$$RMR = \left\{ \sum_{i=1}^{n} r_i m_i s_i \;\middle|\; m_i \in M,\ r_i, s_i \in R,\ n \in \mathbb{N} \right\} \lhd R.$$

Если $M = \{m_1, \ldots, m_n\}$, то для RMR также используется обозначение: $(m_1, \ldots, m_n)$. В случае $M = \{m\}$ будем для краткости опускать фигурные скобки и писать Rm, mR, RmR.

Пример 1.15. Всякий идеал $\mathbb{Z}$ *главный*, то есть может быть порождён одним элементом, а именно наибольшим общим делителем всех своих элементов.

Определение 1.16. Пусть $I \lhd R$ — идеал. Элементы R разбиваются на смежные классы $\{a + I\}$ по аддитивной подгруппе I в R, причём на этих классах корректно определено умножение из R, поскольку при $i, j \in I$ выполнено $(a + i)(b + j) = ab + ib + aj + ij \in ab + I$. Факторгруппа R/I с этой операцией умножения называется *факторкольцом* кольца R по идеалу I.

Пример 1.17. *Кольцо вычетов* $\mathbb{Z}_n$ — факторкольцо $\mathbb{Z}$ по идеалу (n). При простом $|n|$ оно является полем.

Определение 1.18. *Гомоморфизм колец* — отображение $\varphi\colon R \to S$, сохраняющее все кольцевые операции[2], то есть $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$, $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$, $\varphi(0) = 0$ (это следует из первого свойства), $\varphi(1) = 1$.

В случае коммутативного R всякий элемент $r \in R$ корректно определяет гомоморфизм $R[t] \to R$ *вычисления* значения многочлена: $\sum r_i t^i \mapsto \sum r_i r^i$. Для некоммутативного R такие отображения гомоморфизмами обычно не являются.

В теории колец также нужны отображения, которые сохраняют сложение и умножение, но не переводят единицу R в единицу S, например, вложение $M_n(R)$ в $M_{n+1}(R)$, заданное как

$$\begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix} \mapsto \begin{pmatrix} m_{11} & \cdots & m_{1n} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ m_{n1} & \cdots & m_{nn} & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Такие отображения можно рассматривать как гомоморфизмы *колец без единицы*[3], алгебраических систем несколько иного типа. Для них вместо структуры моноида по умножению достаточно полугруппы. Всякий идеал является кольцом без единицы. Гомоморфизмы, сохраняющие единицу, называют *унитальными*, а другие — неунитальными. В нашем курсе мы по умолчанию будем считать всякий гомоморфизм унитальным, если не указано иного.

Определение 1.19. *Изоморфизм* $\varphi\colon R \to S$ колец — это биективный гомоморфизм. В этом случае обратное отображение автоматически является гомоморфизмом (прямая проверка). В случае, когда между кольцами R, S существует изоморфизм, пишут $R \cong S$.

Теорема 1.20 (о гомоморфизме)**.** Пусть $\varphi\colon R \to S$ — гомоморфизм колец. Тогда *ядро* $\ker \varphi = \varphi^{-1}(0)$ гомоморфизма φ является идеалом кольца R, а *образ* $\varphi(R)$ — это подкольцо в S, и отображение $\pi\colon \varphi(R)R/\ker\varphi$, $\varphi(r) \mapsto \varphi^{-1}(\varphi(r))$, есть изоморфизм.

[2] С точки зрения универсальной алгебры константы $0, 1$ можно понимать как 0-местные операции.

[3] В англоязычных работах для колец без единицы используется термин «rng», который возник как каламбур из фразы «ring without i (identity)».

Теорема 1.21 (о соответствии идеалов)**.** Пусть φ: $R \to S$ — гомоморфизм колец. Тогда φ осуществляет сохраняющее включения взаимно-однозначное соответствие между множеством правых идеалов R, содержащих $\ker\varphi$, и множеством всех правых идеалов кольца $\varphi(R)$.

Определение 1.22. Кольцо называется *простым*, если в нём ровно два идеала: $\{0\}$ и всё кольцо[4].

Любое тело является простым кольцом.

Коммутативное кольцо просто тогда и только тогда, когда все его ненулевые элементы обратимы, то есть оно является полем:

если есть необратимый элемент $a \neq 0$, то (a) состоит из необратимых элементов и поэтому собственный.

Теорема 1.23 (идеалы матричного кольца)**.** Если $I \lhd M_n(R)$ — идеал, тогда для некоторого идеала $J \lhd R$ выполнено $I = M_n(J)$.

Доказательство. Докажем, что требуемый идеал совпадает с $J_1 = \{(A)_{11} | A \in I\}$. Умножением на *матричные единицы* можно, оставаясь в I, любой элемент матрицы из I перевести в верхний левый угол: $E_{1i}BE_{j1} = B_{ij}E_{11}$, поэтому $I \subseteq M_n(J_1)$. Наоборот, из матриц вида jE_{11}, $j \in J_1$, можно собрать произвольную матрицу X из $M_n(J_1)$, а именно $X = \sum\limits_{i,j=1}^{n} E_{i1}((X)_{ij}E_{11})E_{1j}$, и поэтому $M_n(J_1) \subseteq I$. □

Следствие 1.24. Кольцо матриц над простым кольцом просто. В частности, матричное кольцо над телом просто.

Отметим, что в матричном кольце над телом нет собственных идеалов, но есть собственные односторонние идеалы при $n > 1$.

Определение 1.25. *Частичный порядок* $\leqslant$ на множестве X — это отношение, которое

1. рефлексивно ($x \leqslant x$),
2. антисимметрично ($x \leqslant y,\ y \leqslant x \Rightarrow x = y$),
3. транзитивно ($x \leqslant y,\ y \leqslant z \Rightarrow x \leqslant z$).

Определение 1.26. Два элемента $x, y \in X$ называются *сравнимыми*, если выполнено по крайней мере одно из условий: $x \leqslant y$, $y \leqslant x$. В противном случае говорят, что x и y *несравнимые*. *Линейный порядок* — частичный порядок, в котором любые два элемента сравнимы. *Цепь* в частично упорядоченном множестве — это линейно упорядоченное подмножество.

[4]Эта формулировка годится и для колец без единицы.

Пример 1.27.

1. Множество целых чисел $\mathbb{Z}$ линейно упорядочено стандартным образом.
2. Множество делителей натурального числа n частично упорядочено отношением делимости.
3. Если S — множество, то семейство всех его подмножеств 2^S частично упорядочено относительно отношения включения.
4. Множество всех правых идеалов кольца частично упорядочено относительно отношения включения. То же можно сказать про левые и двусторонние идеалы.

Определение 1.28. Пусть Y — подмножество частично упорядоченного множества X. Элемент $a \in X$ называется *верхней гранью* Y, если для всех $y \in Y$ выполнено $y \leqslant a$. Если для Y существует хотя бы одна верхняя грань, то Y называют *ограниченным сверху*. Если верхняя грань принадлежит Y, то её называют *наибольшим элементом* множества Y. Двойственным образом определяются нижняя грань, наименьший элемент и ограниченность снизу.

Определение 1.29. Элемент m частично упорядоченного множества X называется *максимальным*, если $\forall x \in X$ верна импликация $(m \leqslant x \Rightarrow m = x)$. Другими словами, все элементы из $X \setminus \{m\}$ либо меньше m, либо не сравнимы с ним. Минимальный элемент определяется двойственным образом.

Любой наибольший элемент является максимальным, обратное неверно.

Максимальных элементов может быть несколько или не быть вовсе. Наибольший элемент, если существует, единственен.

Теорема 1.30 (лемма Цорна)**.** Пусть в частично упорядоченном множестве $X \neq \varnothing$ для каждого линейно упорядоченного подмножества существует верхняя грань. Тогда в X есть по крайней мере один максимальный элемент.

Определение 1.31. Частично упорядоченное множество X называется *вполне упорядоченным*, если любое его непустое подмножество содержит наименьший элемент.

Теорема 1.32 (Цермело)**.** Любое множество может быть вполне упорядочено.

В системе аксиом теории множеств Цермело — Френкеля лемма Цорна, аксиома выбора и теорема Цермело попарно эквивалентны между собой.

Определение 1.33. Максимальные элементы в множестве всех собственных правых идеалов называют *максимальными правыми идеалами*. Аналогично определяются максимальные левые и двусторонние идеалы.

Из теоремы о соответствии идеалов следует, что идеал $I \lhd R$ максимален тогда и только тогда, когда R/I — простое кольцо.

Теорема 1.34 (Крулль)**.** Пусть $R \neq \{0\}$. Тогда всякий собственный правый идеал I кольца R лежит в некотором максимальном правом идеале. В частности, максимальные правые идеалы существуют. Аналогичные утверждения верны для левых и двусторонних идеалов.

Доказательство. Пусть S — множество всех собственных правых идеалов кольца R, содержащих I. Мы можем ввести частичный порядок на S как отношение включения. Рассмотрим произвольную цепь $\{C_\lambda\}_{\lambda\in\Lambda}$ элементов S. Положим $J = \bigcup\limits_{\lambda\in\Lambda} C_\lambda$. Покажем, что J — собственный правый идеал, содержащий I, т.е., что $J \in S$.

Если $a, b \in J$, то $a \in C_{\lambda_1}$ и $b \in C_{\lambda_2}$. Без ограничения общности можно считать, что $C_{\lambda_2} \subseteq C_{\lambda_1}$. Поэтому $a - b \in C_{\lambda_1} \subseteq J$. Отсюда J — аддитивная подгруппа R. Кроме того, если $r \in R$, то $ar \in C_{\lambda_1} \subseteq J$. Поэтому J — правый идеал. Т.к. все C_λ собственные, то для всех $\lambda \in \Lambda$ выполнено $1 \notin C_\lambda$, откуда $1 \notin J$. Следовательно J собственный. Кроме того, $I \subseteq C_{\lambda_1} \subseteq J$. Поэтому $J \in S$, и J — верхняя грань цепи $\{C_\lambda\}_{\lambda\in\Lambda}$ по построению.

Таким образом, множество S удовлетворяет условиям леммы Цорна, значит, в S имеется по крайней мере один максимальный элемент. □

В нулевом кольце нет максимальных идеалов.

Пример 1.35. Макисмальные идеалы кольца целых чисел $\mathbb{Z}$ — это в точности идеалы вида $(p) = p\mathbb{Z}$, где p — простое число.

Для колец без единицы теорема неверна, например, максимальных идеалов нет в *кольце с нулевым умножением* (все попарные произведения элементов нулевые), аддитивная группа которого изоморфна $\mathbb{Q}$ (см. предложение 1.57 далее).

Предложение 1.36. Пусть $R \neq \{0\}$. Для элемента $a \in R$ следующие условия эквивалентны:

1. a необратим справа,
2. a лежит в некотором собственном правом идеале,
3. a лежит в некотором максимальном правом идеале.

Доказательство.
1) $\Rightarrow$ 2). Если a необратим справа, то $aR = \{ar\colon r \in R\}$ не содержит 1, а значит, является собственным.
2) $\Rightarrow$ 3). Теорема Крулля.
3) $\Rightarrow$ 1). От противного, если a обратим справа, то 1 попадает в идеал. Это противоречит тому, что максимальный идеал собственный. □

Необратимый элемент некоммутативного кольца не обязан лежать в собственном двустороннем идеале (пример — матричное кольцо над полем).

Задачи к лекции 1.

Задача 1. Докажите теорему о гомоморфизме для колец.

Задача 2. Докажите теорему о соответствии идеалов.

Задача 3. Найдите центр кольца матриц $M_n(R)$, $n > 1$, если а) R — поле, б) R — некоммутативное тело, в) R — произвольное кольцо.

Задача 4. Приведите примеры подколец в $M_n(\mathbb{R})$, изоморфных $\mathbb{C}$ и $\mathbb{H}$. Докажите, что $\mathbb{H}$ действительно является телом.

Задача 5. Найдите центр группового кольца RG. Когда оно является коммутативным?

Задача 6. Покажите, что если H — подгруппа группы G, то групповое кольцо RH является подкольцом кольца RG.

Задача 7. Опишите левые (правые) идеалы в кольце матриц над телом.

Задача 8. Докажите, что в бесконечном кольце делителей нуля либо нет, либо бесконечно много.

Задача 9. Покажите, что в бесконечном кольце множество обратимых элементов может быть как конечно, так и бесконечно. Приведите пример кольца мощности не меньше 3, в котором 1 — единственный обратимый элемент.

Задача 10. Пусть R — кольцо, $a, v \in R$, v — обратимый элемент, не равный 1, причём $av = a$. Верно ли, что $a = 0$?

Задача 11. Пусть $\varphi\colon M_n(R) \to S$ — гомоморфизм. Верно ли, что его образ тоже изоморфен матричному кольцу над некоторым кольцом T?

Лекция 2. Модули над кольцами.

Определение 1.37. *Правым модулем* $M = M_R$ над кольцом R, или правым R-модулем, называется абелева группа $(M, +)$ с определёнными на ней операциями умножения справа на элементы кольца R, которые удовлетворяют тождествам

$$\forall a, b \in M,\ r, s \in R,\ a(rs) = (ar)s,\ (a+b)r = ar + br,\ a(r+s) = ar + as,\ a \cdot 1 = a.$$

Симметрично определяется левый модуль ${}_R M$.

Пример 1.38. Приведём примеры модулей:

1. Векторное пространство над полем.
2. Всякая абелева группа обладает естественной структурой $\mathbb{Z}$-модуля.
3. Кольцо R может пониматься как правый R_R или левый ${}_R R$ модуль над собой. Такие модули называют *регулярными*.
4. Любой правый (левый) идеал кольца является правым (левым) модулем.
5. Представления группы G над полем $\mathbb{F}$ соответствуют модулям над групповым кольцом $\mathbb{F}G$.

Определение 1.39. *Гомоморфизм правых R-модулей* — отображение $\varphi\colon M_R \to N_R$, для которого

$$\forall a, b \in M,\ r \in R,\ \varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ar) = \varphi(a)r.$$

Гомоморфизмы левых модулей определяются аналогично. Для левых модулей мы будем писать гомоморфизм справа: $(a)\varphi$. Гомоморфизм модулей называется *изоморфизмом*, если он является биективным отображением. Модули, между которыми имеется изоморфизм, называются *изоморфными* (обозначение $M \cong N$).

Определение 1.40. Пусть M — правый R-модуль. Его аддитивная подгруппа N называется *подмодулем*, если

$$\forall r \in R\ \ \forall u \in N\colon\ ur \in N.$$

Обозначение: $N \leqslant M$. *Фактормодуль* M/N — это аддитивная факторгруппа M/N с операцией умножения на элементы кольца R, заданной как $(m+N)r = mr + N$.

Пример 1.41. Подмодули R_R — это в точности правые идеалы кольца R.

Теорема 1.42 (о гомоморфизме модулей)**.** Пусть $\varphi\colon M \to N$ — гомоморфизм модулей. Тогда $\ker\varphi \leqslant M$, $\varphi(M) \leqslant N$ и отображение $\pi\colon \varphi(M) \to M/\ker\varphi$, $\varphi(m) \mapsto \varphi^{-1}(\varphi(m))$, есть изоморфизм.

Теорема 1.43 (о соответствии подмодулей)**.** Пусть $\varphi\colon M \to N$ — гомоморфизм модулей. Тогда φ осуществляет сохраняющее включения взаимно-однозначное соответствие между множеством подмодулей M, содержащих $\ker\varphi$, и множеством всех подмодулей $\varphi(M)$.

Определение 1.44. Модуль M есть *внутренняя прямая сумма* семейства своих подмодулей $\{M_i \mid i \in I\}$, если всякий элемент $m \in M$ однозначно представляется в виде суммы $\sum\limits_{i\in I} m_i$, где $m_i \in M_i$ и количество ненулевых m_i конечно. Обозначение: $M = \bigoplus\limits_{i\in I} M_i$.

Определение 1.45. Пусть $\{M_i\}_{i\in I}$ — семейство правых R-модулей. Рассмотрим аддитивную абелеву группу $\prod\limits_{i\in I} M_i$ всех отображений вида $f\colon I \to \bigsqcup\limits_{i\in I} M_i$, для которых $f(i) \in M_i$. Полагаем $(f_1 + f_2)(i) = f_1(i) + f_2(i)$. Зададим умножение справа на элементы R: $(fr)(i) = f(i)r$. Таким образом мы определили модуль $\prod\limits_{i\in I} M_i$, называемый *прямым произведением* модулей $\{M_i\}_{i\in I}$. Часто бывает удобно записывать функцию f в виде $f = \prod\limits_{i\in I} m_i$, где $m_i = f(i)$.

Определение 1.46. *Внешняя прямая сумма* $\bigoplus\limits_{i\in I} M_i$ правых R-модулей $\{M_i\}_{i\in I}$ — это подмодуль $\prod\limits_{i\in I} M_i$, состоящий из всех функций f таких, что $f(i) \neq 0$ лишь для конечного числа индексов i. Мы также будем использовать обозначение $f = \bigoplus_{i\in I} m_i$, где $m_i = f(i)$. Заметим, что прямая сумма отличается от прямого произведения только в случае бесконечного числа модулей M_i. В дальнейшем мы будем использовать специальное обозначение для суммы n копий одного и того же модуля $M_R^n = \underbrace{M_R \oplus \ldots \oplus M_R}_{n \text{ раз}}$, где n — натуральное число (в общем случае произвольный кардинал). В частности, R_R^n — сумма n копий регулярного модуля.

Определение 1.47.

- *Система порождающих* $S = \{m_i \mid i \in I\}$ правого R-модуля M — такое подмножество M, что всякий $m \in M$ представляется в виде $\sum\limits_{i\in I} m_i r_i$ (среди r_i лишь конечное число ненулевых). Обозначение $SR = M$, $\langle S\rangle_R = M$ или $\langle S\rangle = M$. Нулевой модуль порождается пустым множеством. Модуль называется *циклическим*, если он порождается одним элементом m, в этом случае будем писать $M = mR$.

- Подмножество $S = \{m_i \mid i \in I\}$ правого модуля M *линейно независимо* (справа), если любая конечная сумма вида $\sum\limits_{i\in I} m_i r_i$, где есть ненулевые $r_i \in R$, также ненулевая. Пустое множество считается линейно независимым.

- *Базис* модуля M — это система его порождающих S, которая удовлетворяет любому из двух эквивалентных условий: 1) S линейно независима; 2) представление любого $m \in M$ в виде линейной комбинации $\sum\limits_{i \in I} m_i r_i$ единственно. В этом случае $M = \bigoplus\limits_{i \in I} m_i R$, где $\{m_i\}$ — одноэлементный базис модуля $m_i R$.
- *Свободный R-модуль* — модуль, обладающий базисом.

Пример 1.48. Приведем примеры свободных модулей.

1. Нулевой модуль 0 считается свободным, его базис — пустое множество.
2. Свободная абелева группа = свободный $\mathbb{Z}$-модуль.
3. Векторное пространство над полем.
4. Регулярный модуль R_R, его базис — это $\{1\}$.
5. Множество матриц $M_n(R)$ — свободный правый или левый R-модуль с базисом из матричных единиц.

Предложение 1.49. Правый модуль M свободен тогда и только тогда, когда он изоморфен прямой сумме копий модуля R_R по некоторому индексному множеству I. При этом достаточно взять I, равномощное выбранному базису M.

Доказательство.
($\Rightarrow$) Пусть $\{m_i\}_{i \in I}$ — базис M. Тогда любое $m \in M$ представимо единственным образом в виде $m = \sum_{i \in I} m_i r_i$. Рассмотрим $N = \bigoplus_{i \in I} R_R$ и определим отображение $\varphi : M \to N$ по правилу $\varphi(\sum_{i \in I} m_i r_i) = \bigoplus_{i \in I} r_i$. Тогда $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$ и $\varphi(ar) = \varphi(a)r$. Значит, φ — гомоморфизм. Отображение φ инъективно, т.к. разложение по базису $\{m_i\}_{i \in I}$ единственно. Кроме того, φ сюръективно по построению.
($\Leftarrow$) Следует из того, что внешняя прямая сумма является внутренней прямой суммой проекций на каждое прямое слагаемое. □

Замечание 1.50. Отметим, что у свободных модулей над некоммутативным кольцом могут быть базисы разных мощностей. В частности, существуют такие кольца R, что имеется изоморфизм правых модулей $R_R \cong R_R^2$ (откуда $R_R \cong R_R^n$ для всех $n \in \mathbb{N}$).

Предложение 1.51. Всякий правый модуль M_R изоморфен фактормодулю некоторого свободного модуля F_R. При этом можно считать, что мощность одного из базисов F_R совпадает с мощностью выбранного порождающего подмножества M_R.

Доказательство. Пусть M порождается множеством S, положим $F_R = \bigoplus\limits_{s\in S} R_R$. Отображение φ: $F_R \to M$, $\bigoplus\limits_{i\in I} r_i \mapsto \sum\limits_{i\in I} m_i r_i$ — сюръективный гомоморфизм правых R-модулей, его образ изоморфен фактору F_R по $\ker\varphi$. □

Предложение 1.52. Все модули над телом свободны.

Доказательство. Пусть M — правый модуль над телом R. Пусть Ω — семейство всех линейно независимых подмножеств M, упорядоченное по включению. Заметим, что $\Omega \neq \varnothing$, т.к. $\varnothing \in \Omega$. Рассмотрим произвольную цепь $\{C_\lambda\}_{\lambda\in\Lambda}$ элементов Ω. Положим $C = \bigcup_{\lambda\in\Lambda} C_\lambda$.

Покажем, что C линейно независимо. Пусть $m_1, \ldots, m_n$ — любые n элементов множества C для произвольного натурального n. Предположим, что $\sum_i m_i r_i = 0$ для некоторых элементов кольца $r_i \in R$. Выберем $C_{\lambda_1}, \ldots, C_{\lambda_n}$ такие, что $m_i \in C_{\lambda_i}$. Поскольку $\{C_\lambda\}_{\lambda\in\Lambda}$ — цепь, то без ограничения общности можно считать, что $C_{\lambda_i} \subseteq C_{\lambda_1}$ для $i = 1, \ldots, n$. Тогда $m_i \in C_{\lambda_1}$ для $i = 1, \ldots, n$. Так как C_{λ_1} линейно независимо, то $r_1 = \ldots = r_n = 0$. Отсюда C — линейно независимо в силу произвольности $m_1, \ldots, m_n$ и n.

Значит, Ω содержит максимальный элемент S по лемме Цорна. Покажем, что S — базис M. Т.к. S линейно независимо, то достаточно показать, что S порождает M. Возьмём произвольный $m \in M$, не лежащий в S. Тогда множество $S \cup \{m\}$ линейно зависимо в силу максимальности S. Значит, для некоторых $m_1, \ldots, m_k \in S$ существуют $r_0, r_1, \ldots, r_k \in R$, не все равные нулю, что $mr_0 + \sum_{i=1}^k m_i r_i = 0$. Заметим, что $r_0 \neq 0$, т.к. иначе мы бы получили линейную зависимость элементов S, что невозможно в силу $S \in \Omega$. Наконец воспользуемся тем, что R — тело. Тогда r_0 обратим, откуда $m = \sum_{i=1}^k m_i r_i r_0^{-1}$. Мы показали, что S порождает M в силу произвольности $m \in M$. □

Определение 1.53. *Неприводимый (простой) модуль* M — это модуль, в котором ровно два различных подмодуля: $\{0\}$, M.

Нулевой модуль не считаем неприводимым.

Пример 1.54.

1. Векторное пространство над полем неприводимо тогда и только тогда, когда оно одномерно.

2. Неприводимые модули групповой алгебры $\mathbb{F}G$ соответствуют неприводимым представлениям группы G.

3. Правый идеал $I \leqslant R_R$ неприводим $\Leftrightarrow$ I — *минимальный* правый идеал (в множестве всех ненулевых идеалов). Кольцо не обязано содержать минимальные правые идеалы (пример — $\mathbb{Z}$).

4. Пусть D — тело. Множество строк $M = \{(d_1, \ldots, d_n) \mid d_i \in D\}$ можно понимать как правый $M_n(D)$-модуль. Умножая на матричные единицы, можно показать, что этот модуль неприводим.

Предложение 1.55. Пусть $M_R \neq 0$. Следующие условия эквивалентны:
1) M неприводимый;
2) для всех $0 \neq m \in M$ выполнено $mR = M$;
3) $M \cong R_R/N$ для некоторого максимального правого идеала N.

Доказательство. 1) $\Leftrightarrow$ 2) наличие нетривиальных подмодулей равносильно наличию нетривиальных подмодулей вида Rm.

3) $\Rightarrow$ 1) По теореме о соответствии идеалов.

2) $\Rightarrow$ 3) Пусть $0 \neq m \in M$, тогда отображение φ: $R_R \mapsto M$, $r \mapsto mr$, — сюръективный гомоморфизм R-модулей, его образ изоморфен $R_R/\ker\varphi$ и неприводим по 1), поэтому $\ker\varphi$ — максимальный правый идеал. □

Следствие 1.56. Неприводимые $\mathbb{Z}$-модули — это в точности конечные циклические группы простого порядка.

Предложение 1.57. Аддитивная абелева группа $\mathbb{Q}$ не содержит максимальных подгрупп, то есть для всякой собственной подгруппы $G_1 \lneq \mathbb{Q}$ существует подгруппа G_2 такая, что $G_1 \lneq G_2 \lneq \mathbb{Q}$.

Доказательство. Предположим, что G — максимальная подгруппа. Тогда $\mathbb{Q}/G$ — неприводимый $\mathbb{Z}$-модуль, т.е. циклическая группа простого порядка p. Для любого $s+G \in \mathbb{Q}/G$ выполнено $p(s+G) = 0+G$. Пусть f — рациональное число, не лежащее в G. Положим $s = f/p \in \mathbb{Q}$, тогда $f + G = p(s + G) = 0 + G$. Значит, $f \in G$. Противоречие. □

Отметим, что для конечно порожденных модулей такого примера построить нельзя.

Теорема 1.58. Пусть M — конечно порожденный правый R-модуль. Тогда любой собственный подмодуль $N \leqslant M$ содержится в некотором максимальном подмодуле.

Доказательство. Пусть M порождён своими элементами $m_1, \ldots, m_n$. Рассмотрим Ω — множество собственных подмодулей M, содержащих N. Тогда

$$\Omega = \{K \lneq M \mid N \leqslant K,\ \{m_i\}_{i=1}^n \not\subseteq K\}.$$

Поэтому к Ω применима лемма Цорна. Непосредственно проверяется, что объединение любой цепи в Ω снова принадлежит Ω. □

Теорема 1.59. Следующие условия для кольца $R \neq \{0\}$ эквивалентны.

1) R — тело.
2) R содержит ровно два правых идеала: 0 и R.
3) R_R — неприводимый модуль.
4) 0 — максимальный правый идеал.
5) Каждый ненулевой элемент R обратим справа.
6) Все правые R-модули свободны.
7) Все конечно порождённые правые R-модули свободны.
8) Все циклические правые R-модули свободны.
9) Существует свободный неприводимый правый R-модуль.
2')–9') Левые аналоги условий 2)–9).

Доказательство. Поскольку 1) симметрично, достаточно доказать эквивалентность условий 1)–9).

1) $\Rightarrow$ 2) Идеал, содержащий обратимые элементы, несобственный.

2) $\Leftrightarrow$ 3), 2) $\Rightarrow$ 4) Сразу из определений.

4) $\Rightarrow$ 5) Если $r \neq 0$ не обратим справа элемент, то rR — нетривиальный правый идеал.

5) $\Rightarrow$ 1) Возьмём ненулевой $r \in R$, тогда, согласно 5), найдётся такой $s \in R$, что $rs = 1$. Снова пользуясь 5), выберем для s такое $t \in R$, что $st = 1$. Заметим, что $t = 1t = (rs)t = r(st) = r$. Поэтому $sr = rs = 1$, т.е. r обратим.

1) $\Rightarrow$ 6) Доказано ранее.

6) $\Rightarrow$ 7) $\Rightarrow$ 8) Получается сразу.

8) $\Rightarrow$ 9) По теореме Крулля существует максимальный правый идеал N. Тогда R/N — неприводимый модуль. По предложению 1.55 он циклический, а значит, свободный в силу 8).

9) $\Rightarrow$ 3) Пусть M — свободный неприводимый модуль, в частности, $M \neq 0$. Выберем произвольный базис M и возьмём в нём любой элемент m. Тогда отображение $r \mapsto mr$ задаёт изоморфизм модулей $R_R \cong mR$. С другой стороны, $M = mR$ ввиду неприводимости. Таким образом, $R_R \cong M$, а значит, R_R неприводим.

□

Определение 1.60. *Алгебра* R над коммутативным кольцом K — это кольцо со структурой K-модуля, причём выполнено $(sr)k = s(rk) = (sk)r$ для $r, s \in R$, $k \in K$. *Гомоморфизм K-алгебр* — это отображение между K-алгебрами, которое одновременно является кольцевым и K-модульным гомоморфизмом.

Пример 1.61. Примеры K-алгебр: $M_n(K)$, $K[[t]]$, $K[t]$, KG. Всякое кольцо можно понимать как $\mathbb{Z}$-алгебру. Также любое кольцо является алгеброй над своим центром.

Определение 1.62. *Свободная n-порождённая алгебра* $K\langle x_1, \ldots, x_n\rangle$ над коммутативным кольцом K — множество конечных формальных K-линейных комбинаций

$\sum\limits_I \lambda_I x_{i_1} \cdots x_{i_k}$, $\lambda_I \in K$, *слов* от x_i, где $I = (i_1, \ldots, i_k)$ — конечные упорядоченные наборы натуральных чисел от 1 до n (набор может быть пустым). Умножение слов $x_{i_1} \cdots x_{i_k} \cdot x_{j_1} \cdots x_{j_m}$ производится конкатенацией, элементы K перестановочны со словами; на всё кольцо умножение продолжается в соответствии с дистрибутивностью. Единица алгебры соответствует пустому слову и отождествляется с 1_K.

Определение 1.63. *Кольцо эндоморфизмов* $\operatorname{End} M_R$ — множество всех гомоморфизмов $M_R \to M_R$, на котором заданы операции сложения $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$ и умножения $(\varphi\psi)(m) = \varphi(\psi(m))$. Роль единицы кольца выполняет тождественное отображение id_M, нуля — нулевое отображение.

Для левых модулей аналогично $(m)(\varphi + \psi) = (m)\varphi + (m)\psi$, $(m)(\varphi\psi) = ((m)\varphi)\psi$.

Замечание 1.64. При вычислениях в модулях удобно писать эндоморфизмы и скаляры по разные стороны от элемента модуля. Поскольку операторы привычнее писать слева от аргументов, далее мы будем рассматривать преимущественно правые модули M_R, хотя многие рассуждения естественным образом переносятся и на левые.

Кроме того, мы будем использовать записи вида $\varphi m r$, $\varphi \in \operatorname{End} M_R$, $m \in M$, $r \in R$, где, заметим, расстановка скобок не требуется.

Теорема 1.65. Пусть $M_R = \sum\limits_{i=1}^{n} M_i$ — конечная прямая сумма. Тогда $\operatorname{End} M_R$ изоморфно кольцу *формальных матриц*, в которых на местах с индексами (i, j) записаны произвольные гомоморфизмы $M_i \to M_j$.

Доказательство. Пусть π_i — естественная проекция из M на M_i, ι_i: — естественное вложение M_i в M. Заметим, что $\pi_i \iota_j = \delta_{ij} \mathrm{id}_{M_j}$ (символ Кронекера), $\sum\limits_{i=1}^{n} \iota_i \pi_i = \mathrm{id}_M$.

Для $f \in \operatorname{End} M_R$ рассмотрим "матрицу" (семейство отображений) $\varphi(f) = (f_{ij})$, где $f_{ij}\colon M_i \to M_j$, $f_{ij} = \pi_j f \iota_i$. Напротив, для семейства отображений $g_{ij}\colon M_i \to M_j$ также определён эндоморфизм $\sum\limits_{i,j=1}^{n} \iota_j g_{ij} \pi_i \in \operatorname{End} M_R$. Это взаимно обратные операции: $\sum\limits_{i,j=1}^{n} \iota_j (\pi_j f \iota_i) \pi_i = \mathrm{id}_M f \mathrm{id}_M = f$, $\sum\limits_{i,j=1}^{n} \pi_j (\iota_j g_{ij} \pi_i) \iota_i = \mathrm{id}_{M_j} g_{ij} \mathrm{id}_{M_i} = g_{ij}$, при этом $\varphi(f + g) = \varphi(f) + \varphi(g)$, $(\varphi(fg))_{ij} = \sum (\varphi(f))_{ik} (\varphi(g))_{kj}$. □

При $M_1 \cong \ldots \cong M_n \cong N$ получаем следующий результат.

Следствие 1.66. $\operatorname{End} N_R^n \cong M_n(\operatorname{End} N_R)$.

Пример 1.67. Приведём пример кольца R такого, что $R \cong M_n(R)$ для всех $n \in \mathbb{N}$. Пусть V — векторное пространство над полем $\mathbb{F}$ со счётным базисом. Положим $R = \operatorname{End}_{\mathbb{F}}(V)$. Заметим, что векторные $\mathbb{F}$-пространства V и $V^n = \underbrace{V \oplus \ldots \oplus V}_{n \text{ раз}}$ изоморфны,

так как обладают базисами одной и той же мощности. Поэтому $R = \operatorname{End}_{\mathbb{F}}(V) \cong \operatorname{End}_{\mathbb{F}}(V^n) \cong M_n(R)$ согласно следствию.

Теорема 1.68. $\operatorname{End} R_R \cong R$, $\operatorname{End}_R R \cong R$.

Для второго изоморфизма важно соглашение, что гомоморфизмы левых модулей пишутся справа.

Доказательство. Рассмотрим отображения $m_r \in \operatorname{End} R_R$, сопоставляющее $x \mapsto rx$, тогда $m_r + m_s = m_{r+s}$, $m_r m_s = m_{rs}$, $m_1 = \mathrm{id}_{R_R}$, откуда отображение $m\colon r \mapsto m_r$ является гомоморфизмом колец R и $\operatorname{End} R_R$. Его ядро тривиально: если $m_r = 0$, то $0 = m_r(1) = r \cdot 1 = r$. Пусть $\varphi \in \operatorname{End} R_R$, тогда для всех $r \in R$ выполнено $\varphi(r) = \varphi(1 \cdot r) = \varphi(1)r = m_{\varphi(1)}(r)$. Поэтому $m : R \to \operatorname{End} R_R$ является биективным гомоморфизмом, откуда $R \cong \operatorname{End} R_R$.

В случае ${}_R R$ полагаем симметрично $(x)m_r = xr$ для всех $x \in R$, и все проверки проводятся аналогично. □

Замечание 1.69. Если в предыдущей теореме R — это алгебра над коммутативным кольцом K, то указанные изоморфизмы являются изоморфизмами K-алгебр.

Определение 1.70. Кольцо R^{opp}, *противоположное* к R, — это кольцо с той же абелевой группой по сложению, умножение в котором «$\cdot_{\mathrm{opp}}$» производится в обратном порядке: $x \cdot_{\mathrm{opp}} y = y \cdot x$.

Замечание 1.71. Если бы мы писали гомоморфизмы левых модулей слева, то в предыдущей теореме $\operatorname{End}_R R$ оказалось бы изоморфно R^{opp}.

Задачи к лекции 2.

Задача 1. Докажите теорему о гомоморфизме для модулей.

Задача 2. Докажите теорему о соответствии подмодулей.

Задача 3. Предъявите взаимно-однозначное соответствие левых идеалов матричного кольца над кольцом R с подмодулями в ${}_R R^n$.

Задача 4. Покажите, что у конечно порождённого правого модуля над телом все базисы содержат одинаковое количество элементов.

Задача 5. Приведите пример модуля, не имеющего базиса.

Задача 6. Приведите пример свободного модуля, имеющего два базиса разных мощностей.

Задача 7. Верно ли, что подмодуль свободного модуля является свободным?

Задача 8. Докажите, что кольцо $\left(\begin{smallmatrix}\mathbb{Z}_4 & \mathbb{Z}_2\\ 0 & \mathbb{Z}_2\end{smallmatrix}\right)$ не изоморфно своему противоположному. Найдите кольцо без единицы наименьшей мощности, не изоморфное своему противоположному.

Задача 9. Покажите, что правый (левый) модуль над кольцом R является левым (правым) модулем над кольцом R^{opp}.

Задача 10. Найдите противоположное к кольцу матриц $M_n(R)$.

2 Артиновы и нётеровы модули и кольца.

Лекция 3. Артиновы и нётеровы модули и кольца. Теорема Жордана — Гёльдера.

Предложение 2.1 (модулярность)**.** Пусть K, L, N — подмодули правого R-модуля M_R такие, что $K \subseteq N$. Тогда выполнено[5] $K + (L \cap N) = (K + L) \cap N$.

Доказательство. Заметим, что $K + (L \cap N) \subseteq K + L$, а также $K + (L \cap N) \subseteq N$ в силу того, что $K \subseteq N$. Поэтому $K + (L \cap N) \subseteq (K + L) \cap N$. Обратно, возьмем $n \in (K+L) \cap N$. Тогда $n = k + l$, где $k \in K$, $l \in L$, и $l = n - k \in L \cap (N + K) = L \cap N$, т.к. $K \subseteq N$. Таким образом, $m = k + l \in K + (L \cap N)$. □

Определение 2.2. Модуль M *артинов*, если выполнено одно из следующих эквивалентных условий:

1) нет бесконечной строго убывающей цепочки подмодулей $M_1 \supset M_2 \supset \dots$;

2) всякая бесконечная нестрого убывающая цепочка $M_1 \supseteq M_2 \supseteq \dots$ подмодулей *стабилизируется (обрывается)*, т.е. существует такое n, что $M_n = M_{n+1} = \dots$;

3) любое непустое семейство подмодулей M содержит минимальный (по включению) элемент.

Доказательство корректности.

2) $\Rightarrow$ 1) Получается сразу.

1) $\Rightarrow$ 3) Пусть S — непустое семейство подмодулей в M, которое не содержит минимального элемента. Выберем любой $M_1 \in S$. Т.к. M_1 не минимальный, то можем взять такой $M_2 \in S$, что $M_2 \subset M_1$. Далее рассматриваем $M_3 \subset M_2$ и т.д. Получается бесконечная строго убывающая цепочка, противоречие.

3) $\Rightarrow$ 2) Бесконечная нестрого убывающая цепочка обязана стабилизироваться, начиная с минимального элемента.

□

[5] Это соотношение легче запомнить в виде $(K + L) \cap N = K \cap N + L \cap N$, где $K \cap N = K$ в силу $K \subseteq N$.

Определение 2.3. Модуль M *нётеров*, если выполнено одно из следующих эквивалентных условий:

1) нет бесконечной строго *возрастающей* цепочки подмодулей $M_1 \subset M_2 \subset \ldots$;

2) всякая бесконечная нестрого *возрастающая* цепочка $M_1 \subseteq M_2 \subseteq \ldots$ подмодулей M стабилизируется;

3) всякое непустое семейство подмодулей M содержит *максимальный* (по включению) элемент.

Определения артинова и нётерова модуля двойственны в теоретико-множественном смысле.

Предложение 2.4. Пусть $N \leqslant M$ — подмодуль. Модуль M артинов (нётеров) тогда и только тогда, когда N и M/N оба артиновы (нётеровы).

Доказательство артинова случая. Пусть M артинов. Тогда всякая нестрого убывающая цепочка подмодулей N является цепочкой подмодулей M, и N также артинов. Если $L_1 \supseteq L_2 \supseteq \ldots$ — цепочка подмодулей M/N, то $\pi^{-1}(L_1) \supseteq \pi^{-1}(L_2) \supseteq \ldots$ — цепочка подмодулей M, где $\pi : M \to M/N$ — естественная проекция. Вторая цепочка обрывается, поэтому обрывается и первая.

Пусть N, M/N артиновы, $M_1 \supseteq M_2 \supseteq \ldots$ — подмодули M. Рассмотрим цепочки $M_1 \cap N \supseteq M_2 \cap N \supseteq \ldots$ в N и $(M_1 + N)/N \supseteq (M_2 + N)/N \supseteq \ldots$ в M/N. Пусть обе стабилизируются на n-м шаге или ранее. Тогда при $i \geqslant n$ из $(M_i+N)/N = (M_n+N)/N$ следует $M_i + N = M_n + N$. Остаётся воспользоваться свойством модулярности $M_n = M_n \cap (M_n + N) = M_n \cap (M_i + N) = M_i + (M_n \cap N) = M_i + (M_i \cap N) = M_i$. □

Доказательство нётерова случая двойственно вышеприведённому.

Следствие 2.5. Прямая сумма конечного числа модулей артинова (нётерова) тогда и только тогда, когда все слагаемые артиновы (нётеровы).

Доказательство. Доказывается индукцией по числу слагаемых, поскольку

$$(M_1 \oplus \ldots \oplus M_n)/M_n \cong M_1 \oplus \ldots \oplus M_{n-1}$$

при $n > 1$, с использованием вышеприведенного критерия. □

Предложение 2.6. Модуль нётеров тогда и только тогда, когда каждый его подмодуль конечно порождён.

Доказательство. Для $x_1, \ldots, x_n \in M$ обозначим через $\langle x_1, \ldots, x_n \rangle$ подмодуль, порождённый этими элементами. Пусть подмодуль $N \leqslant M$ не конечно порождён. Значит, найдутся $x_1 \in N \setminus \{0\}$, $x_2 \in N \setminus \langle x_1 \rangle$, $x_3 \in N \setminus \langle x_1, x_2 \rangle$, и так далее. Тогда $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \ldots$ — строго возрастающая цепочка подмодулей в M.

Пусть все подмодули M конечно порождены, и $M_1 \subseteq M_2 \subseteq \ldots$ — цепочка подмодулей M. Рассмотрим $N = \bigcup\limits_{i=1}^{\infty} M_i$. По условию этот подмодуль порождён конечным числом элементов, скажем, $x_1, \ldots, x_n$. Каждый x_i обязан принадлежать некоторому M_{j_i}, значит, все x_i принадлежат M_k, где $k = \max\{j_i \mid i = 1, \ldots, n\}$. Поэтому $N = \langle x_1, \ldots, x_n \rangle \subseteq M_i \subseteq N$ при $i \geqslant k$. Следовательно $M_i = N$ при $i \geqslant k$, и цепочка $M_1 \subseteq M_2 \subseteq \ldots$ стабилизируется на шаге k. □

Предложение 2.7. Эндоморфизм φ артинова (нётерова) модуля является изоморфизмом тогда и только тогда, когда он инъективен (сюръективен).

Доказательство. Пусть $\varphi \in \operatorname{End} M$, $\varphi\colon M \to M$ сюръективен, M нётеров. Цепь подмодулей $0 \subseteq \ker\varphi \subseteq \ker\varphi^2 \subseteq \ldots$ стабилизируется на конечном шаге n. Так как $\varphi^n(M) = \varphi(M) = M$, для $k \in \ker\varphi$ имеем $k = \varphi^n(m)$, однако тогда $m \in \ker\varphi^{n+1} = \ker\varphi^n$, то есть $k = 0$, и $\ker\varphi = 0$.

Доказательство для случая инъективного эндоморфизма артинового модуля проводится аналогично, только теперь нужно расматривать цепочку образов, а не ядер. □

Предложение 2.8 (лемма Фиттинга)**.** Пусть модуль M одновременно артинов и нётеров, $\varphi \in \operatorname{End} M$. Тогда для некоторого n выполнено $M = \varphi^n(M) \oplus \ker\varphi^n$ (произведение эндоморфизмов — их композиция).

Доказательство. Пусть цепочки $M \supseteq \varphi(M) \supseteq \varphi(\varphi(M)) \supseteq \ldots$ и $0 \subseteq \ker\varphi \subseteq \ker(\varphi \circ \varphi) \subseteq \ldots$ стабилизируются на n-м шаге или ранее. Тогда для любого $x \in \varphi^n(M) \cap \ker\varphi^n$ выполнено $x = \varphi^n(y)$, $0 = \varphi^n(x) = \varphi^{2n}(y)$, откуда $y \in \ker\varphi^{2n} = \ker\varphi^n$. Поэтому $x = 0$, а значит, сумма подмодулей $\varphi^n(M)$ и $\ker\varphi^n$ действительно прямая.

В силу $\varphi^n(M) = \varphi^{2n}(M)$, для каждого элемента $m \in M$ найдётся такой $p \in M$, что $\varphi^n(m) = \varphi^{2n}(p)$. Тогда можно представить элемент m в виде $m = \varphi^n(p) + (m - \varphi^n(p))$, где второе слагаемое лежит в $\ker\varphi^n$. Поэтому сумма $\varphi^n(M) \oplus \ker\varphi^n$ составляет весь модуль M. □

Определение 2.9. Кольцо R *артиново (нётерово) справа*, если R_R — артинов (нётеров) R-модуль. Левые аналоги определяются симметрично. Кольцо называется *артиновым (нётеровым)*, если оно артиново (нётерово) и справа, и слева.

В силу того, что подмодули R_R — это в точности правые идеалы кольца R, то условия обрыва цепочек подмодулей следует интерпретировать как условия обрыва цепочек правых идеалов.

Следствие 2.10. Кольцо R нётерово справа тогда и только тогда, когда каждый его правый идеал конечно порождён.

Следствие 2.11. Если в кольце все правые идеалы главные, т.е. порождены одним элементом, то кольцо нётерово справа.

Пример 2.12. $\mathbb{Z}$ нётерово, но $\mathbb{Z}$ не является артиновым кольцом, т.к. $(2) \supset (4) \supset \ldots \supset (2^n) \supset \ldots$ — бесконечная строго убывающая цепочка идеалов.

Пример 2.13. Кольцо $R = \left(\begin{smallmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{R} \end{smallmatrix}\right)$ артиново и нётерово справа: его ненулевые правые идеалы исчерпываются R, $\left(\begin{smallmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & 0 \end{smallmatrix}\right)$ и $\mathbb{R}$-подпространствами $\mathbb{R}$-двумерного векторного пространства $\left(\begin{smallmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{R} \end{smallmatrix}\right)$. Однако R не артиново и не нётерово слева, так как его левым идеалом является, в частности, всякое $\mathbb{Q}$-линейное подпространство в $\left(\begin{smallmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{smallmatrix}\right)$.

Предложение 2.14. Конечно порождённый правый модуль M над артиновым справа (нётеровым справа) кольцом R артинов (нётеров).

Доказательство. Если M порождается n элементами, то из предложений 1.49, 1.51 следует, что $M \cong F/K$, где $F = R_R^n$. Согласно следствию 2.5, F_R артинов (нётеров) как сумма модулей с таким же свойством. Поэтому и его фактормодуль M артинов (нётеров) по предложению 2.4. □

Следствие 2.15. Подмодуль конечно порождённого правого модуля M_R над нётеровым справа кольцом конечно порождён.

Доказательство. Все подмодули нётерова модуля M_R конечно порождены. □

Теорема 2.16 (Гильберт, о базисе)**.** Пусть R — нётерово слева кольцо. Тогда $R[x]$ также нётерово слева.

Без доказательства. Если успеем, докажем более общий результат. □

Далее приведены классические теоремы об изоморфизме модулей. Теорему о гомоморфизме модулей также называют *первой теоремой Нётер об изоморфизме*.

Предложение 2.17 (Вторая теорема Нётер об изоморфизме)**.** Пусть N, K — подмодули модуля M. Тогда $(N + K)/K \cong N/(N \cap K)$.

Доказательство. Рассмотрим канонический эпиморфизм $\pi : N + K \to (N + K)/K$ и естественный мономорфизм $\iota : N \to N + K$. Положим $\phi = \pi \circ \iota$. Заметим, что $\ker \phi = N \cap K$ и $\phi(N) = \pi(N) + 0 = \pi(N) + \pi(K) = \pi(N + K)$. Остаётся применить к ϕ теорему о гомоморфизме. □

Предложение 2.18 (Третья теорема Нётер об изоморфизме)**.** Рассмотрим модули $K \leqslant N \leqslant M$. Тогда $(M/K)/(N/K) \cong M/N$.

Доказательство. Пусть $\pi_1 : M \to M/K$ — естественная проекция. Заметим, что т.к. $K \leqslant N$, то $N/K \leqslant M/K$ и $\pi_1(N) = N/K$. Рассмотрим естественную проекцию $\pi_2 : \pi_1(M) \to \pi_1(M)/\pi_1(N)$. Положим $\phi = \pi_2 \circ \pi_1$. Тогда $\ker \phi = \phi^{-1}(0 + \pi_1(N)) = \pi_1^{-1}(\pi_2^{-1}(0 + \pi_1(N))) = \pi_1^{-1}(\pi_1(N)) = N$. Также ϕ — сюръекция как композиция двух сюръекций. Остаётся применить к ϕ теорему о гомоморфизме. □

Лемма 2.19 (Цассенхауз)**.** Пусть даны модули $N' \leqslant N \leqslant M$ и $K' \leqslant K \leqslant M$. Тогда

$$(N' + (N \cap K))/(N' + (N \cap K')) \cong (K' + (N \cap K))/(K' + (N' \cap K)).$$

Доказательство. Обозначим $X = N \cap K$, $Y = N' + (N \cap K')$. В силу $K' \subseteq K$

$$X + Y = N' + (N \cap K') + (N \cap K) = N' + (N \cap K).$$

Поэтому левая часть в утверждении леммы совпадает с $(X+Y)/Y$. Согласно второй теореме об изоморфизме $(X + Y)/Y \cong X/(X \cap Y)$. Пользуясь $K' \subseteq K$, $N' \subseteq N$ и свойством модулярности, вычислим

$$X \cap Y = (N \cap K) \cap (N' + (N \cap K')) = (N' \cap K) + (N \cap K').$$

Мы показали, что левая часть изоморфна $(N \cap K)/((N' \cap K) + (N \cap K'))$. В предыдущем рассуждении можно везде заменить N на K и N' и K'. Тогда получится, что правая часть в утверждении леммы изоморфна тому же выражению. □

Определение 2.20. Пусть $M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n$ — цепь подмодулей. Её i-м *фактором* будем считать фактормодуль M_i/M_{i-1}, $i = 1, \ldots, n$. Скажем, что цепь подмодулей $M'_0 \subseteq M'_1 \subseteq \ldots \subseteq M'_{n'}$ является *уплотнением* исходной цепи, если $n' \geqslant n$, $M_0 = M'_0$, $M_n = M'_{n'}$ и $(M_i)_{i=1}^{n}$ является подпоследовательностью в $(M'_j)_{j=1}^{n'}$.

Теорема 2.21 (Шрайер)**.** Пусть даны две цепи подмодулей: $N = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_m = M$ и $N = N_0 \subseteq N_1 \subseteq \ldots \subseteq N_n = M$. Тогда существуют уплотнения обеих цепей одной и той же длины k и такая подстановка σ на множестве $\{1, \ldots, k\}$, что i-й фактор уплотнения первой цепи изоморфен $\sigma(i)$-му фактору уплотнения второй цепи.

Доказательство. Вставим между модулями M_i и M_{i+1} подмодули

$$M_{i,j} = M_i + (M_{i+1} \cap N_j),\ j = 0, \ldots, n.$$

Заметим, что $M_i = M_{i,0}$ и $M_{i+1} = M_{i,n}$. Аналогично между модулями N_j и N_{j+1} добавим

$$N_{i,j} = N_j + (N_{j+1} \cap M_i),\ i = 0, \ldots, m.$$

Тогда по лемме Цассенхауза выполнено $M_{i,j+1}/M_{i,j} \cong N_{i+1,j}/N_{i,j}$. □

Отметим, что теорема не исключает наличия нулевых факторов в уплотнениях. Однако их будет одинаковое число. Поэтому если в теореме Шрайера исходные цепи строго возрастали, то можно считать, что уплотнения тоже строго возрастают.

Определение 2.22. *Композиционный ряд* правого модуля M — цепочка подмодулей $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$, в которой все факторы — неприводимые модули.

Композиционный ряд не может содержать повторяющихся подмодулей, в силу того, что нулевой модуль не является неприводимым.

Отметим, что поскольку фактор M_i/M_{i-1} неприводим, не существует такого модуля N, что $M_{i-1} \subsetneq N \subsetneq M_i$. Поэтому любое строго возрастающее уплотнение композиционного ряда совпадает с ним самим.

Композиционный ряд определён неоднозначно (это верно даже для векторного пространства над полем).

Композиционный ряд не всегда существует, например, его нет у $\mathbb{Z}_{\mathbb{Z}}$.

Из теоремы Шрайера сразу получаем следующий результат.

Следствие 2.23 (Жордан, Гёльдер)**.** Пусть M_R обладает композиционным рядом. Тогда выполнено следующее:

1) Любая конечная строго возрастающая цепочка подмодулей может быть уплотнена до некоторого композиционного ряда.

2) Длины всех композиционных рядов равны, и наборы факторов двух композиционных рядов могут быть упорядочены так, что соответствующие факторы будут попарно изоморфны.

Определение 2.24. Если модуль M обладает некоторым композиционным рядом $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$, то будем говорить, что *(композиционная) длина* модуля равна n. Обозначение $l(M) = n$.

Следствие 2.25. Наличие композиционного ряда у модуля M равносильно одновременной артиновости и нётеровости M.

Доказательство. Бесконечная строго возрастающая или убывающая цепочка подмодулей не могла бы быть включена в конечный композиционный ряд.

Обратно, пусть модуль нётеров и артинов. Тогда в силу артиновости у него есть минимальный ненулевой подмодуль M_1. Затем выберем минимальный элемент M_2 в множестве всех подмодулей, строго содержащих M_1. Продолжаем процесс. Заметим, что на некотором шаге k множество подмодулей, строго содержащих M_k, будет пусто: иначе мы бы получили бесконечную строго возрастающую цепочку, что противоречило бы нётеровости. Значит, $M_k = M$. □

Пример 2.26. Пусть V — конечномерное векторное пространство над полем $\mathbb{F}$. Тогда композиционная длина V совпадает с размерностью.

Лемма 2.27. Пусть M — левый или правый модуль над кольцом R и $S = \mathrm{End}_R(M)$. Тогда существует канонический гомоморфизм колец $\varphi : R \to \mathrm{End}_S(M)$.

Доказательство. Пусть M — левый R-модуль. Для любого $r \in R$ определим отображение $\varphi(r) : M \to M$ правилом $\varphi(r)(x) = rx$ для любого $x \in M$. Для произвольных $x \in M$ и $s \in S$ имеем

$$\varphi(r)((x)s) = r \cdot (x)s = (rx)s = (\varphi(r)(x))s,$$

т.е. $\varphi(r)$ — эндоморфизм правого S-модуля.

По определению φ является гомоморфизмом аддитивных групп соответствующих колец. Для любых $r_1, r_2 \in R$ и $x \in M$ проверим, что

$$\varphi(r_1 r_2)(x) = r_1 r_2 x = \varphi(r_1)(r_2 x) = \varphi(r_1)\varphi(r_2)(x),$$

т.е. $\varphi : R \to \mathrm{End}_S(M)$ — гомоморфизм колец.

Для правого R-модуля M определение гомоморфизма φ аналогично: $(x)\varphi(r) = xr$. □

Лемма 2.28 (Шур)**.** Кольцо эндоморфизмов простого модуля является телом.

Доказательство. Пусть V — простой правый модуль и $f : V \to V$ — его эндоморфизм. Если $f \neq 0$, то $\ker f \neq V \Rightarrow \ker f = 0 \Rightarrow V \cong f(V) \neq 0 \Rightarrow f(V) = V$, т.е. f — изоморфизм, стало быть, он обратим в кольце $\mathrm{End}\,(V)$. □

Определение 2.29. Подкольцо S кольца линейных преобразований левого векторного пространства V над телом D называется *плотным*, если для любой конечной линейно независимой над D системы элементов $x_1, \ldots, x_n \in V$ и произвольного набора элементов $y_1, \ldots, y_n \in V$ существует такой элемент $s \in S$, что $x_i s = y_i$ при всех $i = 1, \ldots, n$.

Топологический термин “плотное подкольцо” объясняется следующим образом: кольцо $\mathrm{End}\,(V)$ всех эндоморфизмов левого модуля над произвольным кольцом можно снабдить топологией, используя в качестве базы окрестностей нуля можества вида

$$U(v_1, \ldots, v_n) = \{\varphi \in \mathrm{End}\,(v) | (v_1)\varphi = \ldots = (v_n)\varphi = 0\}$$

для произвольных конечных помножеств $\{v_1, \ldots, v_n\}$ модуля V. Определение плотного подкольца в точности означает, что S плотно в этой топологии.

Теорема 2.30 (Теорема плотности)**.** Пусть M — простой правый модуль над кольцом R, $D = \mathrm{End}_R(M)$. Тогда M — левый D-модуль (векторное пространство V над телом), и любой элемент $r \in R$ определяет D-линейное отображение $\varphi_r : M \to M$, заданное правилом $m \mapsto mr$ и отображение $r \mapsto \varphi_r$ является гомоморфизмом колец $R \to \mathrm{End}_D(M)$, причём образ этого отображения является плотным подкольцом.

Доказательство. Легко видеть, что если $d \in D$, $r \in R$ и $m \in M$, то $(dm)\varphi_r = (d(m))\varphi_r = d(m)r = d(mr) = d((m)\varphi_r)$, т.е. отображение φ_r является D-линейным. То, что отображение $r \mapsto \varphi_r$ является гомоморфизмом колец, мы уже проверили в лемме.

Докажем сначала следующее вспомогательное утверждение:

Если V — конечномерное подпространство пространства ${}_D M$, и $m \in M \setminus V$, то существует элемент $r \in R$ такой, что $mr \neq 0$ и $Vr = 0$.

Проведём доказательство индукцией по размерности пространства V. Если $\dim {}_D V = 0$, утверждение очевидно. Пусть $\dim {}_D V = n > 0$, $e_1, \ldots, e_n$ — базис пространства V и V_0 — подпространство, порождённое $e_1, \ldots, e_{n-1}$. Положим $K = \mathrm{Ann}\ {}_R(V_0) = \{r \in R : V_0 r = 0\}$. Заметим, что по предположению индукции (применённому к $m = e_n$) имеем $e_n K \neq 0$. Но тогда $e_n K = M$, так как модуль M простой. Допустим, что из $Vr = 0$ следует $mr = 0$. Определим отображение $t : M \to M$ следующим правилом: если $x = e_n k$, где $k \in K$, то $t(x) = mk$. Проверим корректность этого определения. Если $k' \in K$ и $e_n k = e_n k'$, то $V(k - k') = 0$ и, по допущению, $mk = mk'$. Ясно, что $t \in D$ и для любого $k \in K$ имеем $mk = t(e_n k) = t(e_n)k$, откуда $(m - t(e_n))K = 0$. Следовательно, $m - t(e_n) \in V_0$, и $m \in De_n + V_0 = V$. Противоречие доказывает справедливость вспомогательного утверждения.

Теперь пусть $x_1, \ldots, x_n \in M$ линейно независимая над D система элементов и $y_1, \ldots, y_n$ — произвольные элементы модуля M. Для всех $i = 1, \ldots, n$ определим V_i как подпространство, порождённое всеми элементами $x_1, \ldots, x_n$, кроме x_i. Поскольку $x_i \notin V_i$, существует элемент $a_i \in R$ такой, что $V_i a_i = 0$ и $x_i a_i \neq 0$. Так как M — простой модуль, $x_i a_i R = M$, т.е. существует элемент $b_i \in R$ такой, что $x_i a_i b_i = y_i$. Непосредственно проверяется, что если $r = a_1 b_1 + \ldots + a_n b_n$, то $s = \varphi_r$ удовлетворяет условию определения плотного подкольца. □

Определение 2.31. Правый R-модуль M называется *точным*, если его аннулятор в кольце R равен нулю, т.е.

$$\forall r \in R, Mr = 0 \Rightarrow r = 0.$$

Определение 2.32. Кольцо R называется *примитивным (справа)*, если существует точный правый простой R-модуль.

Следствие 2.33. Кольцо R является примитивным (справа) тогда и только тогда, когда оно изоморфно плотному подкольцу кольца линейных преобразований левого векторного пространства над некоторым телом.

Доказательство. Пусть R — примитивное справа кольцо и M — точный простой правый R-модуль. В силу теоремы плотности достаточно проверить, что гомоморфизм $r \mapsto \varphi_r$ имеет нулевое ядро, но это равносильно тому, что модуль M точный: если $\varphi_r = 0$, это значит, что $Mr = 0$, откуда $r = 0$.

Обратно, пусть $\varphi : R \to \mathrm{End}\ {}_D(V)$ — инъективный гомоморфизм колец. Определим умножение элемента $v \in V$ на элемент $r \in R$ правилом $vr = (v)\varphi(r)$. Тогда V превращается в точный правый R-модуль. Если $0 \neq v \in V$, то для любого $v' \in V$ существует элемент $r \in R$ такой, что $vr = v'$ (см. определение плотности при $n = 1$.) Следовательно, $vR = V$ и V — простой R-модуль. □

Предложение 2.34. Кольцо R является примитивным (справа) тогда и только тогда, когда в R содержится максимальный правый идеал, не содержащий ненулевых идеалов.

Доказательство. Пусть кольцо R примитивно справа и M — простой правый точный R-модуль. Выберем любой ненулевой элемент $m \in M$ и рассмотрим гомоморфизм правых R-модулей $f : R \to M$, заданный правилом $r \mapsto mr$ для всех $r \in R$. Тогда $f(R) \neq 0$, поэтому $f(R) = M$ и $f(R) \cong R/K$, где $K = \ker(f)$. По предложению 1.55 K — максимальный правый идеал. Пусть $I \lhd R$ и $I \subseteq K$. Тогда $MI = mRI \subseteq mK = 0$. Поскольку M — точный модуль, это означает, что $I = 0$.

Обратно, если K — максимальный правый идеал, не содержащий ненулевых двусторонних идеалов, то R/K — простой модуль по предложению 1.55. Если $I = \operatorname{Ann}_R(M)$, то $I \lhd R$ и из $(1 + K)I = 0$ следует, что $I \subseteq K$. Значит $I = 0$, т.е. M/K — точный модуль. □

Следствие 2.35. Простое кольцо примитивно справа и слева.

Определение 2.36. Идеал I кольца R называется *примитивным (справа), если кольцо R/I примитивно (справа).*

Пример примитивного справа кольца, которое не является примитивным слева, содержится в статье Bergman, G. M. (1964), "A ring primitive on the right but not on the left", Proceedings of the American Mathematical Society, 15 (3): 473–475.

Задачи к лекции 3.

Задача 1. Приведите пример конечно порождённого модуля, который не является нётеровым.

Задача 2. Приведите пример артинова модуля, который не является конечно порождённым.

Задача 3. Докажите, что любой артинов правый модуль над артиновым справа кольцом является конечно порождённым.

Задача 4. Покажите, что подкольцо артинова (нётерова) кольца не обязательно артиново (нётерово).

Задача 5. Покажите, что для любого $n \geqslant 1$ кольцо матриц $M_n(R)$ над артиновым (соотв. нётеровым) справа кольцом R также является артиновым (соотв. нётеровым) справа.

Задача 6. Пусть $R = \mathbb{F}[x]$ — кольцо многочленов над полем. Покажите, что само кольцо R не является артиновым кольцом, но для любого $0 \neq I \lhd R$ факторкольцо R/I — артиново.

Задача 7. Пусть в условиях леммы Фиттинга модуль M — конечномерное векторное пространство над полем. Соответственно, эндоморфизм φ — линейный оператор. Охарактеризуйте наименьшее n, для которого выполнено утверждение леммы, в терминах линейной алгебры.

Задача 8. Найдите все неприводимые правые модули над кольцом верхнетреугольных 2×2-матриц над полем.

Задача 9. Верно ли, что всякий неприводимый правый R-модуль изоморфен некоторому (минимальному) подмодулю R_R?

Задача 10. Пусть модуль M имеет композиционную длину n. Покажите, что любой его собственный подмодуль N также обладает композиционным рядом и $l(N) < n$.

Задача 11. Пусть R_R обладает композиционным рядом. Докажите, что всякий неприводимый R-модуль содержится среди факторов этого ряда.

Задача 12. Найдите композиционную длину кольца вычетов $\mathbb{Z}_n$ как $\mathbb{Z}$-модуля.

3 Полупростые модули и кольца.

Лекция 4. Полупростые модули и кольца. Теорема Веддербёрна — Артина.

Определение 3.1. *Полупростой (вполне приводимый) модуль* — это модуль, раскладывающийся в прямую сумму неприводимых.

Пример 3.2.

- Нулевой модуль полупрост, он раскладывается в пустую сумму неприводимых.
- Всякое (в т.ч. бесконечномерное) векторное пространство над телом полупросто.
- Полупростой $\mathbb{Z}$-модуль — прямая сумма (конечного или бесконечного числа) циклических групп простого порядка.
- Полупростые $\mathbb{F}G$-модули соответствуют вполне приводимым представлениям группы G.

Предложение 3.3. Пусть $M_R = \bigoplus_{i \in I} S_i$, S_i — неприводимые R-модули. Тогда прямая сумма конечна тогда и только тогда, когда M конечно порожден.

Доказательство. В силу неприводимости модуль S_i циклический, т.е. порожден одним элементом, скажем, s_i. При $|I| = n$ получаем $M = \langle s_1, \ldots, s_n \rangle_R$. Обратно, если $M = \langle m_1, \ldots, m_n \rangle_R$, то каждый из элементов m_i, а значит, и весь M лежит в сумме некоторого конечного числа S_j. □

Лемма 3.4. Пусть $M = \sum\limits_{i \in I} S_i$ — необязательно прямая сумма неприводимых подмодулей $S_i \leqslant M$. Тогда M полупрост и, более того, для любого подмодуля $N \leqslant M$ существует такое подмножество индексов $J \subseteq I$, что $M = N \oplus \bigoplus\limits_{j \in J} S_j$.

Доказательство. Докажем второе утверждение леммы, первое получается из него при $N = 0$. Пусть Ω — это множество, состоящее из таких подмножеств индексов $J \subseteq I$, что сумма всех модулей в выражении $N + \sum\limits_{j \in J} S_j$ является прямой. Отметим, что $\Omega \neq \varnothing$, т.к. $\varnothing \in \Omega$ из-за того, что сумма N и нулевого модуля прямая. Упорядочим Ω по включению. Покажем, что если $\{F_\lambda\}_{\lambda \in \Lambda}$ — цепь в Ω, то $F = \bigcup\limits_{\lambda \in \Lambda} F_\lambda$ — также принадлежит Ω. От противного, пусть сумма $P = N + \sum\limits_{j \in F} S_j$ не является прямой. Тогда имеется разложение нуля $0 = n + s_{j_1} + \ldots + s_{j_k}$ для некоторых $n \in N$, $s_{j_i} \in S_{j_i}$, $j_i \in F$, причем не все элементы $n, s_{j_1}, \ldots, s_{j_k}$ равны нулю. Т.к. F — это объединение цепи $\{F_\lambda\}_{\lambda \in \Lambda}$, то найдётся индекс $\lambda \in \Lambda$, для которого все $j_i \in F_\lambda$. Сумма $N + \sum\limits_{j \in F_\lambda} S_j$ прямая в силу $F_\lambda \in \Omega$, но мы получили нетривиальное разложение нуля $0 = n + s_{j_1} + \ldots + s_{j_k}$, соответствующее этой сумме модулей, противоречие. Мы доказали, что $F \in \Omega$.

По лемме Цорна в Ω существует максимальный элемент J. Пусть $P = N + \sum\limits_{j \in J} S_j$. В силу неприводимости S_i пересечение $P \cap S_i$ равно либо S_i, либо 0. Покажем, что для всех $i \in I$ выполнено $P \cap S_i = S_i$. Предположим противное: пусть для некоторого i_0 пересечение $P \cap S_{i_0}$ нулевое. Отсюда $i_0 \notin J$ согласно определению P. Заметим, что тогда сумма всех модулей в выражении $N + \sum\limits_{j \in J \cup \{i_0\}} S_j$ будет прямой. Действительно, если $0 = n + s_{j_1} + \ldots + s_{j_k} + s_0$, где $n \in N$, $s_0 \in S_{i_0}$, $s_{j_i} \in S_{j_i}$, $j_i \in J$, то $-n - s_{j_1} - \ldots - s_{j_k} = s_0 \in P \cap S_{i_0}$, откуда и s_0, и $-n - s_{j_1} - \ldots - s_{j_k}$ равны нулю, а значит, n и s_{j_i} тоже равны нулю, т.к. сумма $N + \sum\limits_{j \in J} S_j$ прямая. Мы показали, что сумма $N + \sum\limits_{j \in J \cup \{i_0\}} S_j$ прямая, поэтому $J \cup \{i_0\} \in \Omega$, что противоречит максимальности J. Итак, $S_i \subseteq P$ для всех $i \in I$, и $P = M$. □

Определение 3.5. Подмодуль $N \leqslant M$ *выделяется прямым слагаемым*, если существует подмодуль $N' \leqslant M$ *(дополнение до N)* такой, что $N \oplus N' = M$. Также говорят, что N — прямое слагаемое модуля M.

Дополнение определено неоднозначно, но как R-модули все дополнения изоморфны M/N.

Лемма 3.6. Пусть $N \leqslant M$ — модули. Если N выделяется в M прямым слагаемым, то N выделяется прямым слагаемым и во всяком модуле P, таком что $N \leqslant P \leqslant M$.

Доказательство. Воспользуемся модулярностью: $P = M \cap P = (N + N') \cap P = N \oplus (N' \cap P)$. □

Теорема 3.7. Для модуля M следующие условия эквивалентны:

1) M раскладывается в сумму неприводимых модулей;

2) M полупрост, т.е. раскладывается в *прямую* сумму неприводимых модулей;

3) всякий подмодуль выделяется в M прямым слагаемым.

Доказательство. 1) $\Rightarrow$ 2) Доказано ранее.

2) $\Rightarrow$ 1) Тавтология.

2) $\Rightarrow$ 3) Доказано ранее.

3) $\Rightarrow$ 2) Пусть S — сумма всех неприводимых подмодулей M. Предположим, что $S \neq M$, тогда $M = S \oplus T$, $T \neq 0$. Рассмотрим произвольный циклический подмодуль $N \leqslant T$. Т.к. он конечно порожден, то можно выбрать в в N максимальный собственный левый подмодуль N' (теорема 1.58). Он выделяется прямым слагаемым как в M, так и в N, то есть $N = N' \oplus P$, и из максимальности N' модуль $P \cong N/N'$ неприводим, что противоречит определению S. □

Следствие 3.8. Пусть $M = \bigoplus\limits_{i \in I} S_i$, S_i — неприводимые модули, $N \leqslant M$. Тогда у N есть дополнение вида $\bigoplus\limits_{k \in K} S_k$, $K \subseteq I$, и N изоморфен (но не обязательно равен) $\bigoplus\limits_{k \in I \setminus K} S_k$. В частности, если N неприводимый, то $N \cong S_i$ и его дополнение $\bigoplus\limits_{j \neq i} S_j$.

Следствие 3.9. Подмодули и фактормодули полупростого модуля полупросты.

Предложение 3.10. Пусть M — полупростой конечнопорождённый R-модуль. Тогда любые два разложения M в прямую сумму неприводимых подмодулей содержат одинаковое конечное число слагаемых, и слагаемые в них могут быть упорядочены так, чтобы соответствующие были попарно изоморфны.

Доказательство. Пусть $M = P_1 \oplus \ldots \oplus P_n = Q_1 \oplus \ldots \oplus Q_m$, где все P_i и Q_j неприводимы. Т.к. $P_1 \leqslant M = Q_1 \oplus \ldots \oplus Q_m$, то P_1 изоморфен одному из Q_j. С точностью до перенумерации можно считать, что $P_1 \cong Q_1$. Это позволяет удалить эти слагаемые и осуществить индукцию по n. □

Пусть $\{N_\lambda\}_{\lambda \in \Lambda}$ — семейство всех максимальных правых идеалов $R \neq 0$. Рассмотрим $\{R/N_\lambda\}_{\lambda \in \Lambda}$ — семейство правых неприводимых R-модулей, которое разбивается на классы эквивалентности отношением изоморфизма. Эти классы будем называть *классами изоморфизма правых неприводимых R-модулей*. Любой неприводимый правый R-модуль M изоморфен какому-нибудь R/N_λ из некоторого класса σ. В этом случае будем говорить, что M — это *модуль класса σ*, или *представитель класса σ*.

Определение 3.11. *Цоколь* $\operatorname{soc} M$ модуля M — сумма всех неприводимых подмодулей M. Сумма всех неприводимых подмодулей класса σ называется *однородной компонентой* M, соответствующей классу σ, или *σ-цоколем* модуля M. Если сумма пуста, то однородная компонента полгается равной нулю.

Отметим, что в определении цоколя сумма не обязана быть прямой. Например, для векторного пространства V над полем, цоколь является суммой всех одномерных подпространств, что, конечно, совпадает со всем V, однако эта сумма очевидно не прямая при $\dim V \geqslant 2$.

Определение 3.12. *Вполне инвариантный* подмодуль $N \leqslant M$ — это такой подмодуль, что $\varphi(N) \subseteq N$ для всех $\varphi \in \operatorname{End} M$.

На модуле M_R действуют скаляры из R умножением справа и эндоморфизмы из $\operatorname{End} M_R$ умножением слева. Вполне инвариантный подмодуль — это абелева подгруппа в M, которая сохраняется сразу обоими действиями.

Теорема 3.13. 1) $\operatorname{soc} M$ — прямая сумма σ-цоколей M по всем различным классам изоморфизма σ неприводимых R-модулей.

2) Всякая сумма σ-цоколей вполне инвариантна. Если M полупрост, то верно и обратное.

Доказательство. Пусть M_σ — σ-цоколь M.

1) M_σ полупрост как сумма неприводимых модулей и не может нетривиально пересекаться с M_τ, $\sigma \neq \tau$, поэтому сумма прямая.

2) Пусть $M_\sigma = \sum S_i$, S_i — все неприводимые модули класса σ, $\varphi \in \operatorname{End} M_R$. Тогда $\varphi(M_\sigma) = \sum \varphi(S_i)$. По теореме о гомоморфизме модулей слагаемые справа либо нулевые, либо также класса σ.

Пусть $N \leqslant M$ вполне инвариантен и M полупрост. Достаточно доказать, что для изоморфных неприводимых подмодулей $P \leqslant N$ и $Q \leqslant M$ модуль Q также обязан лежать в N. Либо $P = Q$, либо сумма $P+Q$ прямая, тогда из полупростоты выполнено $M = P \oplus Q \oplus U$ для некоторого модуля U. Пусть $f\colon P \to Q$ — изоморфизм. Тогда отображение $\theta\colon M = P \oplus Q \oplus U \to M$, $p+q+u \mapsto f(p)+f^{-1}(q)+u$ — эндоморфизм M, переводящий P в Q (и наоборот), поэтому $Q = \theta(P) \subseteq N$, т.к. N вполне инвариантен и содержит P. □

Следствие 3.14. Модуль M полупрост тогда и только тогда, когда $M = \operatorname{soc} M$.

Следствие 3.15. Пусть $\{M_\sigma\}_{\sigma\in\Sigma}$ — это все однородные компоненты полупростого R-модуля M. Тогда $\operatorname{End} M_R = \prod\limits_\sigma \operatorname{End}(M_\sigma)_R$.

Замечание 3.16. Разложение полупростого модуля в прямую сумму неприводимых компонент определено только с точностью до изоморфизма слагаемых; разложение в сумму однородных компонент определено однозначно.

Предложение 3.17. Пусть модуль R_R полупрост. Тогда всякий правый R-модуль M полупрост. Более того, среди минимальных правых идеалов кольца R найдутся представители всех классов изоморфизма неприводимых правых R-модулей.

Доказательство. Представим модуль M в виде $M = F/K$, где $F = R_R^I = \bigoplus_{i\in I} R_R$ — свободный модуль и $K \leqslant F$ (предложения 1.49, 1.51). Вместе с регулярным модулем R_R полупростым будет и свободный модуль F, и все его фактормодули, откуда M полупрост.

Всякий неприводимый правый R-модуль изоморфен R_R/N, где $N \leqslant R_R$ — максимальный правый идеал. Согласно следствию 3.8, модуль N выделяется в R_R прямым слагаемым, а его дополнение $N' \cong R_R/N$, т.е. N' является неприводимым подмодулем R_R, а значит, N' — минимальный правый идеал кольца R. □

Теорема 3.18 (Веддербёрн, Артин)**.** Следующие условия эквивалентны.

1) Модуль R_R полупрост.

2) Модуль ${}_RR$ полупрост.

3) $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$, где числа k, n_i и тела D_i определены однозначно. Такое кольцо R артиново слева и справа.

Доказательство. В силу симметричности 3) достаточно показать, что 1) $\Leftrightarrow$ 3).

1) $\Rightarrow$ 3) Поскольку R_R полупрост и конечно порождён ($R_R = \langle 1\rangle_R$), то он раскладывается в конечную прямую сумму неприводимых подмодулей (минимальных правых идеалов) $R_R \cong \bigoplus_{i=1}^{d} I_i$. Согласно предложению 3.17, среди I_i содержатся представители всех классов изоморфизма неприводимых правых R-модулей, откуда этих классов конечное число, скажем, k штук. С точностью до перенумерации можно считать, что $I_1, \ldots, I_k$ — представители всех этих классов. Положим n_j равным количеству минимальных правых идеалов I_i изоморфных I_j. Тогда $R_R \cong I_1^{n_1} \oplus \ldots \oplus I_k^{n_k}$. Заметим, что мы получили разложение полупростого модуля R_R на его однородные компоненты $I_j^{n_j}$. По теореме 1.68 $R \cong \operatorname{End} R_R$. В силу следствия 3.15 имеем $\operatorname{End} R_R \cong \operatorname{End} I_1^{n_1} \times \ldots \times \operatorname{End} I_k^{n_k}$. По следствию 1.66 выполнено $\operatorname{End} I_j^{n_j} \cong M_{n_j}(D_j)$, где $D_j = \operatorname{End} I_j$ является телом по лемме Шура. Таким образом, $R \cong \prod_{i=1}^{k} M_{n_i}(D_i)$. Число k определено однозначно как количество классов изоморфизма неприводимых R-модулей. Единственность чисел n_j и тел D_j следует из единственности разложения на однородные компоненты.

3) $\Rightarrow$ 1) Модуль R_R представляется в виде прямой суммы правых R-модулей вида $O \oplus \ldots \oplus M_{n_j}(D_j) \oplus \ldots \oplus O$. Для $j = 1, \ldots, k$, $i = 1, \ldots, n_j$ рассмотрим подмножество $V_{j,i} \subseteq M_{n_j}(D_j)$, состоящее из всех матриц вида

$$\begin{pmatrix} 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{i1} & a_{i2} & \ldots & a_{i,n_j} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Тогда $V_{j,i}$ — минимальный правый идеал $M_{n_j}(D_j)$. Значит, $V'_{j,i} = O \oplus ... \oplus V_{j,i} \oplus ... \oplus O$ — это неприводимый правый R-модуль. Тогда $R_R = \bigoplus\limits_{i,j} V'_{j,i}$ — разложение в сумму неприводимых подмодулей.

Модуль R_R является артиновым как конечная прямая сумма неприводимых, а значит, артиновых модулей (следствие 2.5). Для ${}_RR$ аналогично. □

Определение 3.19. Кольцо R называется *полупростым*, если R_R (эквивалентно ${}_RR$) является полупростым модулем. Для таких колец также используются термины *классически полупростое кольцо* и *вполне приводимое кольцо*.

Определение 3.20 (напоминание)**.** *Простое кольцо* — это кольцо, в котором ровно два собственных идеала: $\{0\}$, R.

Простое кольцо необязательно полупросто.

Теорема 3.21 (Молин, Веддербёрн)**.** Следующие условия на кольцо R эквивалентны:

1) R просто и артиново справа;

2) модуль R_R полупрост, и все неприводимые правые R-модули изоморфны;

3) $R \cong M_n(D)$, D — тело;

1'), 2') левые аналоги 1), 2).

Кроме того, натуральное n из 3) единственно, а тело D определено однозначно с точностью до изоморфизма.

Доказательство. В силу симметричности 3) достаточно доказать эквивалентность 1)–3).

1) $\Rightarrow$ 2) Пусть cR — произвольный минимальный правый идеал R. Он существует, поскольку R артиново справа. Из простоты R имеем $R = RcR = \sum\limits_{s \in R} scR$ — сумма правых модулей. Правый идеал scR — образ cR при действии гомоморфизма правых модулей $cr \mapsto scr$. Гомоморфизм сюръективен по построению, его ядро либо 0, либо cR. Поэтому scR либо нулевой, либо изоморфен cR. Отсюда R_R полупрост. Любой неприводимый правый R-модуль изоморфен минимальному правому идеалу в силу предложения 3.17.

2) $\Rightarrow$ 3) Воспользуемся теоремой Веддербёрна — Артина и тем фактом, что у полупростого модуля R_R только одна однородная компонента в силу 2).

3) $\Rightarrow$ 1) Простота кольца $R = M_n(D)$ доказана ранее (следствие 1.24). Артиновость следует из теоремы Веддербёрна — Артина. □

Лемма 3.22. Пусть $\mathbb{F}$ — алгебраически замкнутое поле, R — $\mathbb{F}$-алгебра, M_R — неприводимый R-модуль, конечномерный над $\mathbb{F}$. Тогда $\operatorname{End} M_R \cong \mathbb{F}$.

Доказательство. R-эндоморфизм $\varphi \in \operatorname{End} M_R$ является $\mathbb{F}$-линейным оператором на $M_{\mathbb{F}}$, который в силу алгебраической замкнутости поля обладает собственным значением $\lambda \in \mathbb{F}$, то есть оператор $\varphi - \lambda$ вырожден. По лемме Шура он может быть только нулевым. Значит, $\operatorname{End} M_R$ состоит только из скалярных операторов (с любым скаляром из $\mathbb{F}$) и поэтому само изоморфно $\mathbb{F}$. □

Предложение 3.23. Конечномерная полупростая алгебра над алгебраически замкнутым полем $\mathbb{F}$ изоморфна как кольцо прямому произведению полных матричных алгебр над $\mathbb{F}$.

Доказательство. Минимальные правые идеалы алгебры являются конечномерными векторными пространствами над $\mathbb{F}$. Поэтому в доказательстве теоремы Веддербёрна-Артина все тела D_i изоморфны полю $\mathbb{F}$ по лемме. □

Определение 3.24. Первая *алгебра Вейля* над полем $\mathbb{F}$ определяется как как фактор свободной алгебры $A_1(\mathbb{F}) = \mathbb{F}\langle x, y\rangle / (yx - xy - 1)$.

Зададим на $\mathbb{F}[x]$ структуру левого $A_1(\mathbb{F})$-модуля. Сопоставим переменной $x \in A_1(\mathbb{F})$ линейный оператор на $\mathbb{F}[x]$, умонажющий многочлен на x. Переменной y сопоставим формальное дифференцирование ∂_x по переменной x. По правилу Лейбница $\partial_x(xP) = P + x\partial_x P$, где $P \in \mathbb{F}[x]$, поэтому $\partial_x x - x\partial_x - 1 = 0$ как операторы. Таким образом, можно понимать алгебру Вейля как алгебру формальных дифференциальных операторов с полиномиальными коэффициентами.

Аналогично определяются алгебры $A_n(k)$ — берется n переменных и n соответствующих дифференциальных операторов.

$R = A_1(\mathbb{F})$ — не артиново кольцо: $R \supset xR \supset x^2R \ldots$ — бесконечная строго убывающая цепочка правых идеалов.

Предложение 3.25. Пусть $\operatorname{char}\mathbb{F} = 0$. Тогда $A_1(\mathbb{F})$ — простое кольцо.

Доказательство. Заметим, что элементы $A_1(\mathbb{F})$ обладают канонической формой вида $\sum\limits_{k\in K} a_k x^{i_k}\partial_x^{j_k}$, где K — конечное множество индексов, i_k, j_k — неотрицательные целые числа.

Заметим, что переход от элемента $r \in A_1(\mathbb{F})$ к *коммутатору* $[r, s] = rs - sr$ с элементом $s \in \{x, \partial_x\}$ уменьшает на единицу степени всех "мономов" в его канонической форме либо по ∂_x, либо по x, и умножает их на ненулевые скаляры: для оператора $T = a_k x^{i_k}\partial_x^{j_k}$ имеем $\partial_x T = a_k i_k x^{i_k-1}\partial_x^{j_k} + T\partial_x$;

$\partial_x x = 1 + x\partial_x$, поэтому $\partial_x^m x = \partial_x^{m-1} + \partial_x^{m-1}x\partial_x = \ldots = m\partial_x^{m-1} + x\partial_x^m$,

откуда $Tx = a_k j_k x^{i_k}\partial_x^{j_k-1} + xT$.

Поэтому если идеал $I \lhd A_1(\mathbb{F})$ содержит ненулевой элемент r, то его можно подобными операциями, не покидая I, перевести в ненулевой скаляр. Для этого достаточно зафиксировать в r произвольный "моном" $x^{i_k}\partial_x^{j_k}$ среди "мономов" с максимальной суммой $i_k + j_k$ и взять i_k раз коммутатор с ∂_x и j_k раз коммутатор с x. □

Следствие 3.26. Существует простое, но не артиново кольцо. В частности, существует простое, но не полупростое кольцо.

Задачи к лекции 4.

Задача 1. Покажите, что $\operatorname{soc}(\operatorname{soc} M) = \operatorname{soc} M$ для произвольного R-модуля M.

Задача 2. Для кольца R можно рассмотреть два цоколя: $S_1 = \operatorname{soc}(R_R)$ для правого регулярного модуля, и $S_2 = \operatorname{soc}({}_R R)$ — для левого. Покажите, что
1) S_1 и S_2 являются идеалами кольца R;
2) S_1 и S_2 не обязательно равны.

Задача 3. Пусть M — конечно порождённый модуль над полупростым кольцом. Докажите, что кольцо $\operatorname{End}(M)$ полупросто.

Задача 4. Пусть M — полупростой конечно порождённый R-модуль. Докажите, что он обладает композиционным рядом и его композиционная длина $l(M)$ равна количеству слагаемых в произвольном разложении M в прямую сумму неприводимых модулей.

Задача 5. Докажите, что для полупростого модуля M следующие условия равносильны: 1) M артинов, 2) M нётеров, 3) M конечнопорожден.

Задача 6. Пусть D — конечное тело, $Z(D)$ — его центр, $|Z(D)| = q$; $\Phi_n(x) = \prod\limits_{\substack{\zeta\in\mathbb{C};\,\zeta^n=1;\\ \zeta^k\neq 1,\,0<k<n}} (x-\zeta) \in \mathbb{Z}[x] \subseteq \mathbb{C}[x]$ — многочлен деления круга.
1) Показать, что кольцевые централизаторы элементов D являются линейными пространствами над $Z(D)$. В частности, $|D| = q^n$ для некоторого натурального n.
2) Пользуясь тем, что Φ_n имеет целые коэффициенты, доказать, что ость каждого нетривиального класса сопряжённости в мультипликативной группе D должна быть кратна числу $\Phi_n(q)$.
3) Используя обратное неравенство треугольника, найти все n, при которых $\Phi_n(q)$ может делить $q-1$, и получить *теорему Веддербёрна* о том, что конечное тело является полем.

Задача 7. Используя теорему Веддербёрна, доказать, что конечная подгруппа G мультипликативной группы тела D ненулевой характеристики циклическая (указание: найти в D гомоморфный образ конечной групповой алгебры). Верно ли это для тела характеристики 0?

Задача 8. Является ли полупростым кольцо действительных верхнетреугольных 2×2 матриц?

Задача 9. Пусть $\mathbb{F}$ — поле, G — конечная группа. Докажите, что групповая алгебра $\mathbb{F}G$ полупроста тогда и только тогда, когда $\mathrm{char}F \nmid |G|$ (теорема Машке).

Задача 10. Покажите, что ни для какой конечной группы G групповое кольцо $\mathbb{Z}G$ не полупросто.

4 Радикал Джекобсона

Лекция 5. Радикал модуля. Радикал Джекобсона кольца. Теорема Хопкинса — Левицкого. Нильпотентность радикала артинова кольца.

Вспомним, что подмодуль $N \lneq M$ называется *максимальным*, если не найдется такого подмодуля K, что $N \lneq K \lneq M$. В силу теоремы о соответствии это равносильно тому, что M/N неприводим.

Определение 4.1. *Радикал Джекобсона* $\operatorname{rad} M$ модуля M — это пересечение всех максимальных подмодулей. Если максимальных подмодулей в M нет, то полагаем $\operatorname{rad} M = M$.

Вспомним, что $(\mathbb{Q}; +, 0)$ не имеет максимальных подгрупп (предложение 1.57), отсюда $\operatorname{rad} \mathbb{Q}_{\mathbb{Z}} = \mathbb{Q}$.

Лемма 4.2. Радикал $\operatorname{rad} M$ — это подмодуль в M. Если $N \leqslant M$, то из $\operatorname{rad}(M/N) = 0$ следует $\operatorname{rad} M \subseteq N$. Также выполнено $\operatorname{rad}(M/\operatorname{rad} M) = 0$.

Доказательство. Радикал — подмодуль как пересечение подмодулей. Остальное следует из теоремы о соответствии. □

Лемма 4.3. Радикал Джекобсона полупростого модуля равен 0.

Доказательство. Если $M = \bigoplus\limits_{i \in I} S_i$, S_i — неприводимые R-модули, то модули $M_j = \bigoplus\limits_{i \in I, i \neq j} S_i$ пересекаются по 0, а факторы $M/M_j \cong S_j$. □

Теорема 4.4. Модуль M_R конечно порождён и полупрост тогда и только тогда, когда он артинов и имеет нулевой радикал Джекобсона.

Доказательство. ($\Rightarrow$) Радикал равен нулю по лемме. Если M конечно порожденный полупростой модуль, то он изоморфен конечной прямой сумме неприводимых модулей (предложение 3.3). Тогда M артинов как конечная прямая сумма артиновых модулей (следствие 2.5).

($\Leftarrow$) Для $M = 0$ очевидно, пусть $M \neq 0$. В силу $\operatorname{rad} M = 0$ найдется семейство $S = \{M_i\}_{i \in I}$ подмодулей M, таких что $\bigcap_{i \in I} M_i = 0$ и все M/M_i неприводимы. Обозначим через P множество всевозможных конечных пересечений модулей из S. В

силу артиновости M, множество P содержит минимальный по включению элемент, скажем, $N = M_{i_1} \cap \ldots \cap M_{i_n}$. Покажем, что N может быть равен только 0. Предположим противное, тогда ввиду $\bigcap_{i \in I} M_i = 0$ можно найти подмодуль $M_i \not\supseteq N$. Откуда $M_i \cap N$ строго меньше N, что противоречит минимальности N.

Далее φ: $M \to (M/M_{i_1}) \oplus \ldots \oplus (M/M_{i_n})$, $m \mapsto (m + M_{i_1}, \ldots, m + M_{i_n})$ — это гомоморфизм R-модулей. Его ядро совпадает с $M_{i_1} \cap \ldots \cap M_{i_n} = N$, а потому нулевое. Значит, M изоморфен подмодулю конечнопорождённого полупростого модуля $(M/M_1) \oplus \ldots \oplus (M/M_n)$, следовательно M тоже полупрост и конечнопорождён (см. следствие 3.8 и предложение 3.3). □

Теорема 4.5 (о радикале Джекобсона кольца)**.** Пусть $R \neq 0$. Для элемента $r \in R$ эквивалентны следующие условия:

1) $Mr = 0$ для любого правого неприводимого R-модуля M;

2) r принадлежит пересечению всех максимальных правых идеалов R;

3) для всех $x \in R$ элемент $1 - rx$ обратим справа;

4) для всех $x, y \in R$ элемент $1 - yrx$ обратим;

1') $rM = 0$ для любого левого неприводимого R-модуля M;

2') r принадлежит пересечению всех максимальных левых идеалов R;

3') для всех $x \in R$ элемент $1 - xr$ обратим слева.

Доказательство. Поскольку 4) — симметричное условие, достаточно показать эквивалентность 1)–4).

1) $\Rightarrow$ 2) Если $N \subseteq R$ — максимальный правый идеал, то R_R/N — неприводимый модуль, откуда $(R/N)r = 0 + N$. Поэтому $0 + N = (1 + N)r = r + N$ и $r \in N$.

2) $\Rightarrow$ 3) Предположим противное. Пусть $1 - rx$ необратим справа, тогда $1 - rx$ содержится в некотором максимальном правом идеале N. В силу 2) получаем, что $rx \in N$, откуда $1 = (1 - rx) + rx \in N$. Противоречие с тем, что N собственный.

3) $\Rightarrow$ 1): Пусть $0 \neq m \in M$, где M — неприводимый модуль. Предположим, что $mr \neq 0$, тогда $mrR = M$. В частности, для некоторого x выполнено $mrx = m$, откуда $m(1 - rx) = 0$. Поскольку $1 - rx$ обратим справа по условию, имеем противоречие с тем, что $m \neq 0$.

4) $\Rightarrow$ 3) Положим $y = 1$.

1) + 3) $\Rightarrow$ 4) Так как $Mr = 0$ для всякого неприводимого модуля M, то для всех $y \in R$ имеем $Myr \subseteq Mr = 0$. Поэтому yr также удовлетворяет 1), а значит и 3), то есть $1 - (yr)x$ обладает правым обратным. Выберем его в виде $1 - b$, получаем $(1 - yrx)(1 - b) = 1$. Раскрывая скобки, имеем $b = -yrx(1 - b)$. Заметим, что $Mb = M(-yrx)(1 - b) \subseteq (Mr)x(1 - b) = 0$. Снова получаем, что b удовлетворяет 1), а значит и 3), то есть $1 - b$ имеет правый обратный, скажем, $1 - c$. Поэтому $1 - c = (1 - yrx)(1 - b)(1 - c) = 1 - yrx$, откуда $c = yrx$. Таким образом, $1 - b$ — двусторонний обратный для $1 - yrx$. □

Элементы, удовлетворяющие условиям предыдущей теоремы, образуют важный идеал кольца.

Определение 4.6. *Радикал Джекобсона* $J(R)$ кольца $R \neq 0$ — пересечение всех максимальных правых (эквивалентно, левых) идеалов R. Считаем также $J(0) = 0$.

Любой пункт предыдущей теоремы может быть взят в качестве определения радикала Джекобсона кольца.

Следствие 4.7. Радикал Джекобсона кольца является двусторонним идеалом.

Следствие 4.8. Радикал Джекобсона кольца совпадает с радикалами левого и правого регулярных модулей $J(R) = \operatorname{rad} R_R = \operatorname{rad}{}_R R$.

Доказательство. Максимальные левые (правые) идеалы — это в точности максимальные подмодули левого (правого) регулярного модуля. □

Отметим, что для колец без единицы, вообще говоря, $\operatorname{rad} R_R$ и $\operatorname{rad}{}_R R$ могут не совпадать.

Определение 4.9. *Аннулятором* правого R-модуля M называют множество $\operatorname{Ann} M = \{r \in R \mid mr = 0 \ \ \forall m \in M\}$.

Следствие 4.10. Радикал Джекобсона ненулевого кольца совпадет с пересечением аннуляторов всех неприводимых правых (эквивалентно левых) модулей.

Доказательство. Переформулировка пунктов 1), 1') теоремы. □

Для правого R-модуля M и некоторого подмножества $S \subseteq R$ положим $\operatorname{Ann}_M(S) = \{m \in M \mid ms = 0 \ \forall s \in S\}$. Кольцо R называется полулокальным, если факторкольцо $R/J(R)$ полупросто. Как мы дальше увидим, все артиновы кольца полулокальные. Полулокальные кольца будут рассмотрены подробнее в следующей лекции.

Теорема 4.11. Для любого правого R-модуля M выполнено $\operatorname{soc} M \subseteq \operatorname{Ann}_M(J(R))$. Если же факторкольцо $R/J(R)$ полупросто, то $\operatorname{soc} M = \operatorname{Ann}_M(J(R))$.

Доказательство. По определению цоколь является суммой всех неприводимых подмодулей, поэтому включение $\operatorname{soc} M \subseteq \operatorname{Ann}_M(J(R))$ вытекает из пункта 1) теоремы. Пусть $R/J(R)$ полупросто. Обозначим $N = \operatorname{Ann}_M(J(R))$, $\overline{R} = R/J(R)$. Надо доказать, что $N \subseteq \operatorname{soc} M$. На N естественным образом вводится струтура $\overline{R}$-модуля: $m(r + J(R)) = mr$. Т.к. кольцо $\overline{R}$ полупросто, то M — полупростой $\overline{R}$-модуль, т.е. $N_{\overline{R}} = \bigoplus_{i \in I}(N_i)_{\overline{R}}$, где все $(N_i)_{\overline{R}}$ неприводимы. Тогда $N_R = \bigoplus_{i \in I}(N_i)_R$, и все $(N_i)_R$ неприводимы. Поэтому $N_i \subseteq \operatorname{soc} M$ для всех i, откуда $N \subseteq \operatorname{soc} M$, что и требовалось. □

Определение 4.12. Элемент $r \in R$ называется *квазирегулярным*, если $1-r$ обратим. Аналогично определяется квазирегулярность справа и слева.

Определение 4.13. Правый (левый, двусторонний) идеал I называется *квазирегулярным*, если все его элементы квазирегулярны.

Следствие 4.14. Радикал Джекобсона является квазирегулярным идеалом и, более того, он содержит все правые, а также левые квазирегулярные идеалы.

Доказательство. Радикал квазирегулярен в силу пункта 4) теоремы при $x = y = 1$. Если I — правый квазирегулярный идеал, то для всех $r \in I$ и любого элемента x кольца R имеем $xr \in I$, а значит, $1 - rx$ обратим. Поэтому $I \subseteq J(R)$ в силу пункта 3) теоремы. □

Отметим, что какие-то отдельные квазирегулярные элементы могут и не содержаться в радикале.

Понятие квазирегулярного элемента может быть обобщено на случай кольца без единицы: элемент r квазирегулярен справа, если найдется элемент s, такой что $r + s = rs$. Для кольца с единицей это определение эквивалентно предыдущему, т.к. его можно переписать в виде $(1 + r)(1 + s) = 1$. Обобщенное понятие квазирегулярности позволяет определить радикал Джекобсона для кольца без единицы.

Определение 4.15. *Полупримитивное (полупростое по Джекобсону)* кольцо — это такое кольцо, у которого $J(R) = 0$.

Пример 4.16. Рассмотрим примеры колец с нулевым радикалом:

- простые кольца,
- полупростые кольца (лемма 4.2),
- кольцо целых чисел $J(\mathbb{Z}) = \bigcap\limits_{p \text{ простое}} p\mathbb{Z} = 0$;
- для любого кольца R выполнено $J(R/J(R)) = 0$ в силу теоремы о соответствии.

Следствие 4.17. Кольцо R полупросто тогда и только тогда, когда оно артиново справа и $J(R) = 0$.

Доказательство. Применим доказанную ранее теорему о конечнопорождённом полупростом модуле к R_R (теорема 4.4). □

Нам понадобится следующее вспомогательное утверждение.

Предложение 4.18. Если кольцо R артиново (нётерово) справа и $I \lhd R$, тогда факторкольцо R/I тоже артиново (нётерово) справа.

Доказательство. Если модуль R_R артинов, то R/I — артинов правый R-модуль (предложение 2.4). Пусть $M_1 \supseteq M_2 \supseteq \ldots$ — убывающая цепочка подмодулей R/I как правого R/I-модуля. Тогда она будет цепочкой подмодулей R/I как правого R-модуля. Цепочка оборвется в силу артиновости. Итак, R/I — артинов правый R/I-модуль, т.е. R/I — артиново справа кольцо. □

Аналогичное утверждение для подколец неверно.

Следствие 4.19. Если R артиново справа, то $R/J(R)$ полупросто.

Определение 4.20. *Нильпотент* $r \in R$ — это такой элемент кольца, что для некоторого натурального n выполнено $r^n = 0$. Наименьшее такое n будем называть *индексом нильпотентности* элемента.

Пример нильпотентного элемента: в матричном кольце возьмем верхнетреугольную матрицу, все диагональные элементы которой нулевые.

Если нильпотенты r, s коммутируют, то $r + s$ также нильпотентен, поскольку после раскрытия скобок в $(r + s)^{k+m}$ каждый множитель кратен либо r^k, либо s^m. В некоммутативном кольце сумма нильпотентов может быть обратимой (E_{12}, E_{21} в $M_2(\mathbb{F})$).

Определение 4.21. Произведением подгрупп A и B аддитивной группы $(R, +)$ кольца R называется множество, состоящее из всех возможных конечных сумм вида $a_1b_1 + \ldots + a_nb_n$, где $a_i \in A$, $b_i \in B$, $n \in \mathbb{N}$.

Заметим, что если A — левый идеал, то AB — левый идеал. Аналогично, если B — правый идеал, то AB — правый идеал. В частности, произведение двусторонних идеалов будет двусторонним идеалом. В дальнейшем нас будут интересовать степени правых (левых, двусторонних) идеалов $I^n = \underbrace{I \cdot \ldots \cdot I}_{n \text{ раз}}$. Иногда удобно считать $I^0 = R$.

Определение 4.22.

- Правый идеал, все элементы которого нильпотентны, называется *правым нильидеалом.*
- Правый идеал I называется *нильпотентным*, если $I^n = 0$ для некоторого n. Это равносильно тому, что $i_1 \cdot \ldots \cdot i_n = 0$ для всех $i_j \in I$. Наименьшее такое n называют *индексом нильпотентности.*

Аналогичные определения можно дать для левых и двусторонних идеалов.

Всякий правый нильпотентный идеал является правым нильидеалом. Обратное неверно.

Пример 4.23. В кольце $\mathbb{Q}[x_2, \ldots, x_n, \ldots]$ от счётного числа переменных рассмотрим идеал I, порожденный множеством $\{x_2^2, x_3^3, \ldots, x_n^n, \ldots\}$. Тогда в факторкольце $R = \mathbb{Q}[x_2, \ldots, x_n, \ldots]/I$ идеал, порожденный множеством $\{x_2+I, \ldots, x_n+I, \ldots\}$ является нильидеалом, который не нильпотентен. Более того, индексы нильпотентности элементов этого идеала не ограничены.

Предложение 4.24. Всякий правый (левый) нильидеал I содержится в $J(R)$. В частности, всякий нильпотентный правый (левый) идеал содержится в $J(R)$

Доказательство. Нильидеал квазирегулярен. Действительно, если $r^n = 0$, то $1 - r$ обратим т.к. $(1 - r)(1 + r + r^2 + \ldots + r^{n-1}) = 1 - r^n = 1$, причем эти две скобки коммутируют. □

Теорема 4.25. Пусть R — артиново справа кольцо, тогда $J(R)$ нильпотентен.

Доказательство. В силу артиновости R_R для цепочки $J \supseteq J^2 \supseteq \ldots$ имеем $J^k = J^{k+1} = \ldots$, начиная с некоторого k. Предположим, что $J^k \neq 0$. Рассмотрим множество Ω, состоящее из всех правых идеалов L таких, что $L \subseteq J^k$ и $LJ^k \neq 0$. Множество Ω не пусто, т.к. содержит J^k. В силу артиновости R_R, в Ω есть некоторый минимальный элемент, обозначим его тоже как L. Заметим, что $LJ^k \in \Omega$, т.к. $(LJ^k)J^k = LJ^{2k} = LJ^k \neq 0$. В то же время $LJ^k \subseteq L$, откуда $LJ^k = L$ в силу минимальности L.

Ввиду $LJ^k \neq 0$ найдется элемент $\ell \in L$ такой, что $\ell J^k \neq 0$. Отсюда правый идеал ℓR принадлежит Ω. Однако $\ell R \subseteq L$, а значит, $\ell R = L$ в силу минимальности L. Тогда в силу предыдущего выполнено $(\ell R)J^k = \ell R$. Поэтому найдётся $j \in J^k$, для которого $\ell j = \ell$, откуда $\ell(1 - j) = 0$, но $1 - j$ обратим из-за квазирегулярности радикала. Поэтому $\ell = 0$ и $0 = \ell R = L = LJ^k$. Противоречие с тем, что $L \in \Omega$. □

Следствие 4.26. В артиновом кольце радикал Джекобсона совпадает с наибольшим нильпотентным идеалом. В частности, это верно для конечномерной ассоциативной алгебры над полем.

Пример 4.27. Если R — алгебра верхнетреугольных матриц нал полем, то множество матриц с нулевой диагональю является наибольшим нильпотентным идеалом, а потому совпадает с радикалом Джекобсона.

Следствие 4.28. Артиново кольцо полупросто тогда и только тогда, когда в нём нет ненулевых двусторонних нильпотентных идеалов.

Доказательство. Артиново кольцо полупросто тогда и только тогда, когда его радикал Джекобсона равен нулю. □

Пусть M — правый R-модуль, A — подгруппа аддитивной группы $(M, +)$, I — правый идеал кольца R. Тогда определим произведение AI как множество всех возможных конечных сумм вида $a_1r_1 + \ldots + a_nr_n$, где $a_i \in A$, $r_i \in I$, $n \in \mathbb{N}$. Непосредственно проверяется, что AI — подмодуль в M.

Лемма 4.29 (лемма Накаямы-1)**.** Пусть M — конечнопорождённый правый R-модуль. Если выполнено $MJ(R) = M$, тогда $M = 0$. Другими словами, для ненулевого модуля M всегда $MJ(R) \subsetneq M$

Доказательство. Пусть $M \neq 0$. Т.к. M конечно порожден, то в нём можно выбрать максимальный собственный подмодуль N (теорема 1.58). Тогда M/N неприводим и $(M/N)j = 0$ для всех $j \in J(R)$, откуда $MJ(R) \subseteq N \subsetneq M$. □

Следствие 4.30 (лемма Накаямы-2)**.** Пусть M_R — конечнопорождённый правый R-модуль, $N \leqslant M$ — его подмодуль, а правый идеал I содержится в $J(R)$. Если выполнено $MI + N = M$, то $N = M$.

Доказательство. Факторизуем по N соотношение из условия:

$$M/N = (MI + N)/N = \langle\{mr + N \mid m \in M,\ r \in I\}\rangle_{\mathbb{Z}} = (M/N)I \subseteq (M/N)J(R).$$

Значит, $M/N = (M/N)J(R)$ и $M/N = 0$ по предыдущей лемме. □

Теорема 4.31. Для правого модуля M над артиновым справа кольцом R эквивалентны следующие условия:

1) M артинов;
2) M нётеров;
3) M конечно порождён.
4) M обладает композиционным рядом;

Доказательство. 1) $\Rightarrow$ 2) Пусть $J = J(R)$. Согласно теореме 4.25, $J^n = 0$ для некоторого $n \in \mathbb{N}$. Каждый из модулей $F_i = MJ^{i-1}/MJ^i$, $i = 1, 2, \dots n$ (считая, что $J^0 = R$) аннулируется J, и на нём естественным образом вводится структура R/J-модуля: для $f \in F_i$ полагаем $f(r + J(R)) = fr$. Заметим, что у F_i множества всех R/J-подмодулей и R-подмодулей совпадают, поэтому условия артиновости (нётеровости) F_i как R-модуля равносильно такому же условию для F_i как R/J-модуля. Т.к. кольцо R/J полупросто (следствие 4.19), то каждый из F_i полупрост, т.е. является прямой суммой некоторого множества неприводимых модулей. Эта сумма не может быть бесконечной в силу артиновости. Действительно, любое бесконечное множество содержит счётное подмножество, а счётная прямая сумма $\oplus_{i=1}^{\infty} V_i$ содержит подмодули $K_i = \oplus_{j=i}^{\infty} V_j$, образующие бесконечную строго убывающую цепь. Следовательно, каждый из модулей F_i есть конечная прямая сумма неприводимых (а значит, нётеровых) модулей и является нётеровым модулем. В силу $MJ^n = 0$, получаем, что R-модуль MJ^{n-1} равен $MJ^{n-1}/MJ^n = F_n$, а значит, нётеров. Из нётеровости MJ^{n-1} и $F_{n-1} = MJ^{n-2}/MJ^{n-1}$ следует нётеровость MJ^{n-2}(предложение 2.4) и так далее. В итоге мы получаем, что $M = MJ^0$ нётеров.

2) $\Rightarrow$ 3) Любой подмодуль нётерова модуля конечно порождён, в частности, он сам (предложение 2.6).

3) $\Rightarrow$ 1) Конечнопорождённый правый модуль над артиновым справа кольцом артинов (предложение 2.14).

4) $\Leftrightarrow$ 1) & 2) Верно для любого модуля (следствие 2.25). □

Следствие 4.32 (Теорема Хопкинса)**.** Артиново справа кольцо (напомним: с единицей!) нётерово справа.

Доказательство. Если R артиново справа, то R_R — конечно порожденный (порожден единицей) артинов модуль над артиновым справа кольцом. □

Контрпример для колец без единицы: кольцо с нулевым умножением на p-квазициклической группе $\mathbb{Z}_{p^\infty} \cong \{\zeta \in \mathbb{C} \mid \exists k \in \mathbb{N}\ \zeta^{p^k} = 1\}$ (она является нётеровым, но не артиновым, $\mathbb{Z}$-модулем).

Определение 4.33. Элемент $a \in R$ называется *регулярным по фон Нейману*, если он обладает *псевдообратным* элементом x, для которого $axa = a$. Если все элементы R регулярны по фон Нейману, то и кольцо R также называется регулярным по фон Нейману.

Предложение 4.34. Регулярное по фон Нейману кольцо полупримитивно.

Доказательство. Если $a = axa$, где $a \in J(R)$, то $(1 - xa)$ обратим, поэтому из $a(1 - xa) = 0$ следует $a = 0$. □

Пример 4.35. Пусть $V = \mathbb{F}^\infty$ — пространство всех (счётных) последовательностей $\{x_1, x_2, \ldots\}$ элементов поля $\mathbb{F}$, и $R = \operatorname{End} V$. Его можно понимать как $\mathbb{F}$-алгебру *столбцово-конечных* матриц: элементы этих матриц индексируются парами натуральных чисел, причём в каждом столбце лишь конечное число ненулевых элементов, что позволяет определить умножение таких матриц.

Тогда по упражнению R регулярно по фон Нейману и полупримитивно, но не артиново справа: строго возрастающую цепочку образуют идеалы вида "все строки, кроме первых n, пусты". Поэтому R не полупросто.

Задачи к лекции 5.

Задача 1. Привести пример кольца без единицы, в котором не совпадают пересечение всех левых максимальных идеалов и всех правых максимальных идеалов.

Задача 2. Описать все идемпотенты, содержащиеся в $J(R)$.

Задача 3. Построить коммутативное кольцо R, радикал Джекобсона $J(R)$ которого имеет индекс нильпотентности 3, но все элементы $J(R)$ имеют нулевые квадраты.

Задача 4. Доказать, что в коммутативном кольце сумма обратимого элемента и нильпотента обратима. Верно ли это для некоммутативных колец?

Задача 5. Пусть J — некоторый идеал, содержащийся в $J(R)$. Докажите, что для любого i элементы $1+J^i$ образуют группу по умножению, а также что факторгруппа $(1+J^i)/(1+J^{i+1})$ определена и изоморфна аддитивной группе $J^i/(J^{i+1})$.

Задача 6. Для любого $n>1$ и кольца R покажите, что $J(M_n(R))=M_n(J(R))$.

Задача 7. Найдите $J(R[x])$ для коммутативного кольца коэффициентов R.

Задача 8. Найдите $J(\mathbb{F}_3 S_3)$. Указание: воспользуйтесь тем, что в артиновом кольце радикал Джекобсона — это наименьший идеал, фактор по которому полупрост, а также характеризацией радикала в терминах действия на неприводимые модули.

Задача 9. 1) Докажите, что кольцо эндоморфизмов полупростого правого модуля регулярно по фон Нейману.

2) Найдите все регулярные элементы кольца $M_n(\mathbb{Z})$.

Задача 10. Доказать, что в $\operatorname{End}\mathbb{F}^\infty$ есть ровно один ненулевой собственный идеал — множество операторов с конечномерным образом. Поэтому $J(R)$ может не совпадать с пересечением всех двусторонних идеалов R.

Задача 11. Докажите, что если в правом идеале I все элементы квазирегулярны справа, то I квазирегулярен.

5 Локальные, полулокальные и полусовершенные кольца. Поднятие идемпотентов.

Лекция 6. Локальные, полулокальные и полусовершенные кольца. Поднятие идемпотентов.

Определение 5.1. Для кольца R обозначим через $R^\times$ — множество всех обратимых элементов кольца. При $R\neq 0$ множество $R^\times\neq\varnothing$ является группой по умножению, которую называют *мультипликативной группой кольца.*

Теорема 5.2 (О локальном кольце)**.** Для $R\neq 0$ следующие условия эквивалентны:

1) $R/J(R)$ — тело.

2) $J(R)$ — максимальный правый идеал в R;

2') $J(R)$ — максимальный левый идеал в R;

3) R обладает единственным максимальным правым идеалом;

3') R обладает единственным максимальным левым идеалом;

4) $J(R)$ содержит все необратимые элементы кольца, т.е. $R=R^\times\sqcup J(R)$;

5) необратимые элементы R составляют собственный идеал;

6) необратимые элементы R составляют группу по сложению;

7) для любого $n \in \mathbb{N}$, если $r_1 + \ldots + r_n \in R^\times$, то хотя бы один $r_i \in R^\times$;

8) если $r + s \in R^\times$, то по крайней мере один элемент r или s принадлежит $R^\times$;

9) для всех $r \in R$ по крайней мере один элемент r или $1 - r$ обратим;

10) для всех $r \in R$ по крайней мере один элемент r или $1 - r$ обратим справа;

10') для всех $r \in R$ по крайней мере один элемент r или $1 - r$ обратим слева;

Доказательство. 1) $\Rightarrow$ 2) В теле $R/J(R)$ нет нетривиальных правых идеалов, откуда по теореме о соответствии идеалов $J(R)$ — максимальный правый идеал в R.

2) $\Rightarrow$ 3) Если N — максимальный правый идеал, то $J(R) \subseteq N$, откуда $J(R) = N$ в силу максимальности $J(R)$.

3) $\Rightarrow$ 1) Т.к. $J(R)$ — пересечение всех максимальных правых идеалов, то $J(R)$ совпадает с тем самым единственным максимальным правым идеалом. Тогда в силу теоремы о соответствии идеалов в факторкольце $R/J(R)$ нет нетривиальных правых идеалов, значит, $R/J(R)$ — тело (теорема 1.59).

1) $\Rightarrow$ 2') $\Rightarrow$ 3') $\Rightarrow$ 1) Аналогично предыдущему в силу симметричности 1).

3) & 3') $\Rightarrow$ 4) Если r необратим, то он необратим хотя бы с одной стороны, скажем, справа (слева). Тогда r лежит в некотором максимальном правом (левом) идеале. Но $J(R)$ — единственный максимальный правый (левый) идеал, откуда $r \in J(R)$.

4) $\Rightarrow$ 5) $\Rightarrow$ 6) Получается сразу.

6) $\Rightarrow$ 7) Если все r_i необратимы, то их сумма тоже необратима в силу 6).

7) $\Rightarrow$ 8) Частный случай.

8) $\Rightarrow$ 9) Имеем $r + (1 - r) = 1 \in R^\times$.

9) $\Rightarrow$ 10) Частный случай.

10) $\Rightarrow$ 1) Выберем произольный $a \notin J(R)$. По определению радикала найдется максимальный правый идеал $N \not\ni a$. В силу максимальности N, правый идеал $N + aR$ не может быть собственным, а значит, содержит 1. Поэтому для некоторых $n \in N$, $r \in R$ выполнено $1 = n + ar$. Т.к. n необратим справа, то $1 - n = ar$ обратим справа в силу 10), откуда a обратим справа. В силу произвольности $a \notin J(R)$, получаем, что все ненулевые элементы факторкольца $R/J(R)$ обратимы справа, это одно из эквивалентных определений тела (теорема 1.59).

9) $\Rightarrow$ 10') $\Rightarrow$ 1) Аналогично. □

Определение 5.3. Кольцо R *локально*, если у него есть единственный максимальный правый (эквивалентно, левый) идеал.

Любой пункт предыдущей теоремы может быть взят в качестве определения локального кольца.

Следствие 5.4. Если кольцо R локально, то оно содержит единственный максимальный двусторонний идеал. Обратное верно в случае коммутативного кольца R.

Например, в кольце матриц над телом 0 — единственный максимальный двусторонний идеал, но это кольцо не локально.

Следствие 5.5. Если все необратимые элементы нильпотентны, то кольцо локально.

Доказательство. Если $x^n = 0$, то $1 - x$ — обратный к $(1 + x + \ldots + x^{n-1})$. □

Следствие 5.6. Для элемента r локального кольца R следующие условия равносильны: 1) r обратим справа, 2) r обратим слева, 3) r обратим, 4) $r \notin J(R)$.

Доказательство. Если элемент необратим с какой-либо стороны, то он лежит в некотором максимальном одностороннем идеале, который совпадает с $J(R)$. Однако $J(R)$ — собственный идеал, поэтому этот элемент необратим с двух сторон. □

Пример 5.7.

- Кольцо вычетов $\mathbb{Z}_n$ локально тогда и только тогда, когда $n = p^k$ для некоторого простого p.
- Для простого p рассмотрим множество $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$, состоящее из дробей, у которых в несократимом виде знаменатель не делится на p. Тогда $\mathbb{Z}_{(p)}$ является локальным кольцом: необратимые элементы имеют вид $\frac{m}{n}$, где m делится на p, но n не делится на p — все такие дроби образуют собственный идеал.
- Если D — тело, то локальным является кольцо R, состоящее из таких верхнетреугольных $n \times n$ матриц A над телом, что $(A)_{11} = (A)_{22} = \ldots = (A)_{nn}$. В этом случае $J(R)$ состоит из матриц с нулевой диагональю и $R/J(R) \cong D$.

Определение 5.8. *Идемпотент* $r \in R$ — такой элемент, что $r^2 = r$.

В любом кольце имеются тривиальные идемпотенты: 0 и 1. Примеры нетривиальных идемпотентов — диагональные матричные единицы E_{ii} в матричных кольцах.

Идемпотенты играют важную роль в разложениях в прямую сумму. Если M_R — модуль, то разложение M в прямую сумму подмодулей $M = M_1 \oplus M_2$ равносильно наличию в $\operatorname{End} M_R$ идемпотентов-проекций: $eM = M_1$, $(1 - e)M = M_2$. Это следует из представления $\operatorname{End} M_R$ в виде кольца формальных матриц: $e = \left(\begin{smallmatrix} \mathrm{id}_{M_1} & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $1 - e = \left(\begin{smallmatrix} 0 & 0 \\ 0 & \mathrm{id}_{M_2} \end{smallmatrix}\right)$.

Предложение 5.9. Пусть $e, f \in R$ — идемпотенты. Тогда абелева группа fRe изоморфна абелевой группе $\operatorname{Hom}((eR)_R, (fR)_R)$ всех гомоморфизмов правых R-модулей $eR \to fR$. Более того, имеется изоморфизм колец $\operatorname{Hom}((eR)_R, (eR)_R) = \operatorname{End}(eR)_R \cong eRe$.

Доказательство. Пусть $\psi \in \mathrm{Hom}(eR, fR)$, тогда при $\psi(e) = fr$ имеем $\psi(e) = \psi(e^2) = \psi(e)e = fre \in fRe$, поскольку ψ — гомоморфизм модулей. Определим отображение θ: $\mathrm{Hom}(eR, fR) \to fRe$, $\psi \mapsto \psi(e)$. Как видно, оно является сюръективным гомоморфизмом абелевых групп. Если $\theta(\psi) = 0$, то $\psi(er_1) = \psi(e)r_1 = 0$ для всех $r_1 \in R$, поэтому $\psi(e) = 0$, и θ — изоморфизм.

При $e = f$ можно аналогично проверить, что отображение θ сохраняет умножение. □

Определение 5.10. Модуль M_R *неразложим*, если он не раскладывается в прямую сумму двух ненулевых подмодулей, или, эквивалентно, если $\mathrm{End}\, M$ не содержит нетривиальных идемпотентов.

Неприводимый модуль неразложим; $(\mathbb{Z}_4)_{\mathbb{Z}_4}$ — неразложимый модуль, не являющийся неприводимым.

Предложение 5.11 (лемма Фиттинга, напоминание)**.** Пусть M — артинов и нётеров модуль, $\varphi \in \mathrm{End}\, M$. Тогда для некоторого n выполнено $M = \varphi^n(M) \oplus \ker \varphi^n$ (произведение эндоморфизмов — их композиция).

Следствие 5.12. Если M — неразложимый артинов и нётеров модуль, то любой его эндоморфизм либо биективен, либо нильпотентен. В частности, кольцо $\mathrm{End}\, M$ локально.

Доказательство. Для произвольного $\varphi \in \mathrm{End}\, M$ в разложении Фиттинга одно из слагаемых будет нулевым в силу неразложимости M. Это значит, что φ — либо автоморфизм, либо нильпотент. □

Предложение 5.13. Все идемпотенты локального кольца — это 0 и 1.

Доказательство. Пусть R локально. Если $e^2 = e$, то какой-то из элементов $e, 1 - e$ обратим, однако $e(1 - e) = 0$, поэтому другой элемент нулевой. □

Отметим, что если в кольце есть только тривиальные идемпотенты, то кольцо не обязано быть локальным (например, $\mathbb{Z}$). Тем не менее имеет место следующий факт.

Теорема 5.14. Пусть кольцо $R \neq 0$ артиново справа. Тогда R локально в том и только в том случае, когда все его идемпотенты — это 0 и 1.

Доказательство. По свойствам кольца эндоморфизмов регулярного модуля $R \cong \mathrm{End}\, R_R$. Т.к. модуль R_R артинов, то он будет и нётеровым. Все идемпотенты кольца $R \cong \mathrm{End}\, R_R$ тривиальны, поэтому R_R — неразложимый R-модуль. Отсюда $R \cong \mathrm{End}\, R_R$ локальное кольцо согласно следствию из леммы Фиттинга. □

Определение 5.15. Кольцо R назвается *полулокальным*, если факторкольцо $R/J(R)$ полупросто.

Предложение 5.16. 1) Кольцо R с конечным числом максимальных правых идеалов полулокально. 2) Если R полулокально и $R/J(R)$ коммутативно, то в R конечное число максимальных правых идеалов.

Доказательство. 1) Обозначим $\overline{R} = R/J(R)$. Если в R конечное число максимальных правых идеалов, то для $\overline{R}$ это тоже верно в силу теоремы о соответствии. Пусть $N_1, \ldots, N_n$ — это все максимальные правые идеалы $\overline{R}$, их пересечение равно $J(\overline{R})$, а значит, является нулевым идеалом кольца $\overline{R}$. Тогда отображение правых $\overline{R}$-модулей $\overline{R}_{\overline{R}} \mapsto \bigoplus_{i=1}^{n} \overline{R}_{\overline{R}}/N_i$ имеет нулевое ядро. По теореме о гомоморфизме $\overline{R}_{\overline{R}}$ изоморфен подмодулю полупростого модуля, а значит, и сам полупрост.

2) Кольцо $R/J(R)$ коммутативно и полупросто, поэтому оно изоморфно прямому произведению полей $\mathbb{F}_1 \times \ldots \times \mathbb{F}_n$. Отсюда в $R/J(R)$ лишь конечное число максимальных правых идеалов, это в точности идеалы вида $\mathbb{F}_1 \times \ldots \mathbb{F}_{i-1} \times 0 \times \mathbb{F}_{i+1} \times \ldots \mathbb{F}_n$. По теореме о соответствии идеалов в R тоже будет конечное число максимальных правых идеалов. □

Отметим, что в общем случае в полулокальном кольце может быть бесконечно много максимальных правых идеалов. В качестве примера можно рассмотреть кольцо $n \times n$ матриц над бесконечным полем при $n \geqslant 2$.

Пример 5.17.

- Всякое локальное кольцо полулокально.
- Всякое артиново слева или справа кольцо также полулокально. В частности, всякое конечное кольцо и всякая конечномерная алгебра над полем полулокальны.
- Если R полулокально, то и $M_n(R)$ полулокально, поскольку $J(M_n(R)) = M_n(J(R))$ и $M_n(R)/J(M_n(R)) \cong M_n(R/J(R))$. В частности, кольцо матриц над локальным кольцом полулокально.
- Конечное прямое произведение полулокальных колец также полулокально в силу $J(R \times S) = J(R) \times J(S)$.

Следующий результат приведем без доказательства.

Теорема 5.18 (Кэмпс, Дикс, 1993)**.** Кольцо эндоморфизмов правого артинового модуля полулокально.

Определение 5.19. Пусть $I \subseteq R$ — произвольное подмножество кольца R. Говорят, что *идемпотенты поднимаются по модулю* множества I, если для каждого $r \in R$ такого, что $r - r^2 \in I$, существует идемпотент e, удовлетворяющий $e - r \in I$.

Если I — двусторонний идеал кольца R, то определение равносильно следующему: для любого смежного класса $r+L$, который является идемпотентом в факторкольце R/I, найдется представитель $e \in r+I$, который будет идемпотентом в исходном кольце R.

Напомним, что идеал называется нильидеалом, если для каждого его элемента найдётся степень, при возведении в которую он обратится в ноль.

Теорема 5.20. Идемпотенты поднимаются по модулю любого нильидеала.

Доказательство (Лэди, 1997). Рассмотрим произвольный нильидеал $I \lhd R$. Пусть $\pi : R \to R/I$ — это естественная проекция. Предположим, что элемент $r \in R$ удовлетворяет соотношению $r - r^2 \in I$, что равносильно $\pi(r) = \pi(r)^2$. Необходимо найти идемпотент $e \in R$ такой, что $e - r \in I$.

Обозначим $s = 1-r$. Тогда элементы r, s коммутируют, т.е. $rs = sr$. Более того, их произведение $rs = r - r^2$ лежит в идеале I. Так как I — это нильидеал, то найдётся такое k, что $0 = (rs)^k = r^k s^k$.

Положим $x = 1 - r^k - s^k$. Покажем, что x также принадлежит идеалу I. Действительно, имеем $1 = r + s$, откуда $1 = (r+s)^k$. Так как r и s коммутируют, то применима формула бинома Ньютона: $1 = r^k + rs(\ldots) + s^k$. Ввиду $rs \in I$ получаем $\pi(x) = \pi(1 - r^k - s^k) = \pi(rs)\pi(\ldots) = 0$, откуда $x \in I$.

Так как I — нильидеал, то $x^\ell = 0$ некоторого ℓ. Поэтому $1-x$ обладает обратным по умножению $u = 1 + x + \ldots + x^{\ell-1}$. Элемент x выражается как многочлен от r, s, откуда u — это тоже многочлен от r, s, значит, u коммутирует с ними.

Наконец положим $e = ur^k$, $f = us^k$.

Заметим, что $e+f = 1$. Действительно, $1 = u(1-x) = u(r^k+s^k) = ur^k+us^k = e+f$. Кроме того, $ef = fe = 0$ в силу того, что $r^k s^k = 0$ и все элементы r, s, u коммутируют. Тогда e является идемпотентом: $e = e \cdot 1 = e(e+f) = e^2 + ef = e^2$. Кроме того, $\pi(e) = \pi(u)\pi(r)^k = (1 + \pi(x) + \ldots + \pi(x)^{\ell-1})\pi(r)^k = \pi(r)$, т.е. $e - r \in I$.

Доказательство (Ламбек). Пусть $q = u^2 - u \in I$; будем искать идемпотент e в виде $u + x(1-2u)$ для некоторого x, коммутирующего с u. Тогда $e^2 = e$ равносильно $u^2 + 2ux - 4u^2x + x^2 - 4ux^2 + 4u^2x^2 - u - x + 2ux = 0$, то есть $(x^2 - x)(4q+1) + q = 0$.

Если рассмотреть это уравнение в действительных числах (при малых $q \in \mathbb{R}$), то оно имеет два решения $x_{1,2} = 1/2 \pm (1+4q)^{-1/2}/2$, выражающиеся в виде степенных рядов от q с целыми коэффициентами. Поскольку элемент $q \in R$ нильпотентен, эти разложения в ряды имеют смысл и в R.

Осталось выполнить требование $e - u = x(1-2u) \in I$, для этого нужно выбрать степенной ряд со знаком минус после $1/2$. □

□

Определение 5.21. *Полусовершенное* кольцо R — это полулокальное кольцо, идемпотенты которого поднимаются по модулю $J(R)$.

Следствие 5.22. Артиново справа кольцо полусовершенно.

Доказательство. Радикал артинова справа кольца R всегда нильпотентен и $R/J(R)$ полупросто. □

Пример 5.23. Пусть K — это такое локальное кольцо, что $\mathbb{F} = K/J(K)$ является полем. Например, K коммутативно. Покажем, что кольцо матриц $R = M_n(K)$ полусовершенно. Действительно, $R/J(R) = M_n(K)/M_n(J(K)) \cong M_n(\mathbb{F})$ поэтому R полулокально. Пусть $P \in M_n(\mathbb{F})$ — идемпотент. Он соответствует проекции векторного пространства $\mathbb{F}^n$ на подпространство W, являющееся образом P. Пусть W' это образ $E - P$, тогда $W \oplus W' = \mathbb{F}^n$. Зададим новый базис в $\mathbb{F}^n$ такой, что сначала в нём идут базисные векторы W, а затем W', пусть C — матрица перехода к этому базису. Тогда $C^{-1}PC = \operatorname{diag}(1_\mathbb{F}, \ldots, 1_\mathbb{F}, 0_\mathbb{F}, \ldots, 0_\mathbb{F})$. Рассмотрим гомоморфизм π_n: $M_n(K) \to M_n(\mathbb{F})$, действующий на элементах матриц как $\pi : K \to K/J(K) = \mathbb{F}$. Пусть Q и Q' — любые матрицы из $M_n(K)$, лежащие в прообразах $\pi_n^{-1}(C)$ и $\pi_n^{-1}(C^{-1})$, соответственно. Тогда $QQ' = E + B_1$ и $Q'Q = E + B_2$ для некоторых матриц $B_1, B_2 \in J(R) = M_n(J(K))$. В силу квазирегулярности радикала $J(R)$ матрицы $E + B_1$ и $E + B_2$ обратимы, откуда $QQ'(E + B_1)^{-1} = E$ и $(E + B_2)^{-1}Q'Q = E$, т.е. матрица Q обладает и правой, и левой обратной, но они должны совпадать. Мы получили, что Q обратима. Наконец рассмотрим матрицу $S = Q \operatorname{diag}(1_K, \ldots, 1_K, 0_K, \ldots, 0_K)Q^{-1}$. Заметим, что S — идемпотент, причем $\pi_n(S) = \pi_n(Q)\pi_n(\operatorname{diag}(1_K, \ldots, 1_K, 0_K, \ldots, 0_K))\pi_n(Q)^{-1} = C\operatorname{diag}(1_\mathbb{F}, \ldots, 1_\mathbb{F}, 0_\mathbb{F}, \ldots, 0_\mathbb{F})C^{-1} = P$. Мы показали, что произвольный идемпотент P поднимается по модулю радикала.

Определение 5.24. Множество идемпотентов $\{e_i\}_{i \in I}$ называется *ортогональным*, если $e_i e_j = 0$ при $i \neq j$.

Условие ортогональности бывает удобно записывать в виде $e_i e_j = \delta_{ij} e_i$, где *символ Кронеккера* δ_{ij} равен единице при $i = j$ и нулю иначе.

Лемма 5.25. Пусть $e_1, \ldots, e_n$ — система ортогональных идемпотентов и f — произвольный идемпотент. Тогда $e = \sum\limits_{i=1}^{n} e_i$ — также идемпотент. Более того, если f ортогонален e, то он ортогонален и каждому e_i.

Доказательство. Первое утверждение проверяется непосредственно: $e^2 = \sum\limits_{i=1}^{n} e_i^2 + \sum\limits_{i \neq j} e_i e_j = \sum\limits_{i=1}^{n} e_i$. Пусть $fe = ef = 0$. Тогда для каждого идемпотента e_i имеем $-fe_i = fee_i - fe_i^2 = f(e - e_i)e_i = f(e_1 + \ldots + e_{i-1} + e_{i+1} + \ldots + e_n)e_i = 0$, поскольку e_i ортогонален всем элементам в скобках. □

Определение 5.26. Идемпотент $e \in R$ кольца называется *примитивным*, если он ненулевой и его нельзя представить в виде суммы двух ненулевых идемпотентов s, f таких, что $sf = fs = 0$.

Определение равносильно тому, что правый идеал eR (эквивалентно левый идеал Re) — неразложимый правый (левый) R-модуль. Тогда в кольце eRe элемент e — единственный ненулевой идемпотент. Если ere — идемпотент, то $e - ere$ тоже будет идемпотентом, тогда $e = (e - ere) + ere$, и из неразложимости получаем, что либо $ere = 0$, либо $e = ere$.

Далее мы рассмотрим ортогональные системы идемпотентов нётеровых колец. Нам понадобятся две леммы.

Лемма 5.27. Если кольцо R нётерово справа, то в нём не может быть бесконечного множества ненулевых попарно ортогональных идемпотентов.

Доказательство. От противного, тогда R содержит по крайней мере счётное множество $\{e_i\}_{i\in\mathbb{N}}$ попарно ортогональных ненулевых идемпотентов. Значит, невозможно разложение вида $e_{k+1} = e_1r_1 + \ldots + e_kr_k$, ведь иначе, домножив слева на e_{k+1}, мы получили бы $e_{k+1} = 0$. Отсюда $e_1R \subsetneq e_1R+e_2R \subsetneq \ldots$ — строго возрастающая цепочка правых идеалов, что противречит нётеровости. □

Граф G *связен*, если между любыми двумя вершинами существует конечный путь, соединяющий их. Граф G *локально компактен*, если каждая вершина соединена ребром лишь с конечным числом вершин. Путь в графе называется *простым*, если он не содержит повторяющихся вершин. Отметим, что в связном графе между любыми двумя вершинами найдется простой путь, соединяющий их.

Лемма 5.28 (Лемма Кёнига)**.** Пусть G — локально компактный связный граф с бесконечным числом вершин. Тогда в G существует простой путь, проходящий через бесконечное число вершин и начинающийся в произвольно выбранной вершине.

Доказательство. Выберем любую вершину v_1. По условию из v_1 выходит простой путь конечной длины в любую вершину. Таких путей бесконечно много, т.к. в G бесконечно много вершин. При этом v_1 соединена ребром лишь с конечным числом вершин. Среди них по принципу Дирихле найдётся вершина v_2, через которую проходит бесконечно много указанных путей. Строим путь $v_1e_1v_2$. Пусть мы построили путь $v_1e_1 \ldots v_{k-1}e_{k-1}v_k$ такой, что через v_k идут простые пути в бесконечное множество вершин, причем начала этих путей совпадают с $v_1e_1 \ldots v_{k-1}e_{k-1}v_k$. Но опять v_k соединена ребром лишь с конечным числом вершин. По принципу Дирихле через какую-то вершину v_{k+1} проходит бесконечно много таких путей. При этом v_{k+1} не может совпадать ни с одной из вершин $v_1, \ldots, v_k$, т.к. все рассматриваемые пути простые. Строим путь $v_1e_1 \ldots v_{k-1}e_{k-1}v_ke_kv_{k+1}$ и т.д. □

Напомним, что дерево — это связный граф без циклов.

Теорема 5.29. В нётеровом справа кольце $R \neq 0$ существует конечное ортогональное множество примитивных идемпотентов, сумма которых равна 1.

Доказательство. Если 1 — примитивный идемпотент, то доказывать нечего. Пусть 1 не примитивна. Предположим, что 1 нельзя представить в виде суммы ортогональных примитивных идемпотентов. Будем строить дерево, вершины которого — идемпотенты кольца R. Корень дерева соответствует 1. Так как 1 не примитивна, то её можно представить в виде суммы двух ортогональных идемпотентов $1 = e+f$. Добавим единице в графе две дочерние вершины e, f. Пусть мы построили разложение единицы в сумму m ортогональных идемпотентов $1 = e_1 + \ldots + e_m$. По нашему предположению по крайней мере один e_i не примитивен, значит, $e_i = f_1 + f_2$, где f_1, f_2 — ортогональные идемпотенты. По лемме 5.25 все идемпотенты $e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_m$ ортогональны f_1, f_2. Получаем, что $1 = e_1 + \ldots + e_{i-1} + f_1 + f_2 + e_{i+1} + \ldots + e_m$ — это разложение единицы в сумму $m+1$ ортогональных идемпотентов. Добавим в нашем дереве вершине e_i две дочерние вершины f_1, f_2.

Таким образом можно построить разложение любой длины $m \in \mathbb{N}$, значит, мы получаем дерево с бесконечным числом вершин. У каждой вершины только две дочерние, поэтому наше дерево локально конечно. По лемме Кёнига можно выбрать бесконечный простой путь, начинающийся в любой вершине, например, в корне дерева. Пусть вершины этого пути соответствуют последовательности идемпотентов $1 = e_0, e_1, e_2, \ldots$.

Построим бесконечное множество ортогональных идемпотентов кольца R. У каждого e_i помимо дочернего идемпотента e_{i+1} есть еще один дочерний идемпотент f_{i+1}. Рассмотрим множество всех $f_1, f_2, \ldots$. Покажем, что каждый f_i ортогонален f_{i+k} для любого $k \in \mathbb{N}$. Действительно, f_i ортогонален e_i по построению. При этом $e_i = f_{i+1} + e_{i+1} = f_{i+1} + f_{i+2} + e_{i+2} = \ldots = f_{i+1} + \ldots + f_{i+k} + e_{i+k}$, и всё это разложения в сумму попарно ортогональных идемпотентов, что проверяется индукцией по k при помощи леммы 5.25. Снова применяя лемму 5.25, получаем, что f_i ортогонален f_{i+k}. Отсюда $\{f_i\}_{i\in\mathbb{N}}$ — это бесконечное ортогональное множество идемпотентов. Мы получаем противоречие с нётеровостью кольца ввиду леммы 5.27.

□

Полусовершенное кольцо может быть описано в терминах систем идемпотентов. Идемпотент $e \in R$ называется *локальным*, если eRe — локальное кольцо. Локальный идемпотент является примитивным, т.к. в локальном кольце нет нетривиальных идемпотентов. Приведем без доказательства следующий результат.

Теорема 5.30 (Мюллер)**.** Кольцо $R \neq 0$ полусовершенно тогда и только тогда, когда 1 может быть представлена в виде суммы конечного числа попарно ортогональных локальных идемпотентов.

Определение 5.31. Кольцо R *конечно по Дедекинду*, если в нём $ab = 1 \Rightarrow ba = 1$.

Очевидно, что каждое коммутативное кольцо конечно по Дедекинду. Ранее мы фактически показали, что каждое локальное кольцо конечно по Дедекинду. Приве-

дем пример кольца, в котором присутствуют элементы обратимые только с одной стороны.

Пример 5.32. Пусть $V = \mathbb{F}^\infty$ — пространство последовательностей $(x_1, x_2, x_3, \ldots)$ элементов поля $\mathbb{F}$, и $R = \operatorname{End} V$. Рассмотрим линейные операторы l, r сдвига координат на одну позицию влево и вправо соответственно: $l(x_1, x_2, \ldots) = (x_2, x_3, \ldots)$, $r(x_1, x_2, \ldots) = (0, x_1, x_2, \ldots)$. Тогда lr тождественно на V, а ядро rl нетривиально.

Теорема 5.33. Если кольцо R нётерово справа, то оно конечно по Дедекинду.

Доказательство. Пусть для некоторых элементов $a, b \in R$ выполнено $ab = 1$. Покажем, что $ba = 1$. Рассмотрим эндоморфизм правых модулей $\phi : R_R \to R_R$, $r \mapsto ar$. Заметим, что ϕ сюръективен: для любого $r \in R$ имеем $r = (ab)r = \phi(br)$. Рассмотрим возрастающую цепочку ядер $\ker\phi \subseteq \ker\phi^2 \subseteq \ldots$. Так как модуль R_R нётеров, то на некотором шаге k выполнено $\ker\phi^k = \ker\phi^{k+1}$. При этом ϕ^k — сюръекция как композиция сюръекций. Покажем, что на самом деле $\ker\phi = 0$. Действительно, если $r \in \ker\phi$, то найдется r' такой, что $r = \phi^k(r')$. Тогда $0 = \phi(r) = \phi^{k+1}(r')$, т.е. $r' \in \ker\phi^{k+1} = \ker\phi^k$, откуда $r = 0$. Итак, $\ker\phi = 0$. В то же время $\phi(ba - 1) = (ab)a - a = a - a = 0$. Значит, $ba - 1 = 0$, что и требовалось. □

Следствие 5.34. Полупростое кольцо конечно по Дедекинду. В частности, кольцо матриц над телом конечно по Дедекинду.

Доказательство. Если модуль R_R полупрост, то он изоморфен прямой сумме неприводимых, а значит, нётеровых модулей. Это сумма конечная, т.к. R_R конечно порожден (порожден единицей). Отсюда модуль R_R нётеров. □

Следствие 5.35. Артиново справа кольцо конечно по Дедекинду.

Доказательство. Артиново справа кольцо всегда нётерово справа. □

Следствие 5.36. Полулокальное кольцо конечно по Дедекинду.

Доказательство. Факторкольцо $R/J(R)$ полупросто, а значит, конечно по Дедекинду. Рассмотрим естественную проекцию $\pi : R \to R/J(R)$. Предположим, что для некоторых $a, b \in R$ выполнено $ab = 1$. Тогда $\pi(a)\pi(b) = \pi(b)\pi(a) = \pi(1)$, откуда $ba = 1 + m$ для некоторого $m \in J(R)$. В силу квазирегулярности радикала Джекобсона элемент $1 + m$ обратим, поэтому $(1 + m)^{-1}ba = 1$. Значит, a обладает и правым, и левым обратным, но они должны совпадать. Отсюда $ab = ba = 1$.

□

Иногда приходится поднимать по модулю идеала не отдельные идемпотенты, а целые семейства ортогональных идемпотентов. Для этого нам понадобится следующая лемма.

Лемма 5.37. Рассмотрим идеал, лежащий в радикале Джекобсона $I \subseteq J(R)$. Предположим, что по модулю I поднимаются идемпотенты. Если $g^2 = g \in R$ и $u^2 - u \in I$ и при этом ug, $gu \in I$, то в R существует такой идемпотент e, что e и g ортогональны, и при этом $e - u \in I$.

Доказательство. Пусть $f \in R$ — результат поднятия u по модулю I. Поскольку $gu, ug \in I$, имеем $gf = g(f-u) + gu \in I$, а также $fg = (f-u)g + ug \in I$. Так как I лежит в $J(R)$, то элемент $1 - fg$ обратим. Рассмотрим $h = (1-fg)^{-1}f(1-fg)$. Он идемпотентен, кроме того, $hg = 0$, поскольку $f(1-fg)g = fg - fg^2 = 0$. Кроме того, $(1-fg)h = f(1-fg)$, то есть $h - f = fgh - fg \in I$, так как $fg \in I$.

Положим $e = (1-g)h$. Тогда $ge = eg = 0$, и в факторкольце R/I выполнено $e+I = (1-g)h+I = (1-g)f+I = f+I = u+I$, так как $h-f$, gf, $f-u \in I$. Покажем, что $e^2 = e$. Заметим, что $f(1-fg)(1-g) = (f-fg)(1-g) = f(1-g)^2 = f(1-g) = (f-f^2g) = f(1-fg)$. Поэтому $e^2 = (1-g)(1-fg)^{-1}[f(1-fg)(1-g)](1-fg)^{-1}f(1-fg) = (1-g)(1-fg)^{-1}[f(1-fg)](1-fg)^{-1}f(1-fg) = e$. □

Теорема 5.38. Рассмотрим идеал, лежащий в радикале Джекобсона $I \subseteq J(R)$. Предположим, что по модулю I поднимаются идемпотенты. Тогда любое конечное или счетное ортогональное множество отличных от нуля идемпотентов факторкольца R/I может быть поднято по модулю I до ортогонального множества отличных от нуля идемпотентов кольца R.

Другими словами, для всякой конечной или счётной системы $u_1, u_2, \ldots$ элементов кольца R, таких что $u_i \notin I$ и $u_iu_j - \delta_{ij}u_i \in I$, существует система $e_1, e_2 \ldots$ элементов кольца R, для которых $e_i - u_i \in I$ и $e_ie_j = \delta_{ij}e_i$, причём все e_i ненулевые.

Доказательство. На шаге индукции при построении e_{n+1} применяем предыдущую лемму к $e_1 + \ldots + e_n$ и u_{n+1}. Тогда e_{n+1}, как было уже доказано, ортогонален всем e_i, $i \leqslant n$. Кроме того, по условию $u_i \notin I$, откуда $e_i = u_i + (e_i - u_i) \notin I$ и не может быть равным нулю. □

Задачи к лекции 6.

Задача 1. Покажите, что в общем случае подкольцо локального кольца не обязательно локально.

Задача 2. Покажите, что если подкольцо S артинового справа локального кольца R артиново справа, то S также локально.

Задача 3. Может ли кольцо многочленов $R[x]$ быть локальным?

Задача 4. Приведите пример группы G и кольца R таких, что групповое кольцо RG локально.

Задача 5. Опишите все идемпотенты, содержащиеся в $J(R)$.

Задача 6. Докажите, что следующие условия на идемпотент e эквивалентны:
1) e централен (т.е. лежит в центре кольца);
2) e коммутирует со всеми нильпотентами;
3) $Re = eR$.

Задача 7. Определите, сколько идемпотентов в кольце $\mathbb{Z}_n$. Опишите их.

Задача 8. Покажите, что если множество всех идемпотентов кольца конечно, то его мощность чётна.

Задача 9. Приведите пример кольца, в котором ровно 6 идемпотентов.

Задача 10. Определите максимальную мощность конечного ортогонального множества примитивных идемпотентов, сумма которых равна 1, в кольце матриц $M_n(\mathbb{F})$ над полем.

6 Чистые и заменяемые кольца

Лекция 7. Чистые и заменяемые кольца

Напомним, что $e \in R$ называется идемпотентом, если $e^2 = e$.

Напомним также, что о подмножестве $I \subseteq R$ говорят, что идемпотенты поднимаются по модулю I, если для каждого $r \in R$ такого, что $r - r^2 \in I$, существует идемпотент e, удовлетворяющий $e - r \in I$.

В этой лекции нас будет интересовать поднятие идемпотентов по модулю односторонних идеалов.

Теорема 6.1. Для кольца R следующие условия эквивалентны:

1) Идемпотенты поднимаются по модулю любого правого идеала.

1') Идемпотенты поднимаются по модулю любого левого идеала.

2) Для каждого $r \in R$ существует идемпотент $e \in R$, такой что $e - r \in (r - r^2)R$;

3) Для каждого $r \in R$ найдутся $c \in R$ и идемпотент $e \in rR$, такие что элемент $(1 - e) - (1 - r)c$ лежит в радикале Джекобсона $J(R)$;

4) Для каждого $r \in R$ существует идемпотент $e \in rR$, такой что выполнено соотношение $R = eR + (1 - r)R$;

5) Для каждого $r \in R$ существует идемпотент $e \in rR$, для которого $1-e \in (1-r)R$.

2')–5') Левые аналоги.

Доказательство. 1) $\Rightarrow$ 2) Частный случай правых идеалов вида $I = (r - r^2)R$.

2) $\Rightarrow$ 1) Если $r - r^2$ лежит в правом идеале I, тогда $e - r \in (r - r^2)R \subseteq I$.

2) $\Rightarrow$ 3) Если $e - r = (r - r^2)q$ для некоторого q, тогда $e = r + r(1 - r)q$, откуда e лежит в правом идеале rR. Вычитая из единицы, выражение для e, имеем $1 - e =$

$1-r-(1-r)rq=(1-r)(1-rq)$. Полагая $c=1-rq$, получаем, что указанная в пункте 2) разность просто равна нулю, а значит, лежит в радикале.

3) $\Rightarrow$ 4) Из пункта 2) замечаем, что элемент $e+(1-r)c$ лежит в $1+J(R)$, а потому обратим ввиду квазирегулярности радикала. В частности, этот элемент обратим справа, откуда правый идеал $eR+(1-r)R$ содержит единицу.

4) $\Rightarrow$ 5) По пункту 3) найдутся такие элементы $s,t\in R$, что будет выполнено $1=et+(1-r)s$. Тогда положим $f=e+et(1-e)$. Заметим, что элемент f является идемпотентом. Далее вычтем друг из друга выражения для 1 и для f, тогда после сокращения слагаемых et получим $1-f=(1-r)s+ete-e=(1-r)s+(et-1)e$. Теперь перепишем выражение для 1 в виде $et-1=-(1-r)s$. Подставляя это в формулу для $1-f$ окончательно получаем $1-f=(1-r)s(1-e)$, а значит, $1-f$ лежит в правом идеале $(1-r)R$. Поэтому f — искомый идемпотент.

5) $\Rightarrow$ 2) В разности $e-r$ прибавим и отнимем re, затем, группируя слагаемые, получим $e-r=(1-r)e-r(1-e)$. Ввиду пункта 4) найдутся такие элементы q_1,q_2, что $e=rq_1$, $1-e=(1-r)q_2$. Подставляя это в выражение для $e-r$, получаем $e-r=(1-r)rq_1-r(1-r)q_2=(r-r^2)(q_1-q_2)$, откуда разность $e-r$ лежит в правом идеале $(r-r^2)R$.

1') $\Leftrightarrow$ 2') $\Rightarrow$ 3') $\Rightarrow$ 4') $\Rightarrow$ 5') $\Rightarrow$ 2') Симметрично

5) $\Rightarrow$ 5') Положим $b=1-a$, $f=1-e$. Требуется отыскать такой идемпотент e', что $1-e'\in R(1-a)=Rb$. По условию $e\in aR$, $f\in bR$, то есть найдутся такие $r,s\in R$, что $e=ar$, $f=bs$. При необходимости заменяя r на re и s на sf, можно считать, что выполнено $rar=r$, $rbs=0$, $sbs=s$, $sar=0$. Положим

$$r'=1-sb+rb,\ s'=1-ra+sa,\ e'=r'a\in Ra,\ f'=s'b\in Rb.$$

Отсюда получаем, что $r's=s'r=0$. Далее в силу того, что $ar+bs=e+f=1$, имеем $ar'=a(1-sb)+arb=a(1-sb)+(1-bs)b=a(1-sb)+b(1-sb)=(a+b)(1-sb)=1-sb$. Это означает, что $r'ar'=r'$. Аналогично проверяется, что $bs'=1-ra$, $s'bs'=s'$. Тогда элементы e',f' оказываются идемпотентами. Более того, в силу $ab=ba$, получаем $e'+f'=r'a+s'b=(a-sba+rba)+(b-rab+sab)=a+b=1$. Другими словами, $1-e'=f'\in Rb$, что и требовалось.

5') $\Rightarrow$ 5) Достаточно в предыдущем доказательстве каждое встречающееся произведение элементов кольца $r_1\cdot\ldots\cdot r_n$ переписать в обратном порядке $r_n\cdot\ldots\cdot r_1$. $\square$

Условие 5) бывает удобно переформулировать следующим образом: для любых двух элементов $r,s\in R$, таких что $r+s=1$, найдутся идемпотенты $e\in rR$, $f\in sR$, у которых также $e+f=1$.

Определение 6.2. Кольцо в котором идемпотенты поднимаются по модулю любого правого (эквивалентно, левого) идеала будем называть *заменяемым*[6].

[6]В англоязычной литературе — exchange ring.

Предложение 6.3. Если R — заменяемое кольцо, то для любого идемпотента $e \in R$ кольцо eRe также является заменямым.

Доказательство. Единица кольца eRe — это e. Пусть $r \in eRe$, $f \in rR \subseteq eR$ — идемпотент, для которого $1 - f \in (1 - r)R$. Тогда $ef = f$, и для элемента $g = fe$ имеем $g = g^2 = eg^2 \in r(eRe)$, $e - g = e(1 - f)e \in (e - r)eRe$. □

Далее мы введем понятие конечно-заменяемого модуля. Начнем с примера.

Пусть X — конечномерное векторное пространство над полем $\mathbb{F}$. Предположим, что оно разложено в прямую сумму подпространств какими-нибудь двумя способами $X = M \oplus Y = N_1 \oplus N_2$. Выберем в подпространстве M базис $\{e_1, \ldots, e_m\}$. Также пусть $\{f_{1,1}, \ldots, f_{1,k_1}\}$, $\{f_{2,1}, \ldots, f_{2,k_2}\}$ — базисы пространств N_1, N_2, соответственно. Расширим линейно независимую систему $\{e_i\}_{i=1}^m$ за счет векторов $f_{i,j}$. По очереди будем рассматривать все вектора $f_{i,j}$: если $f_{i,j}$ не выражается линейно через $\{e_i\}_{i=1}^m$ и векторы, добавленные на предыдущем шаге, то добавляем $f_{i,j}$ в нашу систему. По окончании этой процедуры мы построим базис всего пространства X, составленный из всех векторов e_i и каких-то векторов $f_{i,j}$. Среди них выберем все $f_{i,j}$ с индексом $i = 1$, возьмем их линейную оболочку и получим некоторое подпространство $N_1' \subseteq N_1$ (если таких $f_{i,j}$ нет, то $N_1' = 0$). Аналогично строим подпространство $N_2' \subseteq N_2$. Поэтому получаем $X = M \oplus N_1' \oplus N_2'$, где $N_1' \subseteq N_1$, $N_2' \subseteq N_2$. Таким образом у пространства M мы *заменили* дополнительное к нему пространство Y на сумму двух N_1', N_2' лежащих в N_1, N_2, соответственно.

Рассмотрим класс модулей, обладающих аналогичным свойством.

Определение 6.4. Правый R-модуль M называется *конечно заменяемым*[7], если для любого правого R-модуля X, представимого в виде (внутренней) прямой суммы подмодулей двумя способами $X = M' \oplus Y = N_1 \oplus N_2$, где $M' \cong M$, найдутся подмодули $N_1' \subseteq N_1$, $N_2' \subseteq N_2$, такие что $X = M' \oplus (N_1' \oplus N_2')$.

В определении вместо двух N_i можно взять произвольное конечное число. На самом деле тогда получится эквиалентное определение, но мы это доказывать не будем.

Замечание 6.5. Пусть $e^2 = e \in Rr$, тогда существует элемент f, для которого $e = fr$ и $ef = f$. Симметричное утверждение для идемпотента из правого идеала также верно.

Доказательство. Если $e = sr$, то рассмотрим $f = srs$. Тогда $fr = (sr)^2 = e^2 = e$, $ef = (sr)^2 s = srs = f$. □

Теорема 6.6 (Николсон, 1977)**.** Правый R-модуль M конечно заменяемый тогда и только тогда, когда его кольцо эндоморфизмов $\operatorname{End} M_R$ является заменямым.

[7] В англоязычной литературе — modules with the finite exchange property.

Доказательство достаточности разбивается на две части. В первой части мы сконструируем модули N_1', N_2' из определения конечно заменяемого модуля. Во второй части мы покажем, что действительно выполняется $X = M \oplus N_1' \oplus N_2'$.

Доказательство достаточности. [*Часть 1.*] Пусть $\operatorname{End} M$ — заменямое кольцо. Для произвольного правого R-модуля X обозначим $E = \operatorname{End} X$ и предположим, что даны два разложения во внутреннюю прямую сумму $X = M \oplus Y = N_1 \oplus N_2$. Выберем идемпотент $p \in E$ такой, что $M = p(X)$, откуда $\operatorname{End} M = pEp$. Далее найдем два идемпотента $t_1, t_2 \in E$ таких, что $t_1 t_2 = t_2 t_1 = 0$, также $t_1 + t_2 = 1$ и выполнено

$$t_1(X) = N_1,\ t_2(X) = N_2,\ \ker t_1 = N_2,\ \ker t_2 = N_1.$$

Запишем $p = p \cdot 1 \cdot p = pt_1p + pt_2p$. Применим пункт 5') предыдущей теоремы к элементу pt_1p в кольце $\operatorname{End} M = pEp$, учтем, что p — единица этого кольца. Тогда можно выбрать идемпотент v_1, лежащий в левом идеале $pEp(pt_1p) = pEp(t_1p)$, причём идемпотент $v_2 = p - v_1$ будет принадлежать $pEp(p - pt_1p) = pEp(t_2p)$. Значит, найдутся такие элементы $a_1, a_2 \in pEp$, что выполняется $v_i = a_i t_i p$, $i = 1, 2$. В силу замечания выше можно считать, что заведомо $v_i a_i = a_i$.

Положим $h_i = t_i a_i t_i$, $i = 1, 2$. Покажем, что оба h_i являются идемпотентами. Так как $a_i \in pEp$, то $a_i = pa_i$. Поэтому $h_i^2 = (t_i a_i t_i)(t_i p a_i t_i) = t_i(a_i t_i p)a_i t_i = t_i(v_i a_i)t_i = t_i a_i t_i = h_i$. Кроме того, h_1, h_2 ортогональны, т.к. t_1, t_2 ортогональны.

Заметим, что $h_i(X) \subseteq N_i$ в силу $t_i(X) = N_i$, $i = 1, 2$. Обозначим $N_i' = \ker h_i \cap N_i$. Тогда любой элемент $n \in N_i$ представим в виде $n = h_i(n) + (1 - h_i)(n)$, где второе слагаемое лежит в N_i'. Поэтому $N_i = h_i(X) + N_i'$, причем эта сумма прямая, т.к. $N_i' \subseteq \ker h_i$. Возвращаясь к исходному разложению модуля X, получаем $X = N_1 \oplus N_2 = (h_1(X) \oplus N_1') \oplus (h_2(X) \oplus N_2')$, откуда $X = (h_1(X) \oplus h_2(X)) \oplus (N_1' \oplus N_2')$.

[*Часть 2*] Наша цель — доказать, что $X = M \oplus N_1' \oplus N_2'$. Сначала покажем, что сумма модулей M и $N_1' \oplus N_2'$ прямая. Пусть $x \in M \cap (N_1' \oplus N_2')$. Проверим, что $h_1(x) = 0$. Запишем $x = n_1' + n_2'$, где $n_i' \in N_i'$, $i = 1, 2$. Тогда $h_1(x) = h_1(n_2')$ ввиду $N_1' \subseteq \ker h_1$. Распишем h_1 в правой части равенства по определению: $h_1(x) = (t_1 a_1 t_1)(n_2')$, однако $n_2' \in N_2' \subseteq N_2 = \ker t_1$ согласно определению t_1. Поэтому $h_1(x) = 0$, аналогично проверяется, что $h_2(x) = 0$. Так как $x \in M$, то по определению p имеем $x = p(x)$. Перепишем в виде $x = v_1(x) + v_2(x)$. При этом $v_i = v_i v_i = (a_i t_i p)(a_i t_i p) = a_i t_i (p a_i) t_i p = a_i (t_i a_i t_i) p = a_i h_i p$, где мы учли, что $a_i \in pEp$. Тогда $x = (a_1 h_1 p)(x) + (a_2 h_2 p)(x) = (a_1 h_1)(x) + (a_2 h_2)(x) = 0$ ввиду $h_1(x) = h_2(x) = 0$.

Мы показали, что сумма $M \oplus (N_1' \oplus N_2')$ прямая. Осталось проверить, что она совпадает со всем X. Выберем произвольный $x \in X$. Ввиду разложения $X = (h_1(X) \oplus h_2(X)) \oplus (N_1' \oplus N_2')$ можно записать $x = x_1 + x_2 + w$, где $x_i = h_i(y_i)$ для некоторых $y_i \in X$, $i = 1, 2$, а также $w \in N_1' \oplus N_2'$. Рассмотрим элементы $x_i - a_i(x_i)$, $i = 1, 2$. Докажем, что они на самом деле лежат в $N_1' \oplus N_2'$. Учитывая, что $a_1, a_2 \in pEp$, вычислим

$$h_j a_i h_i = (t_j a_j t_j) a_i (t_i a_i t_i) = t_j (a_j t_j p)(a_i t_i p) a_i t_i = t_j (v_j v_i) a_i t_i = \delta_{ij} t_j a_i t_i = \delta_{ij} h_i,$$

где $i, j \in \{1, 2\}$, символ Кронеккера $\delta_{ij} = 1$ при $i = j$, и $\delta_{ij} = 0$ при $i \neq j$. Тогда

$$h_j(x_i - a_i(x_i)) = (h_j h_i)(y_i) - (h_j a_i h_i)(y_i) = \delta_{ij}(y_i) - \delta_{ij}(y_i) = 0.$$

Принимая во внимание разложение $X = (h_1(X) \oplus h_2(X)) \oplus (N_1' \oplus N_2')$, можно расписать $x_i - a_i(x_i) = h_1(z_{i,1}) + h_2(z_{i,2}) + n_{i,1}' + n_{i,2}'$. Применим h_1 к обеим частям равенства. Учитывая, что $h_1^2 = h_1$, элементы h_1, h_2 ортогональны, при этом $N_1' \subseteq \ker h_1$ и, более того, $N_2' \subseteq N_2 = \ker t_1 \subseteq \ker t_1 a_1 t_1 = \ker h_1$, мы получаем, что выполнено $h_1(x_i - a_i(x_i)) = h_1(z_{i,1})$. С другой стороны, $h_1(x_i - a_i(x_i))$ равно нулю, как мы уже показали ранее. Итак, $h_1(z_{i,1}) = 0$, аналогично $h_2(z_{i,1}) = 0$. Таким образом $x_i - a_i(x_i) \in N_1' \oplus N_2'$, $i = 1, 2$.

Наконец, возвращаясь к элементу $x \in X$, мы можем записать $x = x_1 + x_2 + w = a_1(x_1) + a_2(x_2) + (x_1 - a_1(x_1)) + (x_2 - a_2(x_2)) + w$. В этом разложении первые два слагаемых лежат в M в силу того, что $a_1, a_2 \in pEp$, остальные слагаемые попадают в $N_1' \oplus N_2'$, как было показано выше. В силу произвольности $x \in X$ получаем, что $X = M \oplus N_1' \oplus N_2'$, и это завершает доказательство достаточности. $\square$

Доказательство необходимости. Пусть M — конечно заменямый правый R-модуль, покажем, что для $S = \operatorname{End} M$ выполнен пункт 5) из теоремы о поднятии идемпотентов по модулю односторонних идеалов. Выберем произвольный $a \in S$, требуется найти идемпотент $e \in aS$ такой, что $1 - e \in (1 - a)S$. Обозначим $b = 1 - a$.

Положим $X = M \oplus M$. Рассмотрим в X подмодули проекций на каждую координату $N_1 = \{(m, 0) \mid m \in M\}$, $N_2 = \{(0, m) \mid m \in M\}$, а также диагональный подмодуль $D = \{(m, m) \mid m \in M\}$.

Зададим в X подмодуль $M' = \{(a(m), -b(m)) \mid m \in M\}$. Заметим, что отображение $m \mapsto (a(m), -b(m))$ задаёт изоморфизм модулей. Действительно, оно гоморфизм, т.к. a, b — эндоморфизмы. Сюръективность вытекает из определения M'. Если же $a(m) = -b(m) = 0$, то $m = (a + b)(m) = 0$. Итак, $M' \cong M$.

Покажем, что X раскладывается во внутреннюю прямую сумму подмодулей M' и D. Возьмём произвольный $(x, y) \in X$. Положим $u = x - y$ и $v = b(x) + a(y)$. Заметим, что тогда $(a(u), -b(u)) + (v, v) = (a(x) - a(y) + b(x) + a(y), b(y) - b(x) + b(x) + a(y)) = ((a + b)(x), (a + b)(y)) = (x, y)$. Отсюда $M' + D = X$. Если $(x, y) \in M' \cap D$, тогда $a(x) = -b(x)$, а значит, $0 = (a + b)(x) = x$ и $y = -b(x) = 0$.

Получаем два разложения $X = M' \oplus D = N_1 \oplus N_2$, где $M' \cong M$. Воспользуемся тем, что M конечно заменяемый: найдутся подмодули $N_1' \subseteq N_1$, $N_2' \subseteq N_2$ такие, что $X = M' \oplus N_1' \oplus N_2'$. Тогда для каждого $m \in M$ существует единственное разложение вида

$$(m, m) = (a(u), -b(u)) + (m_1, 0) + (0, m_2),$$

где $(m_1, 0) \in N_1'$, $(0, m_2) \in N_2'$. Определим эндоморфизмы $a', b' \in \operatorname{End} M$ по правилу $a'(m) = m_2$, $b'(m) = m_1$. Определение корректно, т.к. сумма $M' \oplus N_1' \oplus N_2'$ прямая.

В силу $a + b = 1$ получаем, что для любого $m \in M$ выполнено $(aa')(m) = (-ba')(m) + a'(m)$. По той же причине $(bb')(m) = (-ab')(m) + b'(m)$. При помощи этих соотношений покоординатно проверяются тождества

$$(aa'(m), aa'(m)) = (aa'(m), -ba'(m)) + (0,0) + (0, a'(m)),$$
$$(bb'(m), bb'(m)) = (-ab'(m), bb'(m)) + (b'(m), 0) + (0,0).$$

Тогда по определению a' получаем из первого тождества, что $a'(aa'(m)) = a'(m)$ для всех $m \in M$, откуда $a'aa' = a'$. Аналогично из второго тождества получаем, что $b'bb' = b'$.

Положим $e = aa'$, $f = bb'$. В силу предыдущих соотношений получаем, что $e^2 = a(a'aa') = aa' = e$ и аналогично $f^2 = f$. Покажем, что $e + f = 1$. Для этого вернёмся к тождеству $(m, m) = (a(u), -b(u)) + (m_1, 0) + (0, m_2)$, где $a'(m) = m_2$, $b'(m) = m_1$. Рассмотрим равенство покоординатно: $m = a(u) + b'(m)$, $m = -b(u) + a'(m)$. Вычитая из первого второе и учитывая, что $a + b = 1$, получаем $u = (a' - b')(m)$. Подставим выражение для u в первое равенство: $m = a(a'(m) - b'(m)) + b'(m) = (aa' - ab' + b')(m) = (aa' - (1-b)b' + b')(m) = (aa' + bb')(m)$. Итак, для любого $m \in M$ выполнено $m = (aa' + bb')(m)$, т.е. $aa' + bb' = 1$. Другими словами, $e + f = 1$. Мы нашли идемпотент $e = aa' \in aS$ такой, что $1 - e = f = bb' \in (1-a)S$, необходимость доказана.

□

Следствие 6.7 (О заменяемом кольце)**.** Для кольца R следующие условия эквивалентны:

1) Идемпотенты поднимаются по модулю любого правого идеала.

2) R_R — конечно заменяемый правый R-модуль.

3) Для каждого $r \in R$ найдется идемпотент $e \in rR$, такой что $(1 - e) \in (1 - r)R$.

1')–3') Левые аналоги.

Доказательство. Объединим все предыдущие результаты и учтем $\operatorname{End} R_R \cong R$. □

Определение 6.8. Элемент кольца называется *чистым*, если он представим в виде суммы идемпотента и обратимого элемента. Кольцо *чистое*, если все его элементы чистые. Модуль M *чист*, если $\operatorname{End} M$ — чистое кольцо.

Предложение 6.9. Локальное кольцо R чистое.

Доказательство. Обратимый элемент $u \in R$ представим в виде $0 + u$. Необратимый u обязан лежать в $J(R)$ из-за локальности R и равен $1 + (u - 1)$, причём $u - 1$ обратим в силу квазирегулярности радикала Джекобсона. □

Пример 6.10. $\mathbb{Z}$ не является чистым кольцом, поскольку все его идемпотенты и все его обратимые элементы — это 0 и ± 1.

Предложение 6.11. Чистые кольца являются заменямыми.

Доказательство. Пусть R чистое, $r = e+u$, тогда $(r-u(1-e)u^{-1})u = eu+u^2-u+ue$, что равно $(e+u)^2 - e - u = r^2 - r$. □

Определение 6.12. Кольцо R называется *абелевым*, или *нормальным*, если все его идемпотенты лежат в центре.

Предложение 6.13. Для абелева кольца R следующие условия эквивалентны:
1) R чистое,
2) R заменяемое.

Доказательство. Если $x \in R$ и $e^2 = e \in rR$, то для f из предложения выше $frf = f$, то есть элементы fr, rf также идемпотентны. Из центральности $fr = f(rf)r = (rf)(fr) = r(fr)f = rf$. Тогда $e = rf = fr$, $fe = f$.

Аналогично f строим элемент g, для которого $g(1-e) = g$ и $(1-r)g = 1-e = g(1-r)$. Тогда $f-g$ — обратный элемент к $r-(1-e)$: $(r-1+e)(f-g) = rf - f + ef - rg + g - eg = e - (1-e)f + (1-e) - eg =$ (из центральности e и $1-e$) $= 1 + f(1-e) - ge = 1 + fe(1-e) - g(1-e)e = 1$, произведение в другом порядке проверяется аналогично. □

Пусть $1 = e_1 + \ldots + e_n$ — разложение в сумму ортогональных идемпотентов единицы кольца R, а $R = e_1R \oplus \ldots \oplus e_nR$ — ему соответствующее разложение R в прямую сумму правых идеалов.

Пусть $r \in R$, тогда $r = 1 \cdot r \cdot 1 = \sum\limits_{i,j=1}^{n} e_i r e_j$, и $R = \bigoplus\limits_{i,j=1}^{n} e_i R e_j$ (прямая сумма абелевых групп).

Тогда элемент $r \in R$ удобно записывать в виде матрицы

$$r = \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix},$$

где $r_{ij} = e_i r e_j$. Иначе говоря,

$$R \cong \begin{pmatrix} R_{11} & \cdots & R_{1n} \\ \vdots & \ddots & \vdots \\ R_{n1} & \cdots & R_{nn} \end{pmatrix},$$

где $R_{ij} = e_i R e_j$ (*двустороннее пирсовское разложение* кольца R).

Элементы $e_i R e_j$ соответствуют гомоморфизмам абелевых групп $e_j R \to e_i R$.

Разложение кольца в конечное прямое произведение соответствует разложению его единицы в сумму центральных ортогональных идемпотентов.

Лемма 6.14. Пусть $e \in R$ — идемпотент, для которого eRe и $(1-e)R(1-e)$ — чистые кольца. Тогда R также чистое.

Доказательство. Для краткости введём обозначение $\overline{r} = 1 - r$.

Пусть $M = \begin{pmatrix} a & x \\ y & b \end{pmatrix} \in \begin{pmatrix} eRe & eR\overline{e} \\ \overline{e}Re & \overline{e}R\overline{e} \end{pmatrix} = R$. По условию $a = f + u$, $f, u \in eRe$, где f — идемпотент, u имеет обратный в кольце eRe элемент u_1. Заметим, что $b - yu_1x \in \overline{e}R\overline{e}$. Поэтому можно записать $b - yu_1x = g + v$, g — идемпотент, v имеет обратный элемент v_1 в $\overline{e}R\overline{e}$.

Тогда $M = \begin{pmatrix} f + u & x \\ y & g + v + yu_1x \end{pmatrix}$. Остаётся доказать, что $\begin{pmatrix} u & x \\ y & v + yu_1x \end{pmatrix}$ обратим в R. Но эта матрица приводится к виду $\operatorname{diag}(u, v)$ следующими "элементарными преобразованиями":

$$\begin{pmatrix} e & 0 \\ -yu_1 & \overline{e} \end{pmatrix} \begin{pmatrix} u & x \\ y & v + yu_1x \end{pmatrix} \begin{pmatrix} e & -u_1x \\ 0 & \overline{e} \end{pmatrix} = \begin{pmatrix} u & x \\ 0 & v \end{pmatrix} \begin{pmatrix} e & -u_1x \\ 0 & \overline{e} \end{pmatrix} = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}. \qquad \square$$

Следствие 6.15. Если в кольце R выполнено $1 = \sum\limits_{i=1}^{n} e_i$, где e_i — ортогональные идемпотенты, и все e_iRe_i — чистые кольца, то R также чистое.

Следствие 6.16. Если R чистое, то и $M_n(R)$ чистое.

Следствие 6.17. Если $M = \bigoplus\limits_{i=1}^{n} M_i$ — модули и все $\operatorname{End} M_i$ чистые, то и $\operatorname{End} M$ чистое.

Определение 6.18. Кольцо R *потентное* (potent), если всякий его правый идеал, не содержащийся в радикале Джекобсона, содержит ненулевой идемпотент.

Предложение 6.19. Чистое кольцо потентно.

Доказательство. Пусть aR не содержит ненулевых идемпотентов. Для $r \in R$ запишем $ar = e + u$ по определению чистого кольца, тогда идемпотент $u(1 - e)u^{-1} = (ar - e)(1 - e)u^{-1} = ar(1 - e)u^{-1}$ лежит в aR, то есть $e = 1$. Получаем, что $1 - ar$ обратим для всех $r \in R$, то есть $aR \subseteq J(R)$. $\square$

Определение 6.20. Идемпотент $e \in R$ *локален*, если eRe — локальное кольцо.

Локальный идемпотент примитивен.

Предложение 6.21. Примитивный идемпотент чистого кольца локален.

Доказательство. Пусть $f \in R$ — примитивный идемпотент, $a \in fRf \setminus J(fRf) = J(R) \cap fRf$.

Так как R потентно, в aR (а следовательно, и fR) есть идемпотент $g \neq 0$; из примитивности f следует $gR = fR = aR$. Если $f = ab$, то в fRf элемент fbf — правый обратный к a: $afbf = abf = f^2 = f$, и поэтому fbf не может лежать в $J(fRf)$. Применяя те же рассуждения к элементу fbf, получаем, что fbf и faf обратимы в fRf, откуда fRf локально. $\square$

Определение 6.22. Кольцо *ортогонально конечное*, если в нём нет бесконечных систем ортогональных идемпотентов.

Пример не ортогонально конечного кольца — $\operatorname{End}\mathbb{F}^\infty$: диагональные матричные единицы образуют счётную ортогональную систему идемпотентов.

Следствие 6.23. Кольцо R полусовершенно тогда и только тогда, когда оно чисто и ортогонально конечно.

Доказательство. Если R полусовершенно, то по теореме Мюллера $1 = \sum\limits_{i=1}^{n} e_i$, где e_i — конечная система локальных ортогональных идемпотентов, поэтому e_iRe_i — локальные кольца, они чистые, откуда и R чисто.

Если R чистое и ортогонально конечное, то $1 = \sum\limits_{i=1}^{n} e_i$, где e_i — примитивные ортогональные идемпотенты. Кольца e_iRe_i локальны по предложению выше, поэтому снова по теореме Мюллера R полусовершенно. □

Следствие 6.24. Всякое артиново справа кольцо чистое.

Определение 6.25. Элемент $r \in R$ *однозначно чист*, если его представление в виде суммы идемпотента и обратимого элемента существует и единственно.

Однозначно чистое кольцо — такое, все элементы которого однозначно чистые.

Определение 6.26. Элемент $r \in R$ *строго чист*, если его можно представить в виде суммы коммутирующих идемпотента и обратимого элемента.

Строго чистое кольцо — такое, все элементы которого строго чистые.

Предложение 6.27. Локальное кольцо R строго чистое. Обратно, если в строго чистом кольце R ровно 2 идемпотента, то оно локально.

Доказательство. Следует из доказательства предложения 6.9.

В обратную сторону, произвольный элемент $a \in R$ строго чист, и его разложение либо имеет вид $a = 0 + u$, тогда a — обратимый, либо $a = 1 + u = 1 - (-u)$ и $1 - a = -u$ — обратимый. Выполнен п. 9 из эквивалентных определений локального кольца. □

Предложение 6.28. Центральные идемпотенты и центральные нильпотенты любого кольца однозначно чисты.

Доказательство. Пусть $e^2 = e$ централен. Тогда имеем $e = (1 - e) + (2e - 1)$, при этом $(2e-1)^2 = 4e^2 - 4e + 1 = 1$; пусть $e = f + u$, $f^2 = f$, u обратим, тогда из $eu = ue$ следует $fu = uf$ и $(f + u)^2 = f + 2fu + u^2 = f + u$, то есть $u = 1 - 2f$ и $f = 1 - e$.

Для нильпотента a, $a^n = 0$, имеем $a = 1 + (a - 1)$. Пусть $a = e + u$ — разложение a как чистого элемента. Тогда имеем $0 = (e + u)^n = e(\sum\limits_{i=0}^{n-1} a_iu^i) + u^n$, $a_i \in \mathbb{Z}$ — биномиальные коэффициенты, то есть обратимый элемент u^n лежит в eR, что возможно только при $e = 1$. □

Для нецентральных элементов эта формулировка неверна: в $M_2(R)$ выполнено $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) + \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&1\\0&1\end{smallmatrix}\right) + \left(\begin{smallmatrix}1&-1\\0&-1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) + \left(\begin{smallmatrix}-1&1\\0&-1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right) + \left(\begin{smallmatrix}-1&1\\-1&0\end{smallmatrix}\right)$.

Прямое произведение колец однозначно (соответственно, строго) чисто тогда и только тогда, когда однозначно (соответственно, строго) чисты все сомножители.

Лемма 6.29. Всякий идемпотент однозначно чистого кольца централен.

Доказательство. Пусть $e^2 = e \in R$. Для произвольного $r \in R$, как было установлено ранее, элемент $e + er(1-e)$ также идемпотентен, а элементы $1 \pm er(1-e)$ взаимно обратные. Тогда из $(e + er(1-e)) + 1 = e + (1 + er(1-e))$ по условию следует, что $er(1-e) = 0$, то есть $er = ere$. Аналогично получаем $re = ere$. □

Следствие 6.30. Если R однозначно чистое и $e^2 = e \in R$, то eRe однозначно чистое.

Следствие 6.31. Нетривиальные матричные кольца и кольца треугольных матриц не могут быть однозначно чистыми.

Следствие 6.32. Однозначно чистое кольцо конечно по Дедекинду.

Доказательство. Если $ab = 1$, то ba — идемпотент и $ba = ba^2b = (ab)^2 = 1$. □

Лемма 6.33. Кольцо R локально тогда и только тогда, когда оно чисто и не содержит нетривиальных идемпотентов.

Доказательство. Для локального кольца утверждение доказано ранее. Пусть R чистое и $a \in R \setminus J(R)$. Тогда для некоторого $r \in R$ элемент $1 - ar$ необратим, то есть $1 - ar = 0 + u$ невозможно, поэтому $(-ar)$ обратим, и a обратим справа; аналогично устанавливаем его обратимость слева. Поэтому в R нет необратимых элементов вне радикала Джекобсона, то есть R локально. □

Теорема 6.34. Следующие условия на кольцо R эквивалентны:

1) R локально и однозначно чисто;

2) R однозначно чисто и не имеет нетривиальных идемпотентов;

3) $R/J(R) \cong \mathbb{Z}/(2)$.

Доказательство. 1) $\Rightarrow$ 2): очевидно.

2) $\Rightarrow$ 3): пусть $\overline{R} = R/J(R)$ и $a \neq 0 \in \overline{R}$. Так как R локально, $\overline{R}$ — тело, и тогда либо $a = 1$, либо a, $1 - a$ — обратимые элементы $\overline{R}$. Но во втором случае $0 + (1 - a) = 1 + (-a)$.

3) $\Rightarrow$ 1): R локально и поэтому чисто. Пусть $e+u = f+v$ — два чистых разложения некоторого элемента R, тогда без ограничения общности $e = 0$, $f = 1$. Отсюда u и $v = 1 - u$ обратимы в R, но тогда среди их образов в $R/J(R)$ должен быть 0. □

Следствие 6.35. Ортогонально конечное однозначно чистое кольцо R изоморфно $R_1 \times \ldots \times R_n$, где $R_i/J(R_i) \cong \mathbb{Z}_2$.

Доказательство. По условию $R = R_1 \times \dots R_n$, где R_i — прямо неразложимые кольца, и им соответствуют центральные идемпотенты e_i ($R_i = e_i R e_i$). При этом все $e_i R e_i$ однозначно чисты, так как однозначно чисто их прямое произведение. По теореме $R_i/J(R_i) \cong \mathbb{Z}_2$. Напротив, во всяком прямое произведение такого вида сомножители локальны и однозначно чисты, поэтому в их произведении есть только 2^n идемпотентов (из которых ортогональную систему образуют только n ненулевых) и выполнена однозначная чистота. □

Напомним, что в чистом кольце идемпотенты поднимаются по модулю каждого правого идеала I: если $r = e + u$, $r^2 - r \in I$, тогда $(r - u(1-e)u^{-1})u = r^2 - r$, то есть "идемпотент по модулю I" r поднимается до (настоящего) идемпотента $u(1-e)u^{-1}$.

Лемма 6.36. Пусть R чисто. Если I — правый идеал, не содержащийся в $J(R)$, то в I есть ненулевой идемпотент.

Доказательство. Предположим противное. Если $r \in I$, то идемпотент $u(1-e)u^{-1} = r - (r^2 - r)u^{-1} \in I$ нулевой, то есть $e = 1$. Отсюда каждый элемент множества $1 - I$ обратим, то есть $I \subseteq J(R)$. □

Определение 6.37. *Характеристика* $\operatorname{char} R$ кольца R — наименьшее натуральное число, равное нулю в R, либо 0, если такого числа не существует.

В кольце характеристики $n \geqslant 0$ единица по сложению образует абелеву подгруппу, изоморфную $\mathbb{Z}/(n)$.

Характеристика тела — простое число.

Лемма 6.38. Пусть R однозначно чистое. Тогда $R/J(R)$ имеет характеристику 2.

Доказательство. Предположим противное: пусть правый идеал $2R$ не содержится в $J(R)$. Тогда в нём есть ненулевой идемпотент e, то есть $e = 2r$, и $er = re$. Без ограничения общности $er = r$, поскольку при уже найденном r для элемента $s = er = 2r^2$ выполнено $es = e^2 r = er = s$.

Тогда $u = (1-e) - 2e$ — обратимый элемент с обратным $(1-e) - r$: их произведение равно $1 - e - r - 3e + 3e^2 + 3re = 1 - 4e + 3e^2 + 2re = 1$. Так как $1 + u = (1-e) + (1-2e)$ ($(1-2e)^2 = 1$), из однозначной чистоты получаем $e = 0$, что противоречит построению e. □

Определение 6.39. *R булево*, если все его элементы идемпотентны.

Булево кольцо соответствует ограниченной дистрибутивной решётке (*булевой алгебре*) с операциями $r \vee s = r + s + rs$; $\neg r = 1 - r$; $r \wedge s = rs$. Пример булева кольца — *булеан* 2^S (множество всех подмножеств) конечного множества S с операциями $+ = \triangle$ (симметрическая разность) и $\cdot = \cap$; $0 = \varnothing$, $1 = S$.

Следующие результаты о связи булевых и однозначно чистых колец пориведём без доказательства.

Теорема 6.40. Следующие условия на кольцо R эквивалентны:

1) R однозначно чисто, $J(R) = 0$;

2) R чисто, $\operatorname{char} R = 2$, единственный обратимый элемент R — единица;

3) R булево;

4) R регулярно по фон Нейману (всякий элемент $a \in R$ обладает псевдообратным x, для которого $axa = a$) и однозначно чисто.

Теорема 6.41. Следующие условия на кольцо R эквивалентны:

1) R однозначно чисто;

2) $R/J(R)$ булево, идемпотенты однозначно поднимаются по модулю $J(R)$;

3) $R/J(R)$ булево, идемпотенты центральны и поднимаются по модулю $J(R)$;

4) для всех $r \in R$ существует единственный идемпотент $e \in R$ такой, что $e - a \in J(R)$.

Пример 6.42. Пусть $R = \left(\begin{smallmatrix} \mathbb{Z}_2 & \mathbb{Z}_2 \\ 0 & \mathbb{Z}_2 \end{smallmatrix}\right)$. Тогда $R/J(R) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ булево, и идемпотенты поднимаются по модулю $J(R)$, но они не центральны, поэтому R не однозначно чисто.

Мы говорили о чистых кольцах, где элеметы раскладываются в суммы идемпотентов и обратимых элементов.

Есть много близких классов колец.

Например, (строго) ниль-чистые: рассматриваются разложения в суммы (коммутирующих) идемпотента и нильпотента.

Далее вместо идемпотентов можно рассматривать k-потенты:

Определение 6.43. Элемент r из кольца R называется *k-потентным*, если выполнено равенство $r^k = r$.

Кольцо R назовем (строго) k-ниль-чистым, если каждый элемент из R представим в виде суммы (коммутирующих) k-потента и нильпотента.

Задачи к лекции 7.

Задача 1. Приведите пример кольца, которое не является заменяемым.

Задача 2. Пусть M— конечно-заменяемый модуль. Покажите, что если подмоуль $N \leqslant M$ выделяется прямым слагаемым, то он также конечно-заменяемый.

Задача 3. Пусть $f = \sum\limits_{i=0}^{n} f_i x^i$ — элемент $R[x]$, где R — коммутативное кольцо. Доказать, что:

1) f обратим $\Leftrightarrow$ f_0 обратим, а остальные коэффициенты нильпотентны (для $fg = 1$ доказать индуктивно, что $f_n^{k+1} g_{m-k} = 0$);

2) f — делитель нуля $\Leftrightarrow$ в R существует элемент r, для которого $fr = 0$ (рассмотреть g наименьшей степени m, для которого $fg = 0$, и доказать по индукции $a_i g = 0$);

3) f нильпотентен $\Leftrightarrow$ все коэффициенты f нильпотентны;
4) f идемпотентен $\Leftrightarrow f = f_0$, f_0 идемпотентен.

Задача 4. Если R коммутативно, то $R[x]$ не может быть чистым.

Задача 5. $R[x]$ не может быть чистым ни для какого R. Указание: аналогично пункту 4) коммутативного случая вывести, что в разложении x идемпотент может быть равен только единице.

Задача 6. R чистое $\Leftrightarrow R[[x]]$ однозначно чистое.

Задача 7. Покажите, что если элемент a кольца R раскладывается в произведение коммутирующих идемпотента и обратимого элемента, то он строго чист.

Задача 8. Приведите пример чистого, но не строго чистого кольца.

Задача 9. Покажите, что ниль-чистое кольцо является чистым.

Задача 10. Покажите, что в ниль-чистом кольце элемент 2 нильпотентен.

7 Первичные и полупервичные идеалы и кольца. Радикал идеала. Первичный радикал кольца

Лекция 8. Первичные и полупервичные идеалы и кольца. Радикал идеала. Первичный радикал кольца

Определение 7.1. *Правый делитель нуля* — элемент $r \in R$, для которого существует такой ненулевой $s \in R$, что $sr = 0$. Аналогично опредлеяется левый делитель нуля. Элемент кольца называется *делителем нуля*, если он является делителем нуля хотя бы с одной стороны. Элемент не являющийся делителем нуля называют *регулярным*.

Правый делитель нуля не может быть обратим справа. Однако если кольцо не конечно по Дедекинду, то он может быть обратим слева. Напомним классический пример.

Пример 7.2. Пусть $V = \mathbb{F}^\infty$ — пространство последовательностей $(x_1, x_2, x_3, \ldots)$ элементов поля $\mathbb{F}$, и $R = \operatorname{End} V$. Рассмотрим линейные операторы l, r сдвига координат на одну позицию влево и вправо соответственно: $l(x_1, x_2, \ldots) = (x_2, x_3, \ldots)$, $r(x_1, x_2, \ldots) = (0, x_1, x_2, \ldots)$. Пусть p_1 — оператор проекции на первую координату: $p_1(x_1, x_2, \ldots) = (x_1, 0, \ldots)$. Тогда lr тождественно на V, но $p_1 r = 0$.

Определение 7.3. Кольцо R называется *областью*, если оно ненулевое и удовлетворяет любому из эквивалентных условий:

1) для любых $r, s \in R$ из условия $rs = 0$ следует, что $r = 0$ или $s = 0$;

2) 0 — единственный левый делитель нуля;

3) 0 — единственный правый делитель нуля;

3) 0 — единственный делитель нуля.

Коммутативную область называют *областью целостности*.

Пример 7.4.

1. Областью является любое тело, поле, а также $\mathbb{Z}$.
2. Если R — область, то $R[t_1, \ldots, t_n]$ — тоже область.
3. Кольцо матриц $M_n(R)$ не будет областью ни для какого кольца R.

Временно ограничимся случаем коммутативного кольца K. Нас будут интересовать такие идеалы $I \lhd K$, что K/I является областью. Это в точности идеалы следующего вида.

Определение 7.5. Идеал I в коммутативном кольце K называется *простым*, если $I \neq R$ и из условия $ab \in I$ следует, что по крайней мере один элемент a или b содержится в I.

Коммутативное кольцо K является областью тогда и только тогда, когда нулевой идеал (0) прост.

Замечание 7.6. Идеал I в коммутативном кольце K является простым тогда и только тогда, когда его теоретико-множественное дополнение $K \backslash I$ мультипликативно замкнуто, т.е. является полугруппой по умножению.

Заметим, что всякий максимальный идеал прост, т.к. фактор по нему будет полем. Обратное неверно. В кольце $K = \mathbb{F}[x, y]$ идеал $(y) = Ky$ прост, т.к. фактор по нему изоморфен области $\mathbb{F}[x]$, но (y) не максимален, т.к. $\mathbb{F}[x]$ не поле.

Определение 7.7. *Радикал* $\sqrt{I}$ идеала I в коммутативном кольце K — множество всех элементов $a \in R$ таких, что для некоторого натурального n выполнено $a^n \in I$.

Отметим, что n в определении может зависить от a.

Радикал идеала сам является идеалом. Действительно, если $a^n \in I$ и $b^m \in I$, тогда $(a + b)^{m+n} \in I$ ввиду формулы бинома Ньютона, а также $(ar)^n = a^n r^n \in I$.

Определение 7.8. Идеал $I \lhd K$ в коммутативном кольце K *радикален*, если $\sqrt{I} = I$.

Таким образом, $\sqrt{I}$ — это наименьший радикальный идеал, содержащий I.

Радикальные идеалы играют важную роль в классической алгебраической геометрии. Для алгебраически замкнутого поля $\mathbb{F}$ между радикальными идеалами кольца многочленов $\mathbb{F}[t_1, \ldots, t_n]$ и решениями систем полиномиальных уравнений существует взаимно-однозначное соответствие, сохраняющее включения. Это следствие теоремы Гильберта о нулях.

Теорема 7.9 (Hilbert's Nullstellensatz)**.** Пусть $\mathbb{F}$ — алгебраически замкнутое поле и I — идеал в кольце $\mathbb{F}[t_1, \ldots, t_n]$. Также пусть $Z(I) \subseteq \mathbb{F}^n$ — множество точек, в которых все многочлены идеала I обращаются в ноль. Тогда, если многочлен f тоже обращается в ноль во всех точках $Z(I)$, то $f^r \in I$ для некоторого $r \in \mathbb{N}$.

Без доказательства. □

Радикал идеала можно выразить в терминах пересечений простых идеалов.

Теорема 7.10. Радикал $\sqrt{I}$ совпадает с пересечением всех простых идеалов, содержащих I. В частности, идеал радикален тогда и только тогда, когда он является пересечением простых идеалов.

Докажем далее в более общей постановке. □

Заметим, $r \in \sqrt{(0)}$ тогда и только тогда, когда $r^n = 0$ для некоторого n. Другими словами, радикал нулевого идеала $\sqrt{(0)}$ совпадаеат с множеством всех нильпотентных элементов коммутативного кольца K. Поэтому $\sqrt{(0)}$ называют *нильрадикалом*.

Следствие 7.11. Нильрадикал коммутативного кольца совпадает с пересечением всех простых идеалов.

В некоммутативном кольце все нильпотенты не обязаны образовывать идеал. Достаточно рассмотреть кольцо матриц над полем.

Обобщим предыдущие конструкции из коммутативной алгебры на случай произвольного ассоциативного кольца R с единицей. Оказывается, что тогда более содержательно рассматривать произведения не отдельных элементов, а целых идеалов. Напомним, что произведением AB двусторонних идеалов A, B называется множество всех конечных сумм вида $\sum\limits_i a_i b_i$, где $a_i \in A$, $b_i \in B$, тогда AB само является идеалом.

Определение 7.12. Двусторонний идеал $I \lhd R$ называется *первичным*, если $I \neq R$ и для любых двусторонних идеалов $A, B \lhd R$ из условия $AB \subseteq I$ следует, что по крайней мере один идеал A или B является подмножеством в I.

Как обычно $(a) = RaR = \{\sum\limits_i r_i a s_i \mid r_i, s_i \in R\}$ — главный идеал, порождённый элементом a в кольце R.

Предложение 7.13. Для двустороннего идеала $I \lhd R$, $I \neq R$, следующие условия эквивалентны:

1) I первичен;
2) из $(a)(b) \subseteq I$ следует, что либо $a \in I$, либо $b \in I$;
3) из $aRb \subseteq I$ следует, что либо $a \in I$, либо $b \in I$;
4) для правых идеалов $A, B \subseteq R$ из $AB \subseteq I$ следует, что либо $A \subseteq I$, либо $B \subseteq I$.
4') для левых идеалов $A, B \subseteq R$ из $AB \subseteq I$ следует, что либо $A \subseteq I$, либо $B \subseteq I$.

Доказательство. 1) $\Rightarrow$ 2) Частный случай.

2) $\Rightarrow$ 3) Из условия $aRb \subseteq I$ вытекает $(a)(b) \subseteq I$, т.к. I — двусторонний идеал.

3) $\Rightarrow$ 4) Предположим, что $B \not\subseteq I$. Рассмотрим $b \in B$, не лежащий в I. Тогда для всякого $a \in A$ выполнено $aRb \subseteq A(RB) = AB \subseteq I$, откуда $a \in I$. Значит, $A \subseteq I$ в силу произвольности a. Случай $A \not\subseteq I$ разбирается аналогично.

4) $\Rightarrow$ 1) Частный случай.

3) $\Rightarrow$ 4') $\Rightarrow$ 1) Симметрично. □

Отметим, что в предыдущем предложении все альтернативы «либо ..., либо ... » не являются взаимоисключающими.

Пример 7.14. Всякий максимальный идеал I первичен: если A, B — идеалы, не лежащие в I, то $R = A + I = B + I$, поэтому $R = (A + I)(B + I) = AB + I$, откуда $AB \not\subseteq I$.

Определения простого и первичного идеала согласованы.

Следствие 7.15. Идеал коммутативного кольца первичен тогда и только тогда, когда он прост.

Доказательство. Применим пункт 2) предложения. □

В англоязычной литературе и для простых идеалов коммутативного кольца, и для первичных идеалов произвольного кольца используют один и тот же термин prime ideals.

Определение 7.16. Непустое подмножество S кольца R называется *m-системой*, если для любых $a, b \in S$ существует элемент $r \in R$ такой, что $arb \in S$.

Заметим, что всякое мультипликативно замкнутое подмножество кольца является m-системой. Обратное в общем случае неверно.

Следствие 7.17. Первичность идеала $I \lhd R$ равносильна тому, что его теоретико-множественное дополнение $R \setminus I$ является m-системой.

Доказательство. Отрицание пункта 3) предложения. □

Нам понадобятся m-системы специального вида.

Определение 7.18. Последовательность $a_0, a_1, \ldots$ элементов кольца R называется m-последовательностью, если $a_{i+1} \in a_i R a_i$ для всех $i \geqslant 0$.

Лемма 7.19. Любая m-последовательность является m-системой.

Доказательство. Пусть $a_0, a_1, \ldots$ — некоторая m-последовательность. Рассмотрим произвольные два ее элемента a_k, a_l, где $l \geqslant k \geqslant 0$. Необходимо показать, что и $a_k R a_l$, и $a_l R a_k$ содержат хотя бы по одному элементу нашей последовательности. Построим цепочку включений

$$a_{l+1} \in a_l R a_l \subseteq (a_{l-1} R a_{l-1}) R a_l \subseteq \ldots \subseteq a_k R a_k R a_{k-1} R \ldots a_{l-1} R a_l.$$

Значит, $a_{l+1} \in a_k R a_l$. Аналогично удлинняя произведение вправо, получаем включение $a_{l+1} \in a_l R a_k$. □

Определение 7.20. *Радикал* $\sqrt{I}$ идеала I в произвольном ассоциативном кольце R с единицей — это множество таких элементов $a \in R$, что всякая m-система, содержащая a, имеет непустое пересечение с идеалом I.

Предложение 7.21. Радикал $\sqrt{I}$ совпадает с множеством таких $a \in R$, что для любой m-последовательности $(a_i)_{i=0}^{\infty}$, начинающейся с $a_0 = a$, некоторый её член a_i попадает в идеал I.

Доказательство. По предыдущей лемме всякая m-последовательность, является m-системой. Поэтому для элемента $a \in \sqrt{I}$ и произвольной m-последовательности $(a_i)_{i=0}^{\infty}$, где $a_0 = a$, получаем, что пересечение $(a_i)_{i=0}^{\infty} \cap I$ непусто по определению радикала идеала. Отсюда некоторый a_i оказывается в идеале I.

Обратно, пусть элемент $a \in R$ удовлетворяет условию на m-последовательности. Покажем, что $a \in \sqrt{I}$. Предположим противное, тогда найдется m-система S, содержащая a, но при этом $S \cap I = \varnothing$. Будем строить m-последовательность. Полагаем $a_0 = a$. По определению m-системы найдется $r_0 \in R$ такой, что элемент $a_1 = a_0 r_0 a_0$ попадает в S. Аналогично найдется $r_1 \in R$ такой, что элемент $a_2 = a_1 r_1 a_1$ попадает в S и т.д. Получаем m-последовательность $(a_i)_{i=0}^{\infty}$, $a_0 = a$. По нашему предположению найдется $a_i \in I$, но по построению $a_i \in S$. Противоречие с $S \cap I = \varnothing$. □

Следствие 7.22. Выполнено $\sqrt{I} \subseteq \{a \in R \mid a^n \in I \text{ для некоторого } n \in \mathbb{N}\}$.

Доказательство. Положим $a_i = a^{2^i}$. Тогда $(a_i)_{i=0}^{\infty}$ — это m-последовательность, т.к. $a_{i+1} = a^{2^{i+1}} = a^{2^i} \cdot 1 \cdot a^{2^i} \in a_i R a_i$. По предыдущему предложению для некоторого i имеем $a^{2^i} \in I$.

□

Следствие 7.23. Для коммутативного кольца K оба определения радикала идеала $I \lhd K$ эквивалентны.

Доказательство. Включение в одну сторону верно для любого кольца в силу предыдущего. Обратно, заметим, что в коммутативном кольце любая m-последовательность, начинающаяся с элемента a, может быть записана в виде $a, a^2 r_1, a^4 r_2, \ldots, a^{2^k} r_k, \ldots$,

где $(r_k)_{k=1}^{\infty}$ — подходящая последовательность элементов кольца. Но для некоторого n имеем $a^n \in I$, при этом I — идеал, откуда при $2^k \geqslant n$ элемент $a^{2^k} r_k$ также содержится в I.

□

Лемма 7.24. Пусть $S \subseteq R$ — это m-система. Предположим, что $I \lhd R$ — это максимальный элемент в множестве всех идеалов, не пересекающихся с S. Тогда I первичен.

Доказательство. От противного, пусть $a, b \notin I$, но $(a)(b) \subseteq I$. В силу максимальности I, в S существуют такие элементы s, s', что $s \in I + (a)$, $s' \in I + (b)$. Рассмотрим $r \in R$, для которого $srs' \in S$. Тогда $srs' \in (I + (a))R(I + (b)) \subseteq I + (a)(b) \subseteq I$, противоречие. □

Теорема 7.25. Радикал $\sqrt{I}$ совпадает с пересечением всех первичных идеалов, содержащих I. В частности, $\sqrt{I}$ — идеал.

Доказательство. Пусть $s \in \sqrt{I}$, $I \subseteq J$, где J — первичный идеал. Рассмотрим m-систему $R \setminus J$. Если бы она содержала s, то пересекалась бы с идеалом I, а значит и с идеалом J, что невозможно. Поэтому $s \in J$. Мы показали, что

$$\sqrt{I} \subseteq \bigcap \{J \lhd R \mid I \subseteq J,\ J \text{ первичен}\}.$$

Пусть $s \notin \sqrt{I}$. Тогда по определению радикала существует m-система S, содержащая s, но не пересекающаяся с идеалом I. Рассмотрим семейство идеалов $\Omega = \{L \lhd R \mid I \subseteq L,\ L \cap S = \varnothing\}$, упорядоченное по включению. Тогда $\Omega \neq \varnothing$, т.к. $I \in \Omega$. Если $\{L_\lambda\}_{\lambda \in \Lambda}$ — цепь в Ω, то её объединение снова принадлежит Ω. Поэтому по лемме Цорна в Ω найдется максимальный элемент J. Идеал J первичен по предыдущей лемме. Поскольку J не пересекает S, элемент s ему не принадлежит. Мы показали, что

$$R \setminus \sqrt{I} \subseteq R \setminus \bigcap \{J \lhd R \mid I \subseteq J,\ J \text{ первичен}\}.$$

□

Определение 7.26. Идеал $I \lhd R$ *полупервичен*, если для всякого идеала $H \lhd R$, для которого $H^2 \subseteq I$, выполнено и $H \subseteq I$.

Первичный идеал всегда полупервичен.

Эквивалентность следующих условий проверяется точно так же, как в случае первичного идеала.

Предложение 7.27. Для идеала $I \lhd R$ эквивалентны условия:
1) I полупервичен;
2) из $(a)^2 \subseteq I$ следует, что $a \in I$;
3) из $aRa \subseteq I$ следует, что $a \in I$;
4) для правого идеала $A \subseteq R$ из $A^2 \subseteq I$ следует, что $A \subseteq I$.
4') для левого идеала $A \subseteq R$ из $A^2 \subseteq I$ следует, что $A \subseteq I$.

Понятие полупервичного идеала — некоммутативное обобщение радикального идеала.

Следствие 7.28. Идеал коммутативного кольца K является радикальным тогда и только тогда, когда он полупервичен.

Доказательство. Если идеал I радикален и $(a)^2 \subseteq I$, то $a^2 \in I$, а значит, $a \in I$ и применим пункт 2) предложения. Обратно, пусть идеал I полупервичен и $a^n \in I$. Выберем какую-нибудь степень двойки 2^k, которая не меньше, чем n. Тогда $a^{2^k} \in I$, откуда $(a)^{2^k} \subseteq I$ в силу коммутативности кольца. Применяя индукцию и пункт 2) предложения, получаем $a \in I$. □

Определение 7.29. Непустое подмножество $S \subseteq R$ называется *n-системой*, если для каждого $a \in S$ существует элемент $r \in R$ такой, что $ara \in S$.

Каждая m-система является n-системой тривиальным образом. Обратное в общем случае неверно.

Следствие 7.30. Идеал полупервичен тогда и только тогда, когда его теоретико-множественное дополнение является n-системой.

Доказательство. Отрицание пункта 3) предложения. □

Лемма 7.31. Пусть $N \subseteq R$ является n-системой, выберем в ней произвольный элемент $a \in N$. Тогда существует m-система $M \subseteq N$ такая, что $a \in M$.

Доказательство. В качестве m-системы возьмем m-последовательность следующего вида. Пусть $a_0 = a$. По определению n-системы, множество N содержит элементы $a_1 = a_0 r_0 a_0$, $a_2 = a_1 r_1 a_1$, …, $a_{n+1} = a_n r_n a_n$, … для некоторых $r_i \in R$. Тогда полагаем $M = \{a_1, a_2, \ldots\}$. □

Теорема 7.32 (О полупервичном идеале)**.** Для идеала $I \lhd R$ эквивалентны условия:
1) I полупервичен;
2) $I = \sqrt{I}$.
3) I — пересечение некоторого множества первичных идеалов;

Доказательство. 1) $\Rightarrow$ 2) Включение $I \subseteq \sqrt{I}$ выполнено всегда, надо показать, что $\sqrt{I} \subseteq I$. Это равносильно $R \setminus I \subseteq R \setminus \sqrt{I}$. Возьмем произвольный $a \in R \setminus I$, но множество $R \setminus I$ является n-системой, т.к. идеал I первичен. По лемме можно выбрать m-систему $M \subseteq R \setminus I$ такую, что $a \in M$. Итак, мы нашли m-систему, содержащую a, но не пересекающуюся с идеалом I. По определению радикала имеем $a \notin \sqrt{I}$, что и требовалось.

2) $\Rightarrow$ 3) Используем предыдущую теорему о том, что радикал $\sqrt{I}$ совпадает с пересечением всех первичных идеалов, содержащих I.

3) $\Rightarrow$ 1) Каждый первичный идеал полупервичен. Заметим, что пересечение любого множества полупервичных идеалов снова полупервичный идеал. $\square$

Следствие 7.33. Радикал $\sqrt{I}$ идеала I — наименьший полупервичный идеал, содержащий I.

Применим все полученные ранее результаты о радикалах идеала к случаю радикала нулевого идеала. Перед этим нам понадобится следующее определение.

Определение 7.34. Элемент a кольца R называется *строго нильпотентным*, если в любой m-последовательности $(a_i)_{i=0}^{\infty}$, начинающейся с элемента $a_0 = a$, найдется нулевой элемент $a_i = 0$ (тогда все последующие члены автоматически тоже равны нулю).

Теорема 7.35 (О первичном радикале)**.** Следующие подмножества кольца R совпадают:

1) радикал нулевого идеала $\sqrt{(0)}$,
2) пересечение всех первичных идеалов,
3) множество всех строго нильпотентных элементов,
4) наименьший полупервичный идеал.

Доказательство. 1) $\Leftrightarrow$ 2) Радикал $\sqrt{I}$ совпадает с пересечением всех первичных идеалов, содержащих I.

1) $\Leftrightarrow$ 3) Характеризация радикала в терминах m-последовательностей.

1) $\Leftrightarrow$ 4) Радикал $\sqrt{I}$ — наименьший полупервичный идеал, содержащий I. $\square$

Определение 7.36. *Первичный радикал* $\mathrm{Nil}_* R$ кольца R — это пересечение всех его первичных идеалов. Также используются названия *нижний нильрадикал* и *радикал Бэра — Маккоя.*

Любой из пунктов предыдущей теоремы может быть взят в качестве определения первичного радикала.

Следствие 7.37. Первичный радикал является нильидеалом, т.е. все его элементы нильпотенты. Другими словами, каждый строго нильпотентный элемент нильпотентен.

Доказательство. В силу следствия из предложения о характеризации радикала в терминах m-последовательностей $\sqrt{I} \subseteq \{a \in R \mid a^n \in I \text{ для некоторого } n \in \mathbb{N}\}$. Полагаем $I = (0)$. □

Следствие 7.38. Первичный радикал всегда содержится в радикале Джекобсона $\mathrm{Nil}_* R \subseteq J(R)$.

Доказательство. Радикал Джекобсона содержит все нильидеалы. □

Следствие 7.39. Первичный радикал содержит все правые и все левые нильпотентные идеалы.

Доказательство. Так как радикал $\mathrm{Nil}_* R$ полупервичен, то для правого идеала I из условия $I^2 \subseteq \mathrm{Nil}_* R$ следует $I \subseteq \mathrm{Nil}_* R$. Значит, если для некоторого k выполнено $I^{2^k} \subseteq \mathrm{Nil}_* R$, то $I \subseteq \mathrm{Nil}_* R$. Однако в случае, когда I нильпотентен, для достаточного большого k имеем $I^{2^k} = (0) \subseteq \mathrm{Nil}_* R$. □

Следствие 7.40. Первичный радикал коммутативного кольца K совпадает с нильрадикалом, т.е. множеством всех нильпотентных элементов.

Следствие 7.41. Если $\phi : R \to T$ — это сюръективный гомоморфизм колец, тогда $\phi(\mathrm{Nil}_* R) \subseteq \mathrm{Nil}_* T$.

Доказательство. От противного, выберем такой $x \in \mathrm{Nil}_* R$, что его образ $y = \phi(x)$ не лежит в $\mathrm{Nil}_* T$. По определению радикала $\sqrt{(0)}$ это значит, что в кольце T найдётся некоторая m-система S, содержащая y, но не содержащая 0. Покажем, что полный прообраз $\phi^{-1}(S)$ будет m-системой в кольце R. Если $a, b \in \phi^{-1}(S)$, то для элементов $\phi(a), \phi(b)$ найдется $t \in T$ такой, что $\phi(a)t\phi(b) \in S$ по определению m-системы. В силу сюръективности ϕ найдется $r \in R$ такой, что $\phi(r) = t$, откуда $\phi(arb) = \phi(a)\phi(r)\phi(b) \in S$, т.е. $arb \in \phi^{-1}(S)$. Итак $\phi^{-1}(S)$ — m-система. Так как $y \in S$, то $x \in \phi^{-1}(S)$. Однако в силу $0 \notin S$ имеем $0 \notin \phi^{-1}(S)$, но это противоречит $x \in \mathrm{Nil}_* R = \sqrt{(0)}$. □

Аналогичное доказательство можно дать в терминах строго нильпотентных элементов.

Перейдем к понятиям первичного и полупервичного кольца.

Определение 7.42. Кольцо *(полу)первично*, если идеал (0) (полу)первичен.

Из определения вытекает, что факторкольцо R/I (полу)первично тогда и только тогда, когда идеал I (полу)первичен.

Используя описание первичных и полупервчиных идеалов получаем более явную характеризацию аналогичных классов колец.

Предложение 7.43. Следующие условия на кольцо R эквивалентны:

1) R первично, т.е. (0) — первичный идеал.
2) из $(a)(b) = (0)$ следует, что либо $a = 0$, либо $b = 0$;
3) из $aRb = 0$ следует, что либо $a = 0$, либо $b = 0$;
4) для правых идеалов A, B из $AB = (0)$ следует, что либо $A = (0)$, либо $B = (0)$.
4') для левых идеалов A, B из $AB = (0)$ следует, что либо $A = (0)$, либо $B = (0)$.

Пример 7.44. Приведём примеры первичных колец.

- Всякая область R является первичным кольцом. Коммутативное кольцо K первично тогда и только тогда, когда оно является областью.
- Всякое простое кольцо первично. Действительно, в простом кольце 0 — максимальный идеал. Максимальный идеал всегда первичен, см. пример ранее.

Предложение 7.45. Следующие условия на кольцо R эквивалентны:

1) R полупервично, т.е. (0) — полупервичный идеал;
2) из $(a)^2 = 0$ следует, что $a = 0$;
3) из $aRa = 0$ следует, что $a = 0$;
4) для правого идеала A из $A^2 = (0)$ следует, что $A = (0)$;
4') для левого идеала A из $A^2 = (0)$ следует, что $A = (0)$.

Напомним, что правый (левый, двусторонний) идеал идеал I называется нильпотентным, если для некоторого n выполнено $I^n = 0$.

Теорема 7.46. Для кольца R эквивалентны условия:

1) R полупервично;
2) $\mathrm{Nil}_* R = 0$;
3) в R нет ненулевых нильпотентных идеалов;
4) в R нет ненулевых нильпотентных правых идеалов;
4') в R нет ненулевых нильпотентных левых идеалов.

Доказательство. 1) $\Rightarrow$ 2) Нулевой идеал полупервичен, при этом радикал совпадает с наименьшим полупервичным идеалом.

2) $\Rightarrow$ 1) Первичный радикал всегда является полупервичным идеалом.

1) $\Rightarrow$ 4) Пусть I — нильпотентый правый идеал. Выберем n — наименьшее число такое, что $I^n = 0$. Предположим, что I ненулевой идеал, т.е. $n > 1$. Тогда $(I^{n-1})^2 = I^{2n-2} \subseteq I^n = 0$. В силу одного из эквивалетных определений полупервичного кольца получаем $I^{n-1} = 0$, что противоречит выбору n. Значит, $n = 1$ и $I = 0$.

4) $\Rightarrow$ 3) Частный случай.

3) $\Rightarrow$ 1) В частности, если $(a)^2 = 0$, то $a = 0$.

1) $\Rightarrow$ 4') $\Rightarrow$ 3) Аналогично. $\square$

Определение 7.47. Кольцо, в котором ноль — единственный нильпотент, называют *редуцированным кольцом*[8].

[8] В англоязычной литературе — reduced ring.

Пример 7.48. Приведем примеры полупервичных колец

- Всякое первичное кольцо полупервично.
- Всякое редуцированное кольцо R является полупервичным. Коммутативное кольцо K полупервично тогда и только тогда, когда оно редуцировано.
- Если кольцо полупримитивно (т.е. обладает нулевым радикалом Джекобсона), то оно всегда полупервично, в силу включения $\mathrm{Nil}_* R \subseteq J(R)$. В частности, полупростые кольца и регулярные по фон Нейману кольца также полупервичны.
- Прямое произведение полупервичных колец полупервично. Отметим, что для первичных колец это неверно.
- Для любого кольца R выполнено $\mathrm{Nil}_*(R/\mathrm{Nil}_* R) = 0$. Действительно, факторкольцо R/I полупервично тогда и только тогда, когда идеал I полупервичен, при этом $\mathrm{Nil}_* R$ как раз полупервичен.

Следующие результаты о первичных и полупервичных групповых кольцах приведем без доказательства.

Теорема 7.49 (Коннелл)**.** Групповое кольцо RG первично тогда и только тогда, когда R первично и единственная конечная нормальная подгруппа в G — это $\{1\}$.

Теорема 7.50 (Пассман)**.** Групповое кольцо RG полупервично тогда и только тогда, когда R полупервично, а порядки всех конечных нормальных подгрупп в G не являются делителями нуля в R.

Определение 7.51. *Аннулятор* $\mathrm{Ann}_R(N)$ подмножества N в правом модуле M_R — это множество всех элементов $r \in R$, для которых $nr = 0$ при всех $n \in N$.

Правый аннулятор $\mathrm{rAnn}(S)$ подмножества $S \subseteq R$ равен $\mathrm{Ann}\,(S)$, где S рассматривается как подмножество R_R.

Отметим, что правый аннулятор всегда является правым идеалом в R.

Напомним, что ненулевой правый идеал называется минимальным, если он не содержит в себе никаких отличных от себя ненулевых правых идеалов.

Лемма 7.52 (Брауэр)**.** Пусть в кольце R существует минимальный правый идеал I. Тогда либо $I^2 = 0$, либо $I = eR$ для некоторого идемпотента e.

Доказательство. Если $I = R$, то I порождается единицей, пусть далее $I \neq R$. Если $I^2 \neq 0$, то $aI \neq 0$ для некоторого $a \in I$, откуда ввиду минимальности $aI = I$. Выберем $r \in I$ таким, что $ar = a$, т.е. $a(r-1) = 0$. Тогда пересечение $\mathrm{rAnn}(a) \cap I$ не может совпадать со всем I, поскольку $r - 1 \notin I$ из-за $r \in I$. В силу минимальности I получаем $\mathrm{rAnn}(a) \cap I = 0$. При этом $r^2 - r \in I$ и $a(r^2 - r) = 0$, а значит $r^2 - r \in \mathrm{rAnn}(a) \cap I = 0$. Отсюда $r^2 = r$ — ненулевой идемпотент. При этом правый идеал rR лежит в I, и снова в силу минимальности получаем $rR = I$. □

Теорема 7.53. Для кольца $R \neq 0$ эквивалентны условия:

1) R полупросто;

2) R полупервично и артиново справа;

3) R полупервично и удовлетворяет условию обрыва убывающих цепей главных правых идеалов.

2'), 3') — левые аналоги

Доказательство. 1) $\Rightarrow$ 2) Для полупростого кольца R выполнено $J(R) = 0$, откуда $\mathrm{Nil}_*(R) = 0$, значит R полупервично. Полупростое кольцо всегда артиново справа.

2) $\Rightarrow$ 3) Частный случай.

3) $\Rightarrow$ 1) Заметим, что каждый правый идеал кольца R содержит минимальный правый идеал, т.к. иначе можно было бы построить бесконечную убывающую цепочку правых идеалов, которые можно выбрать главными. По лемме Брауэра минимальный правый идеал I в полупервичном кольце R сам является главным, причём порождается идемпотентом. Следовательно каждый такой идеал $I = eR$ выделяется прямым слагаемым $R_R = eR \oplus (1 - e)R$. Далее будем рассуждать от противного, пусть R_R не полупростой модуль. Возьмем в R любой правый идеал, выберем в нём минимальный L_1 и выделим его прямым слагаемым: $R_R = L_1 \oplus T_1$. Так как R_R не полупрост, то T_1 не минимальный правый идеал, выберем в нём минимальный L_2 и выделим его прямым слагаемым $T_1 = L_2 \oplus T_2$ и т.д. Мы получаем бесконечную строго убывающую цепочку правых идеалов $T_1 \supsetneq T_2 \supsetneq T_3 \supsetneq \ldots$, причем каждый T_i является прямым слагаемым в R_R, а значит, порождается каким-то идемпотентом, откуда T_i — главный правый идеал. Мы получили противоречие с пунктом 3). $\square$

Задачи к лекции 8.

Задача 1. Пусть в коммутативном кольце K все идеалы главные, т.е. порождаются одним элементом. Докажите, что каждый простой идеал K максимален.

Задача 2. Приведите пример двух первичных идеалов, пересечение которых не будет первичным.

Задача 3. Приведите пример кольца R и его подкольца S, для которых $\mathrm{Nil}_*(S) \neq S \cap \mathrm{Nil}_*(R)$.

Задача 4. Приведите пример элемента некоторого кольца, который нильпотентен, но не строго нильпотентен.

Задача 5. Докажите, что если $I, J \lhd R$, то произведение идеалов $M_n(I) \cdot M_n(J)$ матричного кольца $M_n(R)$ совпадает с $M_n(IJ)$. Вывести отсюда, что кольцо матриц $M_n(R)$ над (полу)первичным кольцом R само окажется (полу)первичным.

Задача 6. Могут ли в первичном кольце быть ненулевые центральные а) делители нуля, б) нильпотенты? Тот же вопрос для полупервичного кольца.

Задача 7. Приведите пример кольца R такого, что его радикал Джекобсона а) совпадает с первичным радикалом, б) сторого содержит в себе первичный радикал.

Задача 8. В кольце многочленов $\mathbb{F}[x]$ над полем $\mathbb{F}$ дан идеал I, порожденный многочленом $(x^2 - 2x - 3)^7$. Найдите $\sqrt{I}$. Представьте $\sqrt{I}$ в виде пересечения простых идеалов.

Задача 9. Пусть R — редуцированное кольцо, докажите следующее:

а) для любых $a, b \in R$ если $ab = 0$, то $ba = 0$;

б) для любых $a, b \in R$ если $ab = 0$, то $aRb = bRa = 0$;

в) для любых $a_1, \ldots, a_n \in R$ и любой подстановки σ на n элементах если произведение $a_1 \cdot \ldots \cdot a_n = 0$, то тогда $Ra_{\sigma(1)}Ra_{\sigma(2)}R \ldots Ra_{\sigma(n)}R = 0$.

8 Радикал Кёте. Классическое кольцо частных. Условие Оре. Кольца Голди

Лекция 9. Радикал Кёте. Классическое кольцо частных. Условие Оре. Кольца Голди

В этой лекции мы введем ещё один радикал кольца. Перед этим нам понадобится следующая лемма.

Лемма 8.1. Если I — левый нильидеал, J — двусторонний нильидеал кольца R, тогда $I + J$ — левый нильидеал.

Доказательство. Пусть $a \in I + J$, тогда $a^n \in J$ для некотрого n. Так как J — нильидеал, то $(a^n)^m = 0$ для некоторого m. □

Определение 8.2. Сумма всех двусторонних нильидеалов кольца R называют *радикалом Кёте*, или *верхним нильрадикалом*. Обозначение $\mathrm{Nil}^* R$.

Как обычно $(a) = RaR = \{\sum\limits_i r_i a s_i \mid r_i, s_i \in R\}$ — главный идеал, порождённый элементом a в кольце R.

Предложение 8.3. Радикал Кёте — двусторонний идеал кольца. Более того, он является наибольшим нильидеалом кольца, и $\mathrm{Nil}^* R = \{a \in R \mid (a) \text{ — нильидеал}\}$.

Доказательство. Радикал $\mathrm{Nil}^* R$ — наибольший нильидеал по лемме. Включение $\mathrm{Nil}^* R \supseteq \{a \in R \mid (a) \text{ — нильидеал}\}$ выполнено по определению. Обратно, если $a \in \mathrm{Nil}^* R$, тогда $(a) \subseteq \mathrm{Nil}^* R$ и все элементы идеала (a) нильпотенты. □

Предложение 8.4. Для любого кольца R выполнено $\mathrm{Nil}_* R \subseteq \mathrm{Nil}^* R \subseteq J(R)$. Если R артиново хотя бы с одной стороны, то все три радикала совпадают.

Доказательство. Так как $\mathrm{Nil}_* R$ — нильидеал, то $\mathrm{Nil}_* R \subseteq \mathrm{Nil}^* R$. Включение $\mathrm{Nil}^* R \subseteq J(R)$ следует из того, что радикал Джекобсона содержит все нильидеалы. Для артинова справа кольца $J(R)$ нильпотентен, но $\mathrm{Nil}_* R$ содержит все нильпотентные идеалы, откуда $J(R) \subseteq \mathrm{Nil}_* R$, и все включения в цепочке радикалов обращаются в равенства. □

Гипотеза Кёте (1930). Если в произвольном кольце R выполнено $\mathrm{Nil}^* R = 0$, то R не имеет ненулевых односторонних нильидеалов.

Другими словами, если в кольце нет ненулевых нильидеалов, то нет и ненулевых *односторонних* нильидеалов. В наибольшей общности эта проблема пока не решена. Мы покажем далее, что гипотеза Кёте верна для нётеровых справа колец.

В этой лекции мы будем часто использовать левые и правые аннуляторы элементов и подмножеств произвольного кольца, поэтому введём для них упрощенные обозначения: если S – подмножество кольца R, то положим

$$l(S) = \mathrm{lAnn}(S) = \{r \in R \mid rS = 0\}, \;\; r(S) = \mathrm{rAnn}(S) = \{r \in R \mid Sr = 0\}.$$

Предложение 8.5. Пусть кольцо R удовлетворяет условию обрыва возрастающих цепей правых аннуляторов вида $r(a)$, $a \in R$. Тогда любой односторонний нильидеал I содержится в первичном радикале $\mathrm{Nil}_* R$. В частности, если дополнительно R полупервично, то в нём нет ненулевых односторонних нильидеалов.

Доказательство. Сначала рассмотрим случай правого нильидеала I. От противного, пусть $I \not\subseteq \mathrm{Nil}_* R$. Среди элементов теоретико-множественной разности $I \setminus \mathrm{Nil}_* R$ выберем a, таким что его правый аннулятор $r(a)$ максимален.

Покажем, что для любого $x \in R$ выполнено $axa \in \mathrm{Nil}_* R$. Если $ax = 0$, то это, конечно, верно, пусть $ax \neq 0$. Так как I — правый нильидеал и $a \in I$, то элемент ax нильпотентен, т.е. можно найти такое k, что $(ax)^k = 0$, но $(ax)^{k-1} \neq 0$. Тогда элемент $x(ax)^{k-2}$ принадлежит правому аннулятору $r(axa)$, но не принадлежит $r(a)$, откуда $r(axa) \supsetneq r(a)$. В силу максимальности $r(a)$ получаем, что axa не может принадлежать $I \setminus \mathrm{Nil}_* R$, а значит, $axa \in \mathrm{Nil}_* R$.

Рассмотрим факторкольцо $\overline{R} = R/\mathrm{Nil}_* R$, пусть $\overline{a}, \overline{x}$ — образы элементов a, x при естественной проекции. Тогда в силу произвольности $x \in R$ имеем $\overline{a}\overline{R}\overline{a} = \overline{0}$ в силу $axa \in \mathrm{Nil}_* R$. Однако кольцо $\overline{R}$ полупервично, поэтому $\overline{a} = \overline{0}$, т.е. $a \in \mathrm{Nil}_* R$, и это потиворечит определению элемента a.

Если теперь I — левый нльидеал, то для всех $a' \in I$ можно рассмотреть правый идеал $a'R$. Покажем, что $a'R$ — правый нильидеал: для любого $b \in R$ и любого $n \in \mathbb{N}$ выполнено $(a'b)^n = a'(ba')^{n-1}b$, причем $ba' \in I$, тогда, выбирая n достаточно большим, можно добиться $(ba')^{n-1} = 0$, откуда $(a'b)^n = 0$. Итак, $a'R$ — правый нильидеал,

значит, по предыдущему $a'R \subseteq \mathrm{Nil}_* R$. В силу произвольности $a' \in I$ получаем $I \subseteq \mathrm{Nil}_* R$. □

Теорема 8.6 (Левицкий)**.** Пусть R — нётерово справа кольцо. Тогда каждый односторонний нильидеал нильпотентен. Первичный радикал $\mathrm{Nil}_* R$ и радикал Кёте $\mathrm{Nil}^* R$ совпадают и равны наибольшему нильпотентому идеалу кольца, который при этом оказывается одновременно и наибольшим левым, и наибольшим правым нильпотентным идеалом.

Доказательство. (Утуми) Так как R — нётерово справа, то в множестве всех двусторонних нильпотентных идеалов существует максимальный элемент N. Тогда в факторкольце R/N нет нильпотентных идеалов, а значит, R/N полупервично, откуда N — полупервчиный идеал. В силу того, что $\mathrm{Nil}_* R$ — наименьший полупервчный идеал, имеем $\mathrm{Nil}_* R \subseteq N$. В то же время $\mathrm{Nil}_* R$ содержит все нильпотентные идеалы, откуда получаем обратное включение, а значит $\mathrm{Nil}_* R = N$.

Так как правые аннуляторы — это правые идеалы, то R удовлетворяет условию обрыва возрастающих цепей правых аннуляторов вида $r(a)$, $a \in R$. По предыдущему предложению каждый односторонний нильидеал I содержится в первичном радикале $\mathrm{Nil}_* R$, но он нильпотентен. Значит I нильпотентен.

Включение $\mathrm{Nil}_* R \subseteq \mathrm{Nil}^* R$ всегда выполнено. Снова по предыдущему предложению каждый двусторонний нильидеал I содержится в первичном радикале $\mathrm{Nil}_* R$, тогда радикал Кёте $\mathrm{Nil}^* R$, как их сумма, также содержится в $\mathrm{Nil}_* R$. Поэтому получаем $\mathrm{Nil}_* R = \mathrm{Nil}^* R = N$.

Если I — произвольный правый (левый, двусторонний) нильпотентный идеал, то он содержится в первичном радикале $\mathrm{Nil}_* R = N$, а значит, тот является наибольшим правым (левым, двусторонним) нильпотентным идеалом. □

Следствие 8.7. Гипотеза Кёте верна для нётеровых справа колец.

Напомним, что ненулевой элемент $s \in R$ *регулярен*, если он не является ни левым, ни правым делителем нуля, т.е. $r(s) = l(s) = 0$. Множество всех регулярных элементов кольца R обозначим $S(R)$.

Всякий обратимый элемент регулярен, но не наоборот.

Заметим, что произведение любых двух регулярных элементов есть регулярный элемент.

Определение 8.8. Пусть $R \subseteq Q$ — кольца. Q называется *правым классическим кольцом частных* для R, если все элементы $S(R)$ обратимы в Q, и при этом каждый элемент $q \in Q$ может быть представлен в виде $q = ab^{-1}$, $a, b \in R$, $b \in S(R)$.

Аналогично вводится понятие левого классического кольца частных.

Пример 8.9.

- $\mathbb{Q}$ — (двустороннее) классическое кольцо частных для $\mathbb{Z}$.
- $\mathbb{Q} \times \mathbb{Q}$ — классическое кольцо частных для кольца $\{(a, b) \colon a \equiv b \pmod 7\} \subseteq \mathbb{Z} \times \mathbb{Z}$.
- $M_n(\mathbb{Q})$ — классическое кольцо частных для $M_n(\mathbb{Z})$.

Определение 8.10. Кольцо R удовлетворяет *правому условию Ope* (или является *правым кольцом Ope*), если для любых элементов $a \in R$, $s \in S(R)$, существуют такие элементы $a' \in R$, $s' \in S(R)$ для которых $as' = sa'$. В случае левого условия Ope последнее соотношение будет выглядеть как $s'a = a's$.

Пример 8.11. Коммутативное кольцо всегда удовлетворяет условию Ope с обеих сторон, достаточно положить $a' = a$ и $s' = s$.

Предложение 8.12. Правое классическое кольцо частных $R \subseteq Q$ удовлетворяет правому условию Ope.

Доказательство. Пусть $a \in R$, $s \in S(R)$. Тогда s обратим в Q, причем элемент $s^{-1}a \in Q$ можно представить в виде $a's'^{-1}$, где $s' \in S(R)$, $a' \in R$, отсюда $as' = sa'$. □

Докажем, что правое условие Ope не только необходимое, но и достаточное условие того, что у кольца имеется классическое правое кольцо частных.

Лемма 8.13 (Приведение к общему знаменателю)**.** Пусть R — правое кольцо Ope, $a, b \in S(R)$. Тогда существуют такие $c, d \in S(R)$, что $ac = bd$.

Доказательство. По условию Ope найдутся элементы $x_0, x_1 \in R$, $s_0, s_1 \in S(R)$, для которых $ax_0 = bs_0$, $as_1 = bx_1$, поэтому достаточно доказать, например, что $x_0 \in S(R)$, то есть что $\operatorname{lAnn}(x_0) = \operatorname{rAnn}(x_0) = \{0\}$.

Для правого аннулятора это очевидно: $\operatorname{rAnn}(x_0) \subseteq \operatorname{rAnn}(bs_0) = \{0\}$. Чтобы доказать это для левого аннулятора, снова воспользуемся правым условием Ope для элементов x_1, s_0: $s_0x_2 = x_1s_2$ для некоторых $x_2 \in R$, $s_2 \in S(R)$. Тогда

$$ax_0x_2 = bs_0x_2 = bx_1s_2 = as_1s_2,$$

откуда $0 = a(x_0x_2 - s_1s_2) = x_0x_2 - s_1s_2$ из регулярности a. Поэтому $\operatorname{lAnn}(x_0) \subseteq \operatorname{lAnn}(x_0x_2) = \operatorname{lAnn}(s_1s_2) = 0$. □

Теорема 8.14. Если R — правое кольцо Ope, то оно обладает правым классическим кольцом частных.

Доказательство. Обозначим $S = S(R)$. Рассмотрим декартово произведение множеств $M = R \times S$ и определим на нём отношение $\sim$:

$$(a, b) \sim (c, d), \text{ если существуют } s_1, s_2 \in S, \text{ для которых } bs_1 = ds_2 \text{ и } as_1 = cs_2.$$

Если понимать M как полугруппу с покомпонентным умножением, то предыдущее условие можно переписать в виде $(a, b) \cdot (s_1, s_1) = (c, d) \cdot (s_2, s_2)$. Заметим также, что при $s \in S$ всегда выполнено $(a, b) \sim (as, bs)$.

Рефлексивность и симметричность отношения $\sim$ очевидны. Проверим транзитивность: пусть $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$. Тогда для некоторых $s_1, s_2, s_3, s_4 \in S$ выполнено

$$bs_1 = ds_2, \quad as_1 = cs_2, \qquad ds_3 = fs_4, \quad cs_3 = es_4,$$

и, кроме того, по лемме существуют $s_5, s_6 \in S$ такие, что $s_2s_5 = s_3s_6$. Имеем $bs_1s_5 = ds_2s_5 = ds_3s_6 = fs_4s_6$ и $as_1s_5 = cs_2s_5 = cs_3s_6 = es_4s_6$, откуда $(a, b) \sim (e, f)$.

Класс эквивалентности пары $(a, b) \in M$ назовём *дробью* и обозначим символом a/b. На множестве Q всех дробей введём операции следующим образом.

Сложение: Для дробей a/b и c/d применяем лемму о приведении к общему знаменателю, находим $s_1, s_2 \in S$ такие, что $bs_1 = ds_2 = s$. Тогда $a/b = (as_1)/s$ и $c/d = (cs_2)/s$, и полагаем $a/b + c/d = (as_1 + cs_2)/s$.

Умножение: Для дробей a/b и c/d применяем правое условие Ope, находим $x' \in R$ $s' \in S$ такие, что $bx' = cs' = n$. Тогда $a/b = (ax')/n$ и $c/d = n/(ds')$ и полагаем $(a/b) \cdot (c/d) = (ax')/(ds')$.

Непосредственно проверяются корректность введённых операций, независимость результата от выбора вспомогательных элементов s_1, s_2, r', s', а также выполнение аксиом кольца для Q. После этого остаётся проверить, что Q — правое классическое кольцо частных кольца R. Для этого заметим, что $(0, b) \sim (0, 1) \not\sim (a, b)$ для любых $b \in S$, $a \in R \setminus \{0\}$, поэтому отображение $r \mapsto r/1$ — вложение кольца R в кольцо Q. Отождествляя $r \in R$ с дробью $r/1$, получаем, что $R \subseteq Q$, $s(1/s) = (1/s)s = 1/1$ для любого $s \in S$, откуда $1/s = s^{-1}$ и $a/b = (a/1)(1/b) = ab^{-1}$ для любой дроби $a/b \in Q$. □

Левое и правое классические кольца частных кольца R, которое удовлетворяет одновременно левому и правому условиям Ope, можно отождествить (без доказательства).

Если кольцо R — это область, тогда в R все ненулевые элементы являются регулярными, поэтому правое условие Ope принимает вид $aR \cap bR \neq 0$ при $a, b \neq 0$.

Определение 8.15. Область называется *областью Ope*, если в ней любые два ненулевых главных правых идеала имеют ненулевое пересечение.

Следствие 8.16. Кольцо R является правой областью Ope тогда и только тогда, когда R обладает правым классическим кольцом частных, которое является телом.

Предложение 8.17. Правые и левые аннуляторы в любом кольце R обладают следующими свойствами:
1) Если $S_1 \subseteq S_2 \subseteq R$, то $l(S_1) \supseteq l(S_2)$ и $r(S_1) \supseteq r(S_2)$;
2) Если $S \subseteq R$, то $S \subseteq r(l(S))$ и $S \subseteq l(r(S))$;
3) Если $S \subseteq R$, то $r(S) = r(l(r(S)))$ и $l(S) = l(r(l(S)))$ (формула тройного аннулятора);
4) Если $S_1, S_2 \subseteq R$, то $l(S_1) \cap l(S_2) = l(S_1 \cup S_2)$ и $r(S_1) \cap r(S_2) = r(S_1 \cup S_2)$.

Доказательство. Действительно, если $s \in S$, $r \in r(S)$, то $sr = 0$, что доказывает первое утверждение. Если $r \in r(S)$, $l \in l(r(S))$, то $rl = 0$ и $r \in r(l(r(S)))$; обратное включение следует из первого утверждения. □

Пусть $l(S_1) \supseteq l(S_2) \supseteq \ldots \supseteq l(S_n)$ — *убывающая* цепочка *левых* аннуляторов. Если применить к ней операцию взятия *правого* аннулятора, а затем снова *левого* аннулятора, то получится исходная цепочка. Поэтому условия обрыва *возрастающих* цепочек *правых* аннуляторов и *убывающих* цепочек *левых* аннуляторов эквивалентны.

Лемма 8.18. Пусть полупервичное кольцо R удовлетворяет условию обрыва возрастающих цепочек правых аннуляторов. Рассмотрим его правые идеалы $I \supseteq J$, для которых $l(I) \neq l(J)$. Тогда существует такое $v \in I$, что $vI \neq 0$, $vI \cap J = 0$.

Доказательство. Как отмечалось выше, кольцо R будет удовлетворять условию обрыва *убывающих* цепочек *левых* аннуляторов. Поэтому упорядоченное по включению множество всех левых аннуляторов U, для которых $l(I) \subsetneq U \subseteq l(J)$, содержит некоторый минимальный элемент K. Множество KI как произведение левого идеала на правый является двусторонним идеалом, который не равен 0, поскольку $l(I) \neq K$.

В силу полупервичности идеал KI не нильпотентен, в частности, $(KI)^2 \neq 0$, откуда существует элемент $v = ik \in IK$, для которого $KvI \neq 0$, поэтому и $vI \neq 0$.

Покажем, что $vI \cap J = 0$. Рассмотрим произвольный элемент $vx \in vI \cap J$, $x \in I$. Имеем $l(x) \supseteq l(I)$. Пересечение двух левых аннуляторов $l(x) \cap K$ — также левый аннулятор (для объединения соответствующих множеств), он лежит в $l(J)$ и содержит $l(I)$, причём строго. Действительно, так как $vx \in J$, то по определению K имеем $Kvx = 0$, то есть $Kv \subseteq l(x) \cap K$, при этом $KvI \neq 0$, поэтому $Kv \not\subseteq l(I)$.

Итак, $l(I) \subsetneq (l(x) \cap K) \subseteq K \subseteq l(J)$. Из минимальности K следует, что $K \subseteq l(x)$, то есть $Kx = 0$ и $vx = ikx = 0$. Отсюда получаем требуемое соотношение $vI \cap J = 0$. □

Отметим, что в предыдущей лемме правый идеал vI всегда содержится в I в силу того, что $v \in I$.

Определение 8.19. Правый идеал $I \leqslant R_R$ называется *существенным (большим)*, если его пересечение с любым ненулевым правым идеалом кольца R отлично от нуля.

Следствие 8.20. Пусть полупервичное кольцо R удовлетворяет условию обрыва возрастающих цепочек правых аннуляторов, а xR, yR — его существенные правые идеалы. Тогда правый идеал xyR также существенный.

Доказательство. Пусть $0 \neq A$ — некоторый правый идеал в R. Требуется доказать, что $A \cap xyR \neq 0$. Заметим, что множество $I = \{t \in R \mid xt \in A\}$ — это правый идеал. Положим также $J = r(x)$. Чтобы применить лемму, надо показать, что $l(I) \neq l(J)$. С одной стороны, элемент $x \notin l(I)$, так как $xI = xR \cap A \neq 0$ ввиду существенности xR. С другой стороны, $l(J) = l(r(x)) \ni x$. Тогда, применяя лемму к I и $J = r(x)$, выберем элемент $v \in I$ такой, что для правого идеала $0 \neq T = vI \subseteq I$ выполнено $T \cap r(x) = 0$.

Теперь рассмотрим правый идеал $L = \{r \in R \mid yr \in T\}$. Так как yR — существенный правый идеал, то $yL = yR \cap T \neq 0$. В силу того, что $yL \subseteq T$ и $T \cap r(x) = 0$, имеем $xyL \neq 0$. Затем, используя включение $T \subseteq I$, можно показать, что $0 \neq xyL \subseteq xT \subseteq xI \subseteq A$. Отсюда заключаем, что пересечение $A \cap xyR$ не равно нулю, т.к. оно содержит $xyL \neq 0$. □

Следствие 8.21. Пусть полупервичное кольцо R удовлетворяет условию обрыва возрастающих цепочек правых аннуляторов, aR — его существенный правый идеал. Тогда a регулярен, т.е. не является делителем нуля.

Доказательство. Рассмотрим правые идеалы $I = R$, $J = aR$. Так как $l(R) = 0$, при $l(aR) \neq 0$ была бы применима лемма, строящая тривиально пересекающий aR ненулевой правый идеал. Это невозможно в силу существенности aR. Значит, $l(a) = l(aR) = 0$.

По предыдущему следствию вместе с aR существенны и все правые идеалы a^2R, …, a^kR, … Теперь рассмотрим возрастающую цепочку $r(a) \subseteq r(a^2) \subseteq \ldots$, пусть $r(a^n) = r(a^{n+1})$. Пусть $x \in a^nR \cap r(a)$. Тогда $x = a^ny$, $0 = ax = a^{n+1}y$, то есть $y \in r(a^{n+1}) = r(a^n)$ и $x = 0$. Поэтому $a^nR \cap r(a) = 0$, откуда $r(a) = 0$ в силу существенности a^nR. □

Определение 8.22. *R — правое кольцо Голди*, если R удовлетворяет условию обрыва возрастающих цепочек правых аннуляторов (всякая цепочка $r(S_1) \subseteq r(S_2) \subseteq \ldots$ стабилизируется) и R_R не содержит бесконечных прямых сумм ненулевых правых идеалов.

Пример 8.23.

- Всякое нётерово справа кольцо является правым кольцом Голди.
- Правая область Оре является правым кольцом Голди. Действительно, в области все аннуляторы нулевые. Любые два правых идеала содержат какие-то два главных идеала, которые обязательно пересекаются, поэтому прямой суммы быть не может.

- Коммутативная область — правое и левое кольцо Голди как частный случай предыдущего примера.

Лемма 8.24. Пусть R — полупервичное правое кольцо Голди, $c \in R$, $r(c) = 0$. Тогда cR существенный, а значит, c регулярен.

Доказательство. Пусть $I \cap cR = 0$, где I — правый идеал. От противного, предположим, что $I \neq 0$. Рассмотрим правые идеалы $c^n I$, $n \geqslant 0$. Так как R — правое кольцо Голди, то их сумма не может быть прямой. Выберем наименьшее n, для которого выполнено $c^n i_n + \ldots + ci_1 + i_0 = 0$ при некоторых $i_j \in I$. Отметим, что I — правый идеал, но необязательно левый, поэтому произведения $c^k i_k$, $k \geqslant 1$ могут и не лежать в I.

Сумма всех слагаемых, кроме i_0, равна $-i_0$, а значит, лежит в $I \cap cR = 0$, поэтому $i_0 = 0$. Кроме того, $c(c^{n-1} i_n + \ldots + i_1) = 0$, откуда $c^{n-1} i_n + \ldots + i_1 = 0$, поскольку $r(c) = 0$ по условию. Получаем противоречие с минимальностью n. Значит, $I = 0$. $\square$

Отметим, что если в *правом* полупервичном кольце Голди у некоторого элемента равен нулю его *левый* аннулятор, то такой элемент не обязан быть регулярным.

Лемма 8.25. Пусть R — полупервичное правое кольцо Голди, I — его существенный правый идеал. Тогда в I содержится регулярный элемент.

Доказательство. Ранее мы доказали, что если полупервичное кольцо удовлетворяет условию обрыва возрастающих цепей правых аннуляторов, то в таком кольце нет ненулевых односторонних нильидеалов (предложение 8.5).

Сначала покажем, что каждый ненулевой правый идеал J нашего кольца R содержит элемент x, который не является нильпотентом, и при этом $r(x) = r(x^2)$. Рассмотрим семейство аннуляторов

$$\Omega = \{r(x) \mid x \in J,\ x^n \neq 0 \ \ \forall n \in \mathbb{N}\},$$

упорядоченное по включению. Так как J не правый нильидеал, то Ω непусто. По условию Голди и лемме Цорна в Ω есть некоторый максимальный элемент $r(x)$. Соотношение $r(x) \subseteq r(x^2)$ выполнено всегда, но строгое включение противоречило бы максимальности $r(x)$, значит, $r(x) = r(x^2)$.

Будем доказывать лемму от противного: предположим, что в существенном правом идеале I нет регулярных элементов. В силу предыдущей леммы это значит, что правый аннулятор каждого $a \in I$ отличен от нуля. Далее будем индуктивно строить бесконечную последовательность ненулевых элементов $a_1, a_2, \ldots$, таких что
1) $r(a_i) = r(a_i^2)$;
2) если $i < j$, то $a_i a_j = 0$;
3) сумма правых идеалов $a_1 R \oplus \ldots \oplus a_n R$ является прямой для всех n.
База индукции $n = 1$ доказана ранее, достаточно положить $J = I$.

Пусть теперь построены элементы $a_1, \ldots, a_n$. Положим $b = a_1 + \ldots + a_n$. Так как сумма $a_1R \oplus \ldots \oplus a_nR$ прямая, то $b \neq 0$, а также $r(b) = \bigcap\limits_{i=1}^{n} r(a_i) \neq 0$. Рассмотрим правый идеал $J = r(b) \cap I$, он не равен нулю в силу существенности I. Тогда в силу предыдущего в J тоже имеется ненильпотентный элемент a_{n+1}, такой что $r(a_{n+1}) = r(a_{n+1}^2)$. Так как $a_{n+1} \in J \subseteq r(b) = \bigcap\limits_{i=1}^{n} r(a_i)$, то выполнено $a_i a_{n+1} = 0$ при $i \leqslant n$.

Осталось доказать, что новое слагаемое $a_{n+1}R$ имеет нулевое пересечение с суммой $a_1R \oplus \ldots a_nR$. Пусть $y \in (a_1R \oplus \ldots a_nR) \cap a_{n+1}R$. Тогда $y = a_{n+1}z = \sum\limits_{i=1}^{n} a_i z_i$ для некоторых $z, z_i \in R$. Умножим это равенство на a_1 слева, тогда в силу пункта 2) получаем $0 = a_1 a_{n+1} z = a_1^2 z_1$, откуда $z_1 \in r(a_1^2) = r(a_1)$ и $a_1 z_1 = 0$. Аналогично умножаем далее на $a_2, a_3, \ldots, a_n$ (строго в этом порядке) и получаем, что $0 = a_2 z_2 = \ldots = a_n z_n$. Значит, $y = 0$ и сумма $a_1R \oplus \ldots \oplus a_{n+1}R$ действительно прямая.

Построена бесконечная прямая сумма правых идеалов $\bigoplus\limits_{i \in \mathbb{N}} a_i R \subseteq R$, что противоречит условию Голди. Поэтому в I обязан найтись регулярный элемент. □

Теорема 8.26. У полупервичного правого кольца Голди R есть правое классическое кольцо частных Q.

Доказательство. Достаточно показать, что кольцо R удовлетворяет правому условию Оре. Если $a \in R$, $b \in S(R)$, то правый идеал bR существенный по одной из предыдущих лемм. Тогда и правый идеал $I = \{u \in R \mid au \in bR\}$ также окажется существенным. Действительно, для правого идеала J равенство $I \cap J = 0$ означает $aJ \cap bR = 0$, поэтому $aJ = 0$ ввиду существенности bR, но тогда заведомо $aJ \subseteq bR$ и $I \cap J = J$, откуда $J = 0$, а значит, I существенный.

В силу предыдущей леммы I содержит регулярный элемент c. Из определения идеала I получаем, что при некотором $t \in R$ выполнено $ac = bt$. □

Лемма 8.27. Пусть R — правое кольцо Оре, $S = S(R)$. Если $I \leqslant R_R$ — правый идеал, то $IS^{-1} = \{xs^{-1} \colon x \in I, s \in S\}$ — правый идеал в RS^{-1}. Если $I_1 \oplus \ldots \oplus I_n$ — прямая сумма правых идеалов R, то сумма $I_1S^{-1} + \ldots + I_nS^{-1}$ правых идеалов RS^{-1} также прямая.

Доказательство. Следует из леммы о приведении к общему знаменателю. Для всякой пары дробей a/b, c/d в RS^{-1} существуют регулярные элементы k, m, для которых $bk = dm = s$. Тогда $a/b = ak/s$, $c/d = cm/s$. □

Лемма 8.28. Пусть R — правое кольцо Оре, $S = S(R)$. Если I — правый идеал RS^{-1}, то $I \cap R$ — правый идеал R, для которого $(I \cap R)S^{-1} = (I \cap R)(RS^{-1})$. Если $I_1 \oplus \ldots \oplus I_n$ — прямая сумма правых идеалов RS^{-1}, то сумма $(I_1 \cap R) + \ldots + (I_n \cap R)$ правых идеалов R также прямая.

Доказательство. Если $x = ab^{-1} \in I$, то $a = xb \subseteq I \cap R$, и $x \in (I \cap R)S^{-1}$. □

Лемма 8.29. Полупервичное правое кольцо Голди R удовлетворяет и условию обрыва *убывающих* цепочек правых аннуляторов.

Доказательство. Пусть $L_1 \supset L_2 \ldots \supset L_n \supset \ldots$ — строго убывающая цепочка правых аннуляторов. Тогда $l(L_i)$ образуют строго *возрастающую* цепочку *левых* аннуляторов, и по лемме о правых идеалах с раличными левыми аннуляторами (лемма 8.18) в каждом L_i существует правый идеал C_i, пересекающий L_{i+1} по 0. Тогда сумма всех C_i прямая, противоречие. □

Замечание 8.30. Пусть e — идемпотент кольца R. Тогда $r(e) = (1-e)R$, $l(e) = R(1-e)$. Действительно, включение $r(e) \supseteq (1-e)R$ тривиально ввиду $e(1-e) = 0$. Обратно, если $ea = 0$, тогда $(1-e)a = a$, откуда $a \in (1-e)R$. Для левого аннулятора проверки такие же.

Теорема 8.31 (Голди)**.** Правое классическое кольцо частных Q полупервичного правого кольца Голди R полупросто.

Доказательство. Пусть I — произвольный правый идеал в Q. Тогда $I_1 = I \cap R$ — правый идеал в кольце R. По правому условию Голди в R_R найдётся такая прямая сумма правых идеалов $J = I_1 \oplus I_2 \oplus \ldots \oplus I_n$, содержащая I_1, что к ней нельзя добавить ещё одно ненулевое слагаемое. Тогда правый идеал J должен нетривиально пересекаться со всеми ненулевыми правыми идеалами R, т.е. быть существенным. Следовательно, J содержит некоторый регулярный элемент кольца R. Такой элемент будет обратим в кольце Q, тогда, полагая $P = I_2 \oplus \ldots \oplus I_n$, получим $Q = JQ = (I_1 \oplus P)Q = I \oplus PQ$. Вспомним, что такое разложение регулярного модуля в прямую сумму соответствует наличию в Q идемпотента e, для которого $I = eQ$, $PQ = (1-e)Q$.

Отсюда получаем, что всякий правый идеал Q является главным, в частности, он конечно порожден, откуда Q нётерово справа. Следовательно Q — правое кольцо Голди. Заметим, что Q к тому же полупервично: ни один ненулевой правый идеал не может быть нильпотентен, так как содержит порождающий его ненулевой идемпотент.

Пусть e — идемпотент, порождающий правый идеал I, т.е. $I = eQ$, $e^2 = e$. Тогда, учитывая замечание перед теоремой, можно записать $I = eQ = r(1-e) = r((1-e)Q)$. В силу произольности I получаем, что всякий правый идеал кольца Q является правым аннулятором. По предыдущей лемме Q удовлетворяет условию обрыва убывающих цепочек правых аннуляторов. Следовательно Q артиново справа и полупервично, а значит, полупросто.

□

Теорема 8.32 (обращение теоремы Голди)**.** Пусть Q — правое кольцо частных для кольца R. Если Q полупросто, то R — полупервичное правое кольцо Голди. Если Q дополнительно является простым кольцом, то R первично.

Без доказательства. □

Определение 8.33. Пусть Q — кольцо, его *правым порядком* P будем называть аддитивную подгруппу, замкнутую относительно умножения, такую что любой элемент $q \in Q$ может быть представлен в виде $q = ab^{-1}$, где $a, b \in P$.

Отметим, что в определении элемент b^{-1} не обязан лежать в P, т.е. b обратим в Q, но необязательно в P.

Пример 8.34.

- Если Q — правое кольцо частных для R, то R — правый порядок в кольце Q.
- Для любого $n \in \mathbb{Z}$ множество $n\mathbb{Z}$ является двусторонним порядком в $\mathbb{Q}$: любое рациональное число a/b может быть записано в виде na/nb.
- Множество $P = \left(\begin{smallmatrix} 2\mathbb{Z} & 3\mathbb{Z} \\ 6\mathbb{Z} & 3\mathbb{Z} \end{smallmatrix}\right)$ — двусторонний порядок в $M_2(\mathbb{Q})$. Действительно, для матрицы A из $M_2(\mathbb{Q})$ положим d равным наименьшему общему кратному знаменателей всех элементов, при этом скалярная матрица $6dE = \left(\begin{smallmatrix} 6d & 0 \\ 0 & 6d \end{smallmatrix}\right)$ лежит в P, тогда $A = (6dA)(6dE)^{-1}$.

Правое кольцо частных Q также может быть определено и в случае, когда исходное кольцо R не содержало единицы. Тем не менее Q, разумеется, должно обладать единицей — иначе бессмысленно говорить об обратимых элементах.

В этих терминах, если P — правый порядок в Q, то P в общем случае является кольцом без единицы, тогда Q — его правое классическое кольцо частных.

Часть предыдущих результатов переносится на кольца без единицы практически с теми же доказательствами, но в ряде случаев требуются модификации.

Теорема 8.35 (Фейт, Утуми)**.** Пусть P — правый порядок в полупростом кольце $Q = M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$, где D_i — тела. Тогда P содержит подмножество $M_{n_1}(F_1) \times \ldots \times M_{n_k}(F_k)$, где F_i — некоторые правые порядки в D_i.

Без доказательства. □

Отметим, что в теореме Фейта — Утуми множество $M_{n_1}(F_1) \times \ldots \times M_{n_k}(F_k)$ может и не содержать единицу 1_Q кольца Q даже в ситуации $1_Q \in P$. Например, рассмотрим упомянутый в начале лекции порядок $P = \{(a, b) : a \equiv b \pmod 7\} \subseteq \mathbb{Z} \times \mathbb{Z}$ в полупростом кольце $\mathbb{Q} \times \mathbb{Q}$. Можно показать, что для любых порядков F_1, F_2 в $\mathbb{Q}$ таких, что $F_1 \times F_2 \subseteq P$, будет заведомо выполнено $(1, 1) \notin F_1 \times F_2$. Хотя при этом очевидно $(1, 1) \in P$.

Задачи к лекции 9.

Задача 1. Докажите, что $M_n(\mathbb{Q})$ — двустороннее классическое кольцо частных для $M_n(\mathbb{Z})$.

Задача 2. Докажите, что $\mathbb{Q}\times\mathbb{Q}$ является классическим кольцом частных для кольца $R = \{(a,b)\colon a \equiv b \pmod 7\} \subseteq \mathbb{Z}\times\mathbb{Z}$. Покажите, что для любых порядков F_1, F_2 в $\mathbb{Q}$ таких, что $F_1 \times F_2 \subseteq P$, будет заведомо выполнено $(1,1) \notin F_1 \times F_2$.

Задача 3. Пусть $\mathbb{F}$ — поле, а отображение $\sigma\colon \mathbb{F} \to \mathbb{F}$ — инъективный кольцевой эндоморфизм, не являющийся автоморфизмом. Пусть множество $\mathbb{F}[x;\sigma]$ состоит из всех конечных формальных линейных комбинаций вида $\{\sum f_i x^i\}$, где $f_i \in \mathbb{F}$, а x — новая переменная, для которой по определению полагаем $xf = \sigma(f)x$ при всех $f \in \mathbb{F}$. Это позволяет определить операцию умножения (некоммутативную) на всём множестве $\mathbb{F}[x;\sigma]$.

1) Докажите, что $\mathbb{F}[x;\sigma]$ является кольцом.

2) Докажите, что в $\mathbb{F}[x;\sigma]$ нет делителей нуля.

3) Постройте пример такого отображения σ для случая $\mathbb{F} = \mathbb{C}(t)$ — поля формальных многочленов Лорана (сумм вида $\sum\limits_{k=-n}^{\infty} c_k t^k$). Обозначим получившееся кольцо $\mathbb{F}[x;\sigma]$ за Σ.

Задача 4. Докажите, что кольцо Σ из предыдущей задачи не удовлетворяет правому условию Оре.

Задача 5. Пусть R — область, в которой все конечнопорождённые правые идеалы главные. Докажите, что тогда R — правая область Оре. Указание: рассмотрите порождающий элемент суммы двух правых главных идеалов.

Задача 6. Покажите, что если R — первичное правое кольцо Голди, то его классическое правое кольцо частных — простое кольцо.

Задача 7. Приведите пример полупервичного правого кольца Голди, которое не является нётеровым справа.

Лекция 10. Расширения Оре. Обобщенная теорема Гильберта о базисе. Теоремы коммутативности

9 Расширения Оре. Обобщенная теорема Гильберта о базисе.

В стандартной конструкции кольца многочленов $R[x]$, перменная x коммутирует с элементами кольца R. Однако от этого условия можно отказаться. Мы построим кольцо *косых многочленов*, в котором для $r \in R$ произведения rx и xr, вообще говоря, могут быть различны. Тем не менее, хотелось бы сохранить аналогию с обычными многочленами, поэтому мы будем требовать выполнения трёх условий:

0) $1 \cdot x = x \cdot 1$, этот элемент традиционно будем записывать просто как x.

1) каждый косой многочлен может быть преобразован к виду $\sum x^i r_i$, где коэффициенты r_i определены однозначно;

2) для любых двух косых многочленов f, g выполнено $\deg fg \leqslant \deg f + \deg g$.

Требовать равенства в пункте 2) — слишком сильное условие, так как коэффициенты при старших степенях f, g могут в произведении дать ноль. Форму записи косого многочлена из пункта 1) назовём представлением в виде *правого многочлена* от x.

Найдём, как свзязаны между собой произведения rx и xr. Согласно 2) многочлен rx должен иметь степень 1, т.е. $rx \in xR + R$, тогда можно записать

$$rx = x\sigma(r) + \delta(r),$$

где σ, δ — какие-то отображения кольца R в себя. Складывая два таких разложения для $r_1 x$ и $r_2 x$, получаем, что $\sigma(r_1 + r_2) = \sigma(r_1) + \sigma(r_2)$, а также $\delta(r_1 + r_2) = \delta(r_1) + \delta(r_2)$. Значит, σ, δ — это некоторые эндоморфизмы (гомоморфизмы в себя) аддитивной группы кольца $(R, +)$.

Теперь рассмотрим моном $(rs)x$ для $r, s \in R$. С одной стороны, имеем $(rs)x = x\sigma(rs) + \delta(rs)$. С другой стороны, это же выражение можно переписать как $r(sx) = r(x\sigma(s) + \delta(s)) = x\sigma(r)\sigma(s) + \delta(r)\sigma(s) + r\delta(s)$, откуда получаем

$$\sigma(rs) = \sigma(r)\sigma(s), \quad \delta(rs) = \delta(r)\sigma(s) + r\delta(s).$$

В силу $1 \cdot x = x \cdot 1$ выполнено $\sigma(1) = 1$. Таким образом, σ — это энодоморфизм кольца R, тогда как δ является отображением следующего вида.

Определение 9.1. Пусть σ — это (унитальный) эндоморфизм кольца R. Тогда отображение $\delta : R \to R$ называется *правым σ-дифференцированием*, или *правым косым дифференцированием* на R, если δ — эндоморфизм аддитивной группы кольца $(R, +)$, удовлетворяющий «обобщённому тождеству Лейбница»:

$$\delta(rs) = \delta(r)\sigma(s) + r\delta(s), \quad \forall r, s \in R.$$

Отметим, что порядок множителей в формуле важен, так как кольцо R может быть некоммутативным. В случае, когда σ — тождественный эндоморфизм, обобщенное тождестве Лейбница переходит в обычное.

Замечание 9.2. Из определения дифференцирования сразу получаем, что $\delta(1) = 0$.

Если бы мы использовали в условии 1) левые многочлены вместо правых, то в итоге получили бы левое дифференцирование, т.е. $\delta(rs) = \sigma(r)\delta(s) + \delta(r)s$. Далее слово «дифференцирование» всегда будет означать правое дифференцирование, если не оговорено обратного.

Пример 9.3. Рассмотрим множество всех вещественных гладких функций $C^\infty(\mathbb{R})$ на прямой. Тогда $C^\infty(\mathbb{R})$ является кольцом относительно операций поточеченого умножения и сложения. Стандартная производная является дифференцированием в этом кольце и в чисто алгебраическом смысле.

Пример 9.4. Пусть $\mathbb{F}$ — поле, $R = \mathbb{F}[y]$ — алгебра обычных многочленов над полем, σ — любой эндоморфизм R, тождественный на k. Зафиксируем произвольный многочлен $h \in \mathbb{F}[y]$. Найдём все σ-дифференцирования δ, такие что $\delta(y) = h$, $\delta\Big|_{\mathbb{F}} \equiv 0$.

Так как δ должно обращаться в ноль на всех элементах поля, то для любого скаляра $\lambda \in \mathbb{F}$ и любого мнгочлена $f \in \mathbb{F}[y]$ имеем $\delta(\lambda f) = \delta(\lambda)\sigma(f) + \lambda\delta(f) = \lambda\delta(f)$, откуда δ обязано быть $\mathbb{F}$-линейным отображением.

Найдем значения δ от мономов y^n. По индукции проверяется, что при $\sigma(y) \neq y$ выполнено

$$\begin{aligned}\delta(y^n) = \delta(y^{n-1} \cdot y) = \delta(y^{n-1})\sigma(y) + y^{n-1}h = (\delta(y^{n-2})\sigma(y) + y^{n-2}h)\sigma(y) + y^{n-1}h = \\ = \delta(y^{n-2})\sigma(y)^2 + y^{n-2}\sigma(y)h + y^{n-1}h = \ldots = \\ = (\sigma(y)^{n-1} + y\sigma(y)^{n-2} + \ldots + y^{n-2}\sigma(y) + y^{n-1})h = \frac{\sigma(y)^n - y^n}{\sigma(y) - y}h\end{aligned}$$

Для удобства мы вышли в поле рациональных функций $\mathbb{F}(y)$, но по-прежнему δ отображает $\mathbb{F}[y]$ в $\mathbb{F}[y]$. Если же $\sigma(y) = y$, то аналогично $\delta(y^n) = ny^{n-1}h$. Тогда для произвольного многочлена $f = \sum\limits_i a_i y^i \in \mathbb{F}[y]$ имеем в силу линейности $\delta(f) = \sum\limits_i a_i\delta(y^i)$. Пользуясь тем, что σ — эндоморфизм кольца $\mathbb{F}[y]$ и $\sigma\Big|_{\mathbb{F}} = \mathrm{id}$, окончательно получаем

$$\delta(f) = \begin{cases} \dfrac{\sigma(f) - f}{\sigma(y) - y}h, & \text{если } \sigma(y) \neq y; \\ \\ (\sum\limits_i i a_i y^{i-1})h, & \text{если } \sigma(y) = y. \end{cases}$$

Мы нашли единственный возможный вид σ-дифференцирования δ со свойствами $\delta(y) = h$, $\delta\Big|_{\mathbb{F}} \equiv 0$. Обратно, если определить δ по формуле выше, то непосредственно проверяется, что выполнено обобщенное тождество Лейбница и остальные условия.

Рассмотрим два частных случая:

1) При $\sigma = \mathrm{id}$, $h \equiv 1$, получаем обычную формальную производную на многочленах.

2) Пусть $q \in \mathbb{F} \setminus \{0\}$, положим $\sigma(f) = f(qy)$, $h \equiv 1$. В этом случае δ называют *q-дифференциальным оператором*, или *производной Эйлера.*

Пример 9.5. Пусть R — некоммутативное кольцо, для любого $x \in R$ зададим *внутреннее дифференцирование* $D_x : R \to R$ по правилу $D_x(r) = [x, r] = xr - rx$ для всех

$r \in R$. Эту конструкцию можно немного обобщить. Если σ — произвольный эндоморфизм кольца, тогда $D_{x,\sigma}(r) = x\sigma(r) - rx$ окажется правым σ-дифференцированием, его называют *внутренним σ-дифференцированием*. Все дифференцирования, не являющиеся внутренними, будем называть *внешними*.

Теперь необходимо дать формальное определение кольца косых многочленов и показать, что оно действительно существует.

Определение 9.6. Пусть R — кольцо, σ — его (унитальный) гоморфизм, δ — правое σ-дифференцирование. Кольцо $S = R[x; \sigma, \delta]$ называется (правым) *расширением Оре* кольца R, или кольцом *косых многочленов*[9], если выполнены следующие условия:

а) S содержит кольцо R (или его изоморфную копию) в качестве подкольца.

б) S содержит такой элемент x, что S является свободным правым R-модулем с базисом $\{1, x, x^2, \ldots\}$.

в) для всех $r \in R$ выполнено $rx = x\sigma(r) + \delta(r)$.

Заметим, что из определения сразу получаем условия 0), 1), упомянутые ранее. Условие 2) докажем чуть позже.

Если σ тождественно и при этом $\delta \equiv 0$, то расширение Оре становится обычным кольцом многочленов. Отметим, что часто рассматриваются случаи, когда выполнено только одно из этих условий. Так, в ситуации $\sigma = \mathrm{id}$ говорят о *дифференциальном кольце многочленов* $R[x, \delta]$. Если же $\delta \equiv 0$, то часто используется обозначение $R[x; \sigma]$, это кольцо называют кольцом *скрученных многочленов*[10].

Замечание 9.7. Симметрично можно определить «левое» расширение Оре, если взять левое дифференцирование δ, левый модуль в пункте б) и соотношение $xr = \sigma(r)x + \delta(r)$ в пункте в). В этом случае любой косой многочлен можно записать в виде *левого многочлена*. Вообще говоря, левое расширение Оре может не являться правым, и наоборот. Однако если σ — биективно, то левое расширение Оре для σ, δ — это в точности правое расширение Оре вида $R[x; \sigma^{-1}, -\delta\sigma^{-1}]$.

Теорема 9.8 (Существование)**.** Пусть R — кольцо, σ — его (унитальный) гомоморфизм, δ — правое σ-дифференцирование. Тогда расширение Оре $R[x; \sigma, \delta]$ существует.

Доказательство. Пусть M — множество бесконечных последовательностей $(r_i)_{i=0}^{\infty}$ элементов кольца R. На M стандартным образом зададим структуру правого R-модуля, полагая $(r_i) \cdot r = (r_i r)$, а также $(r_i) + (s_i) = (r_i + s_i)$. В то же время можно понимать M как левый $\mathbb{Z}$-модуль. Пусть E — кольцо эндоморфизмов M как левого $\mathbb{Z}$-модуля. Напомним, что так как модуль левый, то по нашему соглашению эндоморфизмы будут записываться справа от элементов модуля M.

[9] В англоязычной литературе — skew polynomials.

[10] В англоязычной литературе — twisted polynomials.

Зададим отображение из R в E по правилу $r \mapsto \lambda_r$, где $(m)\lambda_r = mr$ для всех $m \in M$. Тогда $\lambda_r + \lambda_s = \lambda_{r+s}$, $\lambda_r\lambda_s = \lambda_{rs}$, $\lambda_1 = \mathrm{id}$. Кроме того, если $(m)\lambda_r = 0$ для всех $m \in M$, то, полагая $m = (1, 0, 0, \ldots)$, получаем $r = 0$. Итак, мы построили инъективный гомоморфизм из R в E. Без ограничения общности можно считать, что $R \subseteq E$, вместо λ_r будем писать просто r.

Рассмотрим в E эндоморфизм x, действующий по правилу $(r_i)x = (\sigma(r_{i-1}) + \delta(r_i))$, где формально полагаем $r_{-1} = 0$. Рассмотрим в E подкольцо S, состоящее из сумм всех возможных произведений элементов множества $R \cup \{x\}$. Покажем, что S — искомое расширение Оре. Условие а) выполнено по построению. Проверим в). Для произвольной последовательности $(r_i) \in M$ имеем

$$(r_i)(rx) = (r_ir)(x) = (\sigma(r_{i-1}r) + \delta(r_ir)) = (\sigma(r_{i-1})\sigma(r) + \delta(r_i)\sigma(r) + r_i\delta(r)) =$$
$$(\sigma(r_{i-1}) + \delta(r_i))\sigma(r) + (r_i)\delta(r) = (r_i)(x\sigma(r)) + (r_i)\delta(r) = (r_i)(x\sigma(r) + \delta(r)),$$

откуда $rx = x\sigma(r) + \delta(r)$.

Перейдем к пункту б). Заметим, что из соотношения $rx = x\sigma(r)+\delta(r)$ следует, что $Rx \subseteq xR + R$, откуда по индукции получаем, что $Rx^i \subseteq x^iR + x^{i-1}R + \ldots + xR + R$. Значит, $(Rx^i)(Rx^j) \subseteq x^{i+j}R + \ldots + x^{\min\{i,j\}}R$. При этом по определению кольцо S является суммой всех возможных произведений вида $Rx^{i_1}R \ldots Rx^{i_k}R$. Отсюда $S = R + xR + x^2R + \ldots$, а значит, множество $\{1, x, x^2, \ldots\}$ порождает S как правый R-модуль.

Осталось проверить, что множество $\{1, x, x^2, \ldots\}$ линейно независимо над R. Предположим, что $\xi = a_0 + xa_1 + \ldots + x^na_n$ — нулевой эндоморфизм в E, $a_i \in R$. Пусть $e_i \in M$ — последовательность, в которой i-й член равен единицы, а остальные равны нулю. Заметим, что $(e_0)x^i = e_i$, так как $\sigma(0) = \delta(0) = \delta(1) = 0$, но $\sigma(1) = 1$. Отсюда $(0, 0, \ldots) = (e_0)\xi = (a_0, \ldots, a_n, 0, \ldots)$, откуда все a_i равны нулю. □

Чтобы доказать единственность расширения Оре, нам понадобится следующее свойство.

Предложение 9.9 (Универсальное свойство расширений Оре)**.** Пусть $S = R[x; \sigma, \delta]$ — расширение Оре. Предположим, что даны кольцо T, гомоморфизм $\phi : R \to T$ и элемент $y \in T$ такой, что $\phi(r)y = y\phi(\sigma(r)) + \phi(\delta(r))$ для всех $r \in R$. Тогда существует и притом единственный гомоморфизм $\chi : R[x;, \sigma, \delta] \to T$ такой, что $\chi(x) = y$ и ограничение $\chi\Big|_R = \phi$.

Доказательство. Заметим, что единственность очевидна. Действительно, для любого правого многочлена $\sum_i x^ir_i \in R[x; \sigma, \delta]$ имеем $\chi(\sum_i x^ir_i) = \sum_i y^i\phi(r_i)$, где элемент y и гоморфизм ϕ даны по условию. Для доказательства существования, достаточно проверить, что отображение χ, заданное по предыдущей формуле будет гомоморфизмом колец. По построению χ является гомоморфизмом аддитивных групп, надо

проверить, что χ сохраняет умножение. Пусть $f = \sum\limits_i x^i r_i \in R[x;\sigma,\delta]$, тогда

$$\chi(fx) = \chi(\sum_i x^i r_i x) = \chi(\sum_i x^{i+1}\sigma(r_i) + x^i\delta(r_i)) = \sum_i (y^{i+1}\phi(\sigma(r_i)) + y^i\phi(\delta(r_i))) =$$
$$\sum_i y^i(y\phi(\sigma(r_i)) + \phi(\delta(r_i))) = \sum_i y^i\phi(r_i)y = \chi(f)y.$$

Рассуждая по индукции, получаем $\chi(fx^i) = \chi(f)y^i$ для всех $i \geqslant 0$ и всех $f \in R[x;\sigma,\delta]$. Далее для любого $s \in R$ имеем

$$\chi(fs) = \chi(\sum_i x^i r_i s) = \sum_i y^i\phi(r_i s) = \sum_i y^i\phi(r_i)\phi(s) = \chi(f)\phi(s).$$

В итоге для произвольного $g = \sum\limits_i x^i s_i \in R[x;\sigma,\delta]$ получаем

$$\chi(fg) = \chi(\sum_i f x^i s_i) = \sum_i \chi(f x^i s_i) = \sum_i \chi(f x^i)\phi(s_i) = \sum_i \chi(f) y^i \phi(s_i) = \chi(f)\chi(g).$$

□

Следствие 9.10 (Единственность)**.** Пусть R — кольцо, σ — его (унитальный) гомоморфизм, δ — правое σ-дифференцирование. Предположим, что даны два расширения Оре $S = R[x;\sigma,\delta]$ и $S' = R[x';\sigma,\delta]$. Тогда существует и притом единственный изоморфизм колец $\chi : S \to S'$, такой что $\chi(x) = x'$ и ограничение $\chi\Big|_R$ является тождественным отображением.

Доказательство. Применим универсальное свойство к тождественному вложению $\phi : R \to R[x';\sigma,\delta]$, полагая $y = x'$, получим гомоморфизм $\chi : R[x;\sigma,\delta] \to R[x';\sigma,\delta]$, причем $\chi(x) = x'$, $\chi\Big|_R = \mathrm{id}$. Затем применим универсальное свойство к тождественному вложению $\phi' : R \to R[x;\sigma,\delta]$, теперь $y = x$, получаем гомоморфизм $\chi' : R[x';\sigma,\delta] \to R[x;\sigma,\delta]$, аналогично $\chi'(x') = x$, $\chi'\Big|_R = \mathrm{id}$. Тогда композиция $\chi'\chi$ оставляет x на месте, значит, является тождественным отображением на $R[x;\sigma,\delta]$. Точно также $\chi'\chi$ сохраняет x', поэтому она тождественна на $R[x';\sigma,\delta]$. Мы показали, что χ — искомый изоморфизм. Единственность следует из единственности χ в универсальном свойстве. □

Пример 9.11. Пусть $R = \mathbb{C}$ — поле комплексных чисел, определим автоморфизм σ как комплексное сопряжение $\sigma(a) = \overline{a}$. Тогда в кольце $\mathbb{C}[x;\sigma]$ для любого $a \in \mathbb{C}$ выполнено $ax = x\overline{a}$. Центр кольца $\mathbb{C}[x;\sigma]$ совпадает с $\mathbb{R}[x^2]$. Можно показать, что факторкольцо $\mathbb{C}[x;\sigma]/(x^2+1)$ изоморфно телу кватернионов, роль мнимых единиц i, j, k в нём будут играть i, x, ix.

Пример 9.12. Пусть $R = \mathbb{F}$ — поле ненулевой характеристики p, положим σ равным *эндоморфизму Фробениуса*, т.е. $\sigma(a) = a^p$. Тогда в кольце $\mathbb{F}[x;\sigma]$ для любого $a \in \mathbb{F}$ выполнено $ax = xa^p$. Так как $\mathbb{F}$ — поле, то σ автоматически инъективен. Однако σ необязательно сюръективен, например, рассмотрим поле рациональных функций $\mathbb{F} = \mathbb{F}_p(t)$ над полем $\mathbb{F}_p$ вычетов по модулю p.

Пример 9.13. Пусть $\mathbb{F}$ — поле, $q \in \mathbb{F} \setminus \{0, 1\}$. Определим *координатное кольцо квантовой плоскости* Q как фактор свободной алгебры $\mathbb{F}\langle x, y\rangle$ по идеалу, порождённому элементом $xy - qyx$. Можно получить алгебру Q как расширение Оре. Положим $R = \mathbb{F}[y]$. В кольце R рассмотрим автороморфизм $\sigma(f) = f(qy)$. Тогда $Q \cong R[x;\sigma]$.

Пример 9.14. Первая алгебра Вейля $A_1(\mathbb{F}) = \mathbb{F}\langle x, y\rangle / (xy - yx - 1)$, может быть построена как расширение Оре. Положим $R = \mathbb{F}[y]$, тогда $A_1(\mathbb{F}) \cong R[x, d/dy]$.

Пример 9.15. Пусть $\mathbb{F}$ — поле, $q \in \mathbb{F} \setminus \{0, 1\}$. Определим *первую квантовую алгебру Вейля* $A_1^q(\mathbb{F})$ как фактор свободной алгебры $\mathbb{F}\langle x, y\rangle$ по идеалу, порождённому элементом $xy - qyx - 1$. Можно получить алгебру $A_1^q(\mathbb{F})$ как расширение Оре. Положим $R = \mathbb{F}[y]$. В кольце R рассмотрим автороморфизм $\sigma(f) = f(qy)$. Тогда $A_1^q(\mathbb{F}) \cong R[x;\sigma,\delta]$, где δ — производная Эйлера, см. пример ранее.

Определение 9.16. Пусть $f \in R[x;\sigma,\delta]$, $f \not\equiv 0$. Так как множество $\{1, x, x^2, \ldots\}$ — это базис $R[x;\sigma,\delta]$ как свободного правого R-модуля, то f может быть записан как $f = x^n r_n + \ldots + xr_1 + r_0$, где $r_n \neq 0$, и это разложение определено однозначно. Тогда (правой) *степенью*[11] $\deg f$ многочлена назовём указанное число $n \geqslant 0$, коэффициент r_n будем называть *старшим коэффициентом*, а произведение $x^n r_n$ — *старшим мономом* . Формально полагаем, что степень нулевого многочлена равна $-\infty$, а его старший коэффициент равен нулю.

Лемма 9.17. Пусть $R[x;\sigma,\delta]$ — расширение Оре, $r \in R$, $n \in \mathbb{N}$, тогда

$$rx^n = x^n\sigma^n(r) + x^{n-1}a_{n-1} + \ldots + xa_1 + \delta^n(r)$$

для некоторых $a_1, \ldots, a_{n-1} \in R$. В частности, если $r \notin \ker\sigma^n$, то (правая) степень многочлена rx^n равна n.

Доказательство. Прямая проверка по индукции:

$$rx^n = (x\sigma(r) + \delta(r))x^{n-1} = (x^2\sigma^2(r) + \ldots + \delta^2(r))x^{n-2} = \ldots = x^n\sigma^n(r) + \ldots + \delta^n(r).$$

□

Предложение 9.18. Для любых $f, g \in R[x;\sigma,\delta]$ выполнено $\deg fg \leqslant \deg f + \deg g$. Если R — область и σ инъективно, то неравенство обращается равенство.

[11] Для кольца дифференциальных многочленов $R[x,\delta]$ часто используется термин *порядок*.

Доказательство. Из соотношения $rx = x\sigma(r)+\delta(r)$ следует, что $Rx \subseteq xR+R$, откуда по индукции получаем, что $Rx^i \subseteq x^iR + x^{i-1}R + \ldots + xR + R$. Значит, $(Rx^i)(Rx^j) \subseteq x^{i+j}R + \ldots + x^{\min\{i,j\}}R$. Следовательно, $fg \in Rx^{\deg f+\deg g} + \ldots + xR + R$.

Пусть R — область и σ инъективно. Обозначим через m, n — степени, а через f_m, g_n — старшие коэффициенты f и g, соответственно. Перемножим $x^m f_m$ и $x^n g_n$. По лемме $x^m f_m x^n g_n = x^{m+n}\sigma^m(f_m)g_n + \ldots$, где $\sigma^m(f_m) \neq 0$ в силу инъективности σ, а также $\sigma^m(f_m)g_n \neq 0$, так как R — область. □

Следствие 9.19. Если σ инъективно, R — область, то и $R[x;\sigma,\delta]$ — область.

Доказательство. Так как $\deg fg = \deg f + \deg g$, то равенство $fg = 0$ невозможно для ненулевых f, g. □

Предложение 9.20. Если σ — биекция, R первично, то и $R[x;\sigma,\delta]$ первично.

Доказательство. Вспомним, что первичность кольца R эквивалентна $aRb \neq 0$ при $a, b \neq 0$. Обозначим $S = R[x;\sigma,\delta]$. Рассмотрим произвольные ненулевые косые многочлены $f = \sum\limits_{i=1}^{m} x^i f_i$, $g = \sum\limits_{i=1}^{n} x^i g_i$, где $f_m, g_n \neq 0$. Требуется показать, что $fSg \neq 0$. Положим $a = \sigma^n(f_m)$, тогда $a \neq 0$ ввиду инъективности σ. Также пусть $b = g_n$. В силу первичности R можно выбрать $r \in R$ таким, что $arb \neq 0$. Поскольку σ сюръективен, то σ^n тоже сюръективен, поэтому найдется $s \in R \subseteq S$ такой, что $r = \sigma^n(s)$. Вычислим старший моном в произведении fsg, имеем $x^m f_m s x^n g_n = x^{m+n}\sigma^n(f_m s)g_n + \ldots = x^{m+n}arb + \ldots$, но $arb \neq 0$, откуда $fsg \neq 0$. □

Напомним, что правый (левый, двусторонний) идеал называется главным, если он порождается единственным элементом. Кольцо R называется *кольцом главных правых идеалов*, если все его правые идеалы главные. Кольцо главных правых идеалов автоматически является нётеровым справа, так как каждый его правый идеал конечно порождён.

Напомним, что множество X с линейным порядком $\leqslant$ называется вполне упорядоченным, если любое непустое подмножество обладает наименьшим элементом. Простейший пример — любое подмножество $\mathbb{Z}$ относительно стандартного порядка.

Определение 9.21. Кольцо R назовём *евклидовым справа*, если существует такое вполне упорядоченное множество X и такая функция $\phi : R \to X$, что для любых $a, b \in R$, $b \neq 0$ найдется $q \in R$, что выполнено хотя бы одно из двух условий

$$a = bq \quad \text{или} \quad \phi(a - bq) < \phi(b).$$

При этом ϕ называют *евклидовой функцией*.

Стандартные примеры таких колец: $\mathbb{Z}$, $\mathbb{F}[x]$. В первом случае евклидовой функцией является модуль $|\cdot| : \mathbb{Z} \to \mathbb{N} \cup \{0\}$, а во втором — степень многочлена $\deg(\cdot) : \mathbb{F}[x] \to \mathbb{N} \cup \{0, -\infty\}$.

Предложение 9.22. Евклидово справа кольцо является кольцом главных правых идеалов.

Доказательство. Пусть I — правый идеал R. Рассмотрим образ $\phi(I) \subseteq X$. Так как X вполне упорядочено, то в $\phi(I)$ существует наименьший элемент $\phi(b)$. Покажем, что $I = bR$. От противного, пусть найдётся такой $a \in I$, что $a \notin bR$. В силу евклидовости существует $q \in R$, удовлетворяющий $\phi(a - bq) < \phi(b)$, это противоречит минимальности $\phi(b)$. □

Приведём без доказательства следующий результат.

Теорема 9.23 (Брунгс, 1973)**.** Если кольцо R евклидово справа, то кольцо матриц $M_n(R)$ также евклидово справа.

Отметим, что в теореме Брунгса при переходе к кольцу матриц, может потребоваться вполне упорядоченное множество большей мощности.

Предложение 9.24. Пусть D — тело. Тогда любое его (правое) расширение Оре $S = D[x; \sigma, \delta]$ — евклидова справа область.

Доказательство. Ядро эндоморфизма σ — двусторонний идеал, но D — тело, поэтому σ заведомо инъективно, откуда S — область.

Покажем, что корректно определен *правый* алгоритм деления многочленов с остатком: даны $f, g \in S$, $g \neq 0$, $\deg f \geqslant \deg g$ необходимо найти многочлены $q, r \in S$, такие что

$$f = gq + r,\ \deg r < \deg g.$$

Пусть $f = x^m f_m + \dots$, $g = x^n g_n + \dots$, где f_m, g_n не равны нулю, $m \geqslant n$. Положим $q_1 = g_n^{-1} x^{m-n} f_m \in S$. Рассмотрим произведение gq_1. Его старший моном

$$x^n g_n g_n^{-1} x^{m-n} f_m = x^m f_m$$

совпадает со старшим мономом f. Поэтому $\deg(f - gq_1) < \deg(f)$. Заменяя f на $f - gq_1$, можно провести те же рассуждения и получить многочлен q_2, такой что $\deg(f - gq_1 - gq_2) < \deg(f - gq_1)$ и так далее. Будем продолжать этот процесс до тех пор пока не получится многочлен $f - gq_1 - gq_2 - \dots - gq_t$, степень которого будет строго меньше, чем $\deg g$, это и есть искомый многочлен r. Тогда q будет равен сумме всех q_i, построенных на каждом шаге. □

Напомним, что область R называется правой областью Оре, если для всех $a, b \in R \setminus \{0\}$ выполнено $aR \cap bR \neq 0$. Каждая нётерова справа область является правой областью Оре. Это следует из теоремы Голди, однако может быть проверено и непосредственно (см. задачи).

Теорема 9.25. Пусть D — тело. Тогда любое его (правое) расширение Оре $S = D[x; \sigma, \delta]$ является областью главных правых идеалов. Если при этом σ не сюръективно, то S не является левой областью Оре, в частности, S не может быть нётерово слева.

Доказательство. Из предыдущего предложения S — правая евклидова область, откуда S — область правых главных идеалов. Пусть σ не сюръективно. Выберем произвольный $c \in S$, не лежащий в образе σ. Покажем, что $Sx \cap Scx = 0$. От противного, тогда найдутся $f = x^m f_m + \dots$, $g = x^m g_m + \dots$, где $f_m, g_m \neq 0$, такие что $fx = gxc$. При этом $x^m f_m x = x^{m+1}\sigma(f_m) + \dots$, а также $x^m g_m xc = x^{m+1}\sigma(g_m)c + \dots$. Тогда, приравнивая старшие коэффициенты в равенстве $fx = gxc$, получим, что $\sigma(f_m) = \sigma(g_m)c$, откуда $c = \sigma(f_m g_m^{-1})$, что противоречит определению c. □

Следствие 9.26. Существует область нётерова справа, но не слева.

Следствие 9.27. Существует область главных правых, но не левых идеалов.

Следствие 9.28. Существует правая, но не левая евклидова область.

Теорема 9.29 (обобщение теоремы Гильберта о базисе)**.** Пусть S — кольцо, содержащее нётерово справа (слева) подкольцо R. Предположим, что найдется $x \in S$ такой, что любой элемент $s \in S$ представим в виде $\sum\limits_{i=1}^{n} x^i r_i$ для некоторых $r_i \in R$, $n \in \mathbb{N}$. Пусть также $Rx + R = xR + R$. Тогда кольцо S само является нётеровым справа (слева).

Доказательство. Заметим, что всякий элемент кольца S раскладывается и по степеням x с левыми коэффициентами: $x^k R \subseteq x^{k-1}(Rx + R) \subseteq x^{k-2}(Rx^2 + Rx + R) \subseteq \dots \subseteq Rx^k + \dots + Rx + R$.

Пусть I — произвольный правый идеал S. Для целого $n \geqslant 0$ рассмотрим множество старших коэффициентов левых многочленов I, у которых степени не превосходят n, т.е.

$$I_n = \{a_k \mid k \leqslant n,\ a_k x^k + \dots + a_0 \in I\}.$$

Докажем, что это правый идеал. Если $f = f_k x^k + \dots + f_0$ и $g = g_m x^m + \dots + g_0$ — два многочлена из идеала I, $k \leqslant m \leqslant n$, то выравняем степени этих многочленов, домножив f справа на x^{m-k} (I — правый идеал), а затем сложим, чтобы получить левый многочлен со старшим коэффициентом $f_k + g_m$. Далее возьмем любой $r \in R$ и воспользуемся соотношением $Rx + R = xR + R$, откуда $(f_k r)x^k = f_k(rx)x^{k-1} = f_k x s_1 x^{k-1} + \dots = \dots = f_k x^k s_k + \dots$, значит, у многочлена fs_k будет старший коэффициент $f_k r$. Мы показали, что I_n — правый идеал, будем называть его **идеалом правых старших коэффициентов**.

Итак, для любого правого идеала I кольца S строится возрастающая цепочка правых идеалов $I_0 \subseteq I_1 \subseteq \dots$ кольца R. Ключевая идея доказательства состоит в

следующем. Заметим, что если для двух идеалов $I, I' \lhd S$ выполнено $I \subseteq I'$ и $I_n = I'_n$ для всех $n \geqslant 0$, то тогда $I = I'$. От противного, предположим, что множество $I' \setminus I$ непусто, выберем в нём многочлен наименьшей степени h. Пусть $\deg h = n$. В силу $I_n = I'_n$ в I найдется многочлен h' той же степени с тем же старшим коэффициентом. Тогда многочлен $h - h'$ не лежит в I, так как иначе h лежал бы в I. В то же время $\deg(h - h') < \deg(h)$, противоречие.

Покажем, что S нётерово справа. Рассмотрим произвольную возрастающую цепочку $L_0 \subseteq L_1 \subseteq \ldots$ правых идеалов кольца S. Для каждого L_i обозначим его n-й правых идеал старших коэффициентов как L_{in}. Заметим, что при $a \leqslant c, b \leqslant d$ выполнено $L_{ab} \subseteq L_{cd}$. Из нётеровости справа кольца R на некотором j-м шаге обязана стабилизироваться диагональная последовательность $L_{00} \subseteq L_{11} \subseteq L_{22} \subseteq \ldots$, поэтому в бесконечной таблице на рисунке все L_{ab}, располагающиеся ниже и правее L_{jj} обязаны совпасть с L_{jj}. Также для каждого k на некотором m_k-м шаге стабилизируется «вертикальная» последовательность $L_{0k} \subseteq L_{1k} \subseteq L_{2k} \subseteq \ldots$, поэтому все правые идеалы из k-го столбца, находящиеся в таблице ниже $L_{m_k k}$, равны ему.

$$\begin{array}{cccccc}
L_{00} & \ldots & L_{0j} & \ldots & & \\
\vdots & \ddots & \vdots & & & \\
L_{j0} & \ldots & L_{jj} & L_{jj} & \ldots & \\
\vdots & \vdots & L_{jj} & \ddots & & \\
L_{m_0 0} & & \vdots & & & \\
L_{m_0 0} & & & & & \\
\vdots & & & & &
\end{array}$$

Положим $m = \max(j, m_0, \ldots, m_j)$. Тогда при $i \geqslant m$ и всех $n \geqslant 0$ имеем $L_{in} = L_{mn}$. Поэтому в силу предыдущего наблюдения получаем $L_i = L_m$ при $i \geqslant m$. □

Следствие 9.30. Если R нётерово справа, а σ — биекция, то и $R[x; \sigma, \delta]$ нётерово справа.

Доказательство. Если $rx = x\sigma(r) + \delta(r)$ при $r \in R$, то из обратимости σ имеем для всех $s \in R$, что $xs = \sigma^{-1}(s)x - \delta(\sigma^{-1}(s))$, откуда $Rx + R = xR + R$. □

Следствие 9.31 (классическая теорема Гильберта о базисе)**.** Если R — нётерово справа, то $R[x]$ нётерово справа. Отсюда каждый правый идеал $R[x]$ конечно порожден.

10 Теоремы коммутативности

Предложение 10.1 (задача к лекции 4)**.** Пусть D — тело характеристики $p \neq 0$, G — конечная подгруппа в мультипликативной группе G. Тогда G циклическая.

Доказательство. Рассмотрим подмножество $A = \{\sum a_i g_i | a_i \in \mathbb{F}_p, g_i \in G\}$ в D. Это гомоморфный образ конечной групповой алгебры $\mathbb{F}_p G$, поэтому A — конечное подкольцо в D, а следовательно и подтело. По теореме Веддербёрна A является полем, поэтому его мультипликативная группа циклическая, и G также циклическая как её подгруппа. □

Предложение 10.2. Биномиальный коэффициент $C_{p^m}^k = \dfrac{(p^m)!}{k!(p^m-k)!}$, где p простое, либо равен 1, либо делится на p.

Доказательство. Вспомним, что наибольшая степень числа p, входящая в разложение $q!$, равна $\sum\limits_{i=1}^{\infty} \left\lfloor \dfrac{q}{p^i} \right\rfloor$. Поэтому степень числа p, входящая в разложение $C_{p^m}^k$, равна $\sum\limits_{i=1}^{\infty} \left(\left\lfloor p^{m-i} - \dfrac{k}{p^i} - \dfrac{p^m-k}{p^i} \right) \right\rfloor$. Каждое слагаемое последнего ряда целое неотрицательное, и при этом в сумме есть ненулевые слагаемые, если p^m не делит k. □

Лемма 10.3. Пусть D — тело характеристики $p \neq 0$, Z — центр D, $a \in D \setminus Z$, и при этом $a^{p^s} = a$ для некоторого натурального s. Тогда a сопряжён некоторой своей степени: существует $x \in D$, для которого $xax^{-1} = a^d \neq a$.

Доказательство. Рассмотрим $\mathbb{F}_p$-линейный оператор $f\colon D \to D$, переводящий $x \in D$ в $[x, a] = xa - ax$; поскольку $a \notin Z$, оператор f ненулевой. Легко проверить по индукции, что значение m-й степени этого оператора на x равно $f^n x = \sum\limits_{k=0}^{n} (-1)^k C_n^k a^k x a^{n-k}$. Из предыдущего предложения следует, что при $n = p^m$ из-за характеристики кольца в этой сумме ненулевые только крайние слагаемые, откуда $f^{p^m}(x) = xa^{p^m} - a^{p^m}x$ для любого $m \geqslant 0$. Элемент a алгебраичен над $\mathbb{F}_p$, поэтому поле $\mathbb{F}_p(a)$ конечно. Если $|\mathbb{F}_p(a)| = p^m$, то $a^{p^m} = a$, и тогда многочлен $t^{p^m} - t$ — аннулирующий для оператора f.

Рассмотрим теперь на D операторы λE умножения на элементы $\lambda \in \mathbb{F}_p(a)$. Имеем $f(\lambda x) = \lambda xa - (a\lambda)x =$ (так как λ коммутирует с a) $\lambda f(x)$, то есть все эти операторы коммутируют с f. Поле $\mathbb{F}_p(a)$ является полем разложения для многочлена $t^{p^m} - t$, он равен $\prod\limits_{\lambda \in \mathbb{F}_p(a)} (t - \lambda)$, откуда $\prod\limits_{\lambda \in \mathbb{F}_p(a)} (f - \lambda E) = f^{p^m} - f = 0$. Рассмотрим всевозможные произведения скобок вида $(f - \lambda E)$, содержащие скобку f, и выберем среди них произведение наименьшей длины, равное нулю как оператор: $f(f-\lambda_1 E)\dots(f-\lambda_k E) = 0$. Так как $f \neq 0$, $k \geqslant 1$. Если $g = f(f - \lambda_1 E)\dots(f - \lambda_{k-1}E)$, то для некоторого $r \in D$ выполнено $w = gr \neq 0$ и $(f - \lambda_k E)w = 0$, то есть $wa - aw = \lambda_k w$, $waw^{-1} = \lambda_k + a \neq a$.

Как сопряжённый к a элемент waw^{-1} имеет тот же порядок p^m по умножению, при этом $waw^{-1} \in \mathbb{F}_p(a)$, значит, он также является образующим мультипликативной группы $\mathbb{F}_p(a)$, а значит, некоторой степенью элемента a. □

Лемма 10.4. Пусть D — тело, в котором для любого $a \in D$ существует такое натуральное число $n = n(a) > 1$, что $a^{n(a)} = a$. Тогда D коммутативно.

Доказательство. Заметим, что D имеет ненулевую характеристику p: либо $2 = 0$ в D, либо $\operatorname{char} D$ делит натуральное число $2^{n(2)} - 2$.

Предположим, что D некоммутативно. Пусть Z — центр D, а элемент a лежит вне его. Поле $\mathbb{F}_p(a)$ конечно; если оно состоит из p^s элементов, то $a^{p^s} = a$, откуда a сопряжён некоторой своей степени: $bab^{-1} = a^k \neq a$. Это значит, что любое слово от a, b представляется в виде $a^\alpha b^\beta$ и, кроме того, по условию α, β могут быть ограничены, то есть мультипликативная подгруппа $\langle a, b\rangle$ в теле D конечна и в силу утверждения выше циклична. Это противоречит тому, что $bab^{-1} \neq a$. □

Лемма 10.5. Пусть R — кольцо, в котором для любого $a \in R$ существует такое натуральное число $n = n(a) > 1$, что $a^{n(a)} = a$. Тогда всякий правый идеал R двусторонний.

Доказательство. Достаточно доказать утверждение для главных правых идеалов вида rR. При условиях леммы a^{n-1} является идемпотентом.

Заметим, что R редуцированное, откуда при $e^2 = e$ выполнено $ex(1-e) = (1-e)xe$, то есть $ex = xe$ и кольцо абелево. Поэтому для всякого $r \in R$ выполнено $raR = ra^{n-1}aR = a^{n-1}raR \in aR$. □

Лемма 10.6. Пусть R — кольцо, в котором для любого $a \in R$ существует такое натуральное число $n = n(a) > 1$, что $a^{n(a)} = a$. Тогда все коммутаторы элементов R лежат в $J(R)$.

Доказательство. По теореме Крулля в R существует максимальный правый идеал I. Он двусторонний, поэтому существует факторкольцо R/I; так как в нём нет собственных правых идеалов, R/I — тело. Факторизация сохраняет алгебраические соотношения между элементами, поэтому R/I — поле, и образы всех элементов $xy - yx$ при факторизации нулевые, то есть все коммутаторы лежат в I. □

Теорема 10.7 (Джекобсон)**.** Пусть R — кольцо, в котором для любого $a \in R$ существует такое натуральное число $n = n(a) > 1$, что $a^{n(a)} = a$. Тогда R коммутативно.

Доказательство. Рассмотрим элемент $r \in J(R)$. По условию элемент $r^{n(r)-1}$ идемпотентен, но единственный идемпотент в $J(R)$ — это 0. Отсюда $r^{n(r)} = r = 0$ и $J(R) = 0$; в частности, по предыдущей лемме $[x, y] = 0$ для всех x, $y \in R$. □

Теорема 10.8 (Херстейн)**.** Пусть R — кольцо, в котором для любых $x, y \in R$ существует такое натуральное число $n = n(x, y) > 1$, что $[x, y]^{n(x,y)} = [x, y]$. Тогда R коммутативно.

Без доказательства. □

Определим по индукции *высшие* (или *длинные*) коммутаторы:

$$[x_1, \ldots, x_m] = [[x_1, \ldots, x_{m-1}], x_m].$$

Теорема 10.9 (Херстейн)**.** Пусть R — кольцо, в котором для любых $x_1, \ldots, x_m \in R$ существует такое натуральное число $n = n(x_1, \ldots, x_m) > 1$, что $[x_1, \ldots, x_m]^{n(x_1,\ldots,x_m)} = [x_1, \ldots, x_m]$. Тогда R удовлетворяет тождеству $[x_1, \ldots, x_m] = 0$.

Без доказательства. □

Задачи к лекции 10.

Задача 1. Пусть Σ — область, построенная в задачах к предыдущей лекции. Докажите, что она удовлетворяет левому условию Оре.

Задача 2. Пусть R — область, удовлетворяющая условию Оре слева, но не справа.

Из результатов предыдущей лекции (например, из обращения теоремы Голди) следует, что $T = M_2(R)$ — полупервичное левое кольцо Голди. Приведите пример элемента $c \in T$, для которого $r(c) = 0$, но $l(c) \neq 0$ (то есть лемма 8.24 верна только с одной стороны).

Задача 3. Докажите следующую теорему Голди.

Пусть R — область. Тогда эквивалентны следующие условия:

1) в R выполнено правое условие Оре;

2) в R нет прямых сумм $I \oplus J$ двух ненулевых правых идеалов;

3) в R нет прямых сумм $I_1 \oplus \ldots \oplus I_n \oplus \ldots$ бесконечного числа ненулевых правых идеалов.

Указание: для доказательства нетривиальной импликации предположите противное и рассмотрите множество элементов $\{a^i b | i = 0, 1, \ldots\}$.

Задача 4. Найдите центр кольца скрученных многочленов из примера 9.12.

Задача 5. Пусть $R = \mathbb{F}$ — поле, σ — его автоморфизм, $R = \mathbb{F}[x; \sigma]$ – кольцо скрученных многочленов. Если для многочленов $f, g, h \in R$ выполнено равенство $f = hg$, назовем h (соответственно, g) — левым (соответственно, правым) делителями f. Приведите примеры, показывающие, что

1. правый делитель f может не является его левым делителем;

2. количество различных правых унитарных линейных делителей f может быть больше степени f.

Задача 6. Пусть $\mathbb{F}$, $K = \mathbb{F}(t)$ — поля. Определим кольцо R следующим образом: $R = K \oplus Kx$ как левые K-подпространства, причём $x^2 = 0$, $xf(t) = f(t^2)x$ при $f \in K$. Докажите, что $Kx = xK \oplus txK$, откуда правая размерность R над K равна 3 и не совпадает с левой.

Задача 7. Пусть в кольце R выполнено тождество $a^2b^2 = (ab)^2$; докажите, что R коммутативно. Приведите пример некоммутативного кольца без единицы, в котором выполнено это тождество.

Задача 8. Пусть R — трипотентное кольцо, т.е. в нём выполнено тождество $x^3 = x$. Докажите, любой элемент кольца R представляется в виде суммы двух идемпотентов.

Лекция 11. Проективные модули. Наследственные кольца. Кольца регулярные по фон Нейману.

11 Проективные модули. Наследственные кольца.

Определение 11.1. Пусть M, N — правые R-модули, обозначим через $\mathrm{Hom}_R(M, N)$, или просто $\mathrm{Hom}(M, N)$, множество всех гомоморфизмов из M в N.

Отметим, что $\mathrm{Hom}_R(M, N)$ — абелева группа с операцией $(f + g)(m) := f(m) + g(m)$. Для коммутативного кольца R получаем также, что $\mathrm{Hom}_R(M, N)$ — это R-модуль, если положить $(rf)(m) = f(rm)$. Если R некоммутативно, $\mathrm{Hom}_R(M, N)$ может и не быть R-модулем. Тем не менее, $\mathrm{Hom}_R(M, N)$ всегда является модулем над центром $Z(R)$ кольца R.

Предложение 11.2. Для гомоморфизма модулей $f \in \mathrm{Hom}(M, N)$ следующие условия эквивалентны:

1) $\ker f = 0$;

2) f — инъекция;

3) f — *мономорфизм* (сократим слева), т.е. для любых $g, h \in \mathrm{Hom}(L, M)$, удовлетворяющих $fg = fh$, выполнено $g = h$.

Доказательство. 1) $\Leftrightarrow$ 2) Для любых $m_1, m_2 \in M$ равенство $f(m_1) = f(m_2)$ равносильно $f(m_1 - m_2) = 0$.

1) $\Rightarrow$ 3) Получаем, что для всех $l \in L$ выполнено $g(l) - h(l) \in \ker f = 0$.

3) $\Rightarrow$ 1) Пусть $L = \ker f$, также g — тождественное вложение $\ker f$ в M, тогда как h — нулевой гомоморфизм. Тогда из 3) следует, что $g = h$, откуда $\ker f = 0$. □

Также сразу из определений получается аналогичное утверждение про сюръективные гомоморфизмы.

Предложение 11.3. Для гомоморфизма модулей $f \in \mathrm{Hom}(M, N)$ следующие условия эквивалентны:

1) *Коядро* $\mathrm{coker} f := N/\mathrm{Im} f$ равно нулю;

2) f — сюръекция;

3) f — *эпиморфизм* (сократим справа), т.е. для любых $g, h \in \mathrm{Hom}(N, L)$, удовлетворяющих $gf = hf$, выполнено $g = h$.

Определение 11.4. Гомоморфизм $f \in \mathrm{Hom}(M, N)$ *обратим слева (справа)*, если существует такой гомоморфизм $\overline{f} \in \mathrm{Hom}(N, M)$, что $\overline{f}f = \mathrm{id}_M$ ($f\overline{f} = \mathrm{id}_N$).

Обратимый слева гомоморфизм заведомо является мономорфизмом; аналогично обратимость справа гарантирует, что гомоморфизм является эпиморфизмом. Действительно, в обоих этих случаях равенство, свзязывающее f, g, h, можно домножить с нужной стороны на $\overline{f}$. Обратное неверно: не всякий мономорфизм обратим слева, также как не всякий эпиморфизм обратим справа.

Определение 11.5. Последовательность правых R-модулей $\{M_i\}$ и гомоморфизмов $f_i : M_{i-1} \to M_i$ между ними

$$\ldots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \ldots$$

называется *точной в члене* M_i, если выполнено $\mathrm{Im} f_i = \ker f_{i+1}$. Последовательность называется *точной*, если она точна в каждом своём члене.

Пример 11.6. Последовательность вида $0 \longrightarrow N \xrightarrow{f} M$ точна тогда и только тогда, когда $\ker f = 0$, т.е. f инъективен. Напротив, последовательность $N \xrightarrow{f} M \longrightarrow 0$ точна в том и только в том случае, если $\mathrm{Im} f = M$, т.е. f сюръекция.

Определение 11.7. Точная последовательность вида

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

называется *короткой точной последовательностью.*

Пример 11.8. Если M — правый R-модуль, N — его подмодуль, тогда последовательность

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0,$$

где ι — тождественное вложение, π — естественная проекция, будет короткой и точной. Действительно, ι инъективно, поэтому имеется точность в члене N. Из сюръективности π вытекает точность в члене M/N. Кроме того, $\ker \pi = N = \mathrm{Im}\iota$, откуда следует точность в члене M.

Пример 11.9. Пусть $f : M \longrightarrow N$ — произвольный гомоморфизм правых R-модулей. Рассмотрим *кограничение* (сужение) функции f на свой образ, т.е. $\hat{f} : M \longrightarrow \mathrm{Im} f$, где $\hat{f}(m) = f(m)$ для всех $m \in M$. Тогда последовательность

$$0 \longrightarrow \ker f \xrightarrow{\iota} M \xrightarrow{\hat{f}} \mathrm{Im} f \longrightarrow 0,$$

где ι — тождественное вложение, является короткой точной последовательностью. Действительно, $\hat{f}$ — сюръекция, ι — инъекция, $\ker \hat{f} = \ker f = \mathrm{Im}\iota$.

Предложение 11.10. Пусть $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ — короткая точная последовательность. Тогда f — инъекция, g — сюръекция, $A \cong \mathrm{Im} f$, а также $C \cong B/\mathrm{Im} f$

Доказательство. В силу точности f — инъекция, g — сюръекция. По теореме о гомоморфизме $A \cong \mathrm{Im} f$, а также $C \cong B/\ker g$, где $\ker g = \mathrm{Im} f$ в силу точности. □

Определение 11.11. Короткая точная последовательность

$$0 \longrightarrow X \xrightarrow{f} M \xrightarrow{g} Y \longrightarrow 0$$

называется *расщепляющейся*, если гомоморфизм g обратим справа, то есть найдется $\overline{g} \in \mathrm{Hom}(Y, M)$, что $g\overline{g} = \mathrm{id}_Y$.

На самом деле предыдущее определение эквивалентно тому, что f обратим слева, но мы это доказывать не будем.

Предложение 11.12. Если короткая точная последовательность

$$0 \longrightarrow X \xrightarrow{f} M \xrightarrow{g} Y \longrightarrow 0$$

расщепляется, то M раскладывается во внутреннюю прямую сумму $\mathrm{Im} f \oplus Y'$, где $\mathrm{Im} f \cong X$, $Y' \cong Y$. В частности, модуль M изоморфен внешней прямой сумме $M \cong X \oplus Y$.

Доказательство. Изоморфизмы $\mathrm{Im} f \cong X$, $Y' \cong Y$ следуют из предыдущего предложения, поэтому достаточно доказать, что $\mathrm{Im} f$ выделяется в M прямым слагаемым. Мы покажем, что $M = \mathrm{Im} f \oplus \mathrm{Im}\overline{g}$, где $\overline{g}$ — правый обраный для g. Пусть $m \in M$. Проверим, что $m - (\overline{g}g)(m)$ лежит в $\ker g$. Действительно, $g(m) - (g\overline{g}g)(m) = g(m) - g(m) = 0$. В силу точности $\mathrm{Im} f = \ker g$. Итак, $m = (m - (\overline{g}g)(m)) + (\overline{g}g)(m)$, где первое слагаемое лежит в $\mathrm{Im} f$, а второе — в $\mathrm{Im}\overline{g}$. Отсюда $M = \mathrm{Im} f + \mathrm{Im}\overline{g}$. Покажем, что эта сумма прямая: пусть для некоторых $x \in X$, $y \in Y$ выполнено $m = f(x) = \overline{g}(y)$. Тогда с одной стороны, $g(m) = (gf)(x) = 0$, так как $\mathrm{Im} f = \ker g$. С другой стороны, $g(m) = (g\overline{g})(m) = m$, так как $g\overline{g} = \mathrm{id}_Y$. Отсюда $m = 0$. □

Отметим, что не всякая точная последовательность вида $0 \longrightarrow X \longrightarrow X \oplus Y \longrightarrow Y \longrightarrow 0$ является расщепляющейся.

Определение 11.13. Пусть $f : M \longrightarrow N$ — гомоморфизм правых R-модулей, A — произвольный R-модуль. Тогда определены два *индуцированных отображения*:

- $f_* : \mathrm{Hom}_R(A, M) \longrightarrow \mathrm{Hom}_R(A, N)$ по правилу $f_*(h) = fh$,
- $f^* : \mathrm{Hom}_R(N, A) \longrightarrow \mathrm{Hom}_R(M, A)$ по правилу $f^*(h) = hf$.

Непосредственно проверяется, что f_*, f^* являются гомоморфизмами соответствующих $Z(R)$-модулей.

Теорема 11.14. Пусть A — некоторый правый R-модуль.

- Если $0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M$ — точная последовательность правых R-модулей, тогда $0 \longrightarrow \mathrm{Hom}_R(A,K) \xrightarrow{f_*} \mathrm{Hom}_R(A,L) \xrightarrow{g_*} \mathrm{Hom}_R(A,M)$ — точная последовательность $Z(R)$-модулей.

- Если $K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$ — точная последовательность правых R-модулей, тогда $0 \longrightarrow \mathrm{Hom}_R(M,A) \xrightarrow{g^*} \mathrm{Hom}_R(L,A) \xrightarrow{f^*} \mathrm{Hom}_R(K,A)$ — точная последовательность $Z(R)$-модулей.

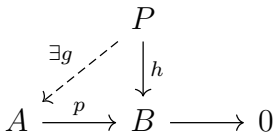
Доказательство. Прямая проверка по определению. Покажем в первом случае, во втором — аналогично.

1. Докажем $\ker f_* = 0$. Если $f_*(h) = 0$, тогда $f(h(a)) = 0$ для всех $a \in A$. Однако $\ker f = 0$ в силу точности исходной последовательности. Отсюда $h(a) = 0$ для всех $a \in A$, т.е. $h = 0$.

2. Проверим $\mathrm{Im} f_* \subseteq \ker g_*$. Пусть $p = f_*(h) = fh$. Тогда образ $g_*(p)$ лежит в $\mathrm{Hom}(A,M)$. Для любого $a \in A$ имеем $(g_*(p))(a) = (gp)(a) = (gfh)(a) = 0$, т.к. $\mathrm{Im} f = \ker g$ в силу точности исходной последовательности. Отсюда $p \in \ker g_*$.

3. Осталось показать $\ker g_* \subseteq \mathrm{Im} f_*$. Пусть $g_*(p) = 0$. Значит, $g(p(a)) = 0$, т.е. $p(a) \in \ker g$ для всех $a \in A$. Однако $\mathrm{Im} f = \ker g$ в силу точности исходной последовательности. Поэтому для каждого a найдется такое $k \in K$, что $p(a) = f(k)$. Определим функцию $h : A \longrightarrow K$, сопоставляющую каждому $a \in A$ указанное значение $k \in K$. Функция определена корректно, т.к. $\ker f = 0$ ввиду точности. Покажем, что h — гомоморфизм. Действительно, если $p(a_1) = f(k_1)$, $p(a_2) = f(k_2)$, тогда $p(a_1 + a_2) = p(a_1) + p(a_2) = f(k_1) + f(k_2) = f(k_1 + k_2)$, откуда $h(a_1 + a_2) = h(a_1) + h(a_2)$. Также для всех $r \in R$ выполнено $p(a_1 r) = p(a_1)r = f(k_1)r = f(k_1 r)$. Итак, $h \in \mathrm{Hom}(A,K)$. Наконец, покажем, что $f_*(h) = p$: для всех $a \in A$ выполнено $(f_*(h))(a) = f(h(a)) = p(a)$. □

Определение 11.15. Правый R-модуль P называется *проективным*, если для любого сюръективного гомоморфизма $p : A \longrightarrow B$ любых правых модулей A, B, и любого гомоморфизма $h : P \longrightarrow B$ существует гомоморфизм $g : P \longrightarrow A$ такой, что $pg = h$. В этом случае говорят, что p *поднимается* до h.



Напомним, что модуль называется свободным, если он обладает базисом.

Теорема 11.16 (О проективном модуле)**.** Для правого R-модуля P следующие условия эквивалентны.

1) Каждая короткая точная последовательность вида $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$ расщепляется.

2) P изоморфен прямому слагаемому некоторого свободного модуля.

3) P — проективный модуль.

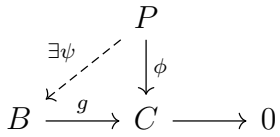
4) Для любой короткой точной последовательности $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ последовательность $0 \longrightarrow \mathrm{Hom}(P, A) \xrightarrow{f_*} \mathrm{Hom}(P, B) \xrightarrow{g_*} \mathrm{Hom}(P, C) \longrightarrow 0$ также точна.

Доказательство. 1) $\Rightarrow$ 2) Каждый модуль изоморфен фактормодулю некоторого свободного модуля. Пусть $P \cong F/G$, где F — свободный модуль, G — некоторый его подмодуль. Тогда последовательность $0 \longrightarrow G \longrightarrow F \longrightarrow P \longrightarrow 0$ точна. В силу 1) она расщепляется, откуда $F \cong G \oplus P$.

2) $\Rightarrow$ 3) Имеем разложение некоторого свободного модуля $F = P \oplus P'$. Пусть дан сюръективный гоморфизм $p : A \longrightarrow B$ и некоторый гомоморфизм $h : P \longrightarrow B$. Требуется найти g из определения проективного модуля. Рассмотрим гомоморфизм $q : F \longrightarrow B$, который является композицией $h : P \longrightarrow B$ и проекции на прямое слагаемое $\pi : F \longrightarrow P$, то есть $q = h\pi$. Пусть $\{u_\lambda\}_{\lambda\in\Lambda}$ — базис модуля F. Тогда множество образов $\{q(u_\lambda)\}_{\lambda\in\Lambda}$ лежит в B. Так как $p : A \longrightarrow B$ — сюръекция, то у каждого $q(u_\lambda)$ найдется[12] хотя бы один прообраз относительно p, обозначим его как a_λ. Рассмотрим множество $\{a_\lambda\}_{\lambda\in\Lambda} \subseteq A$, для него выполнено $p(a_\lambda) = q(u_\lambda)$. Построим отображение $q' : F \longrightarrow A$, зададим его на элементах базиса как $q'(u_\lambda) = a_\lambda$, а затем продолжим по линейности. Заметим, что тогда $pq' = q$. Действительно, достаточно проверить это соотношение на элементах базиса: $p(q'(u_\lambda)) = p(a_\lambda) = q(u_\lambda)$. Наконец положим $g : P \longrightarrow A$ равным композиции q' и естественного вложения прямого слагаемого $\iota : P \longrightarrow F$, то есть $g = q'\iota$. Проверим соотшение из определения проективного модуля: $pg = pq'\iota = q\iota = h\pi\iota = h$ — что и требовалось.

3) $\Rightarrow$ 4) В силу предыдущей теоремы остается только проверить точность в члене $\mathrm{Hom}(P, C)$, то есть надо показать, что g_* — сюръекция. Рассмотрим произвольный гоморфизм $\phi : P \longrightarrow C$. Гомоморфизм $g : B \longrightarrow C$ сюръективен в силу точности исходной последовательности. Тогда по определению проективного модуля найдется такой $\psi : P \longrightarrow B$, что $\phi = g\psi$. По определению g_* можно это переписать в виде $\phi = g_*(\psi)$.

[12] В этом месте мы пользуемся аксиомой выбора.



4) $\Rightarrow$ 1) Применим к каждому члену последовательности $\mathrm{Hom}(P, \cdot)$, получится $0 \longrightarrow \mathrm{Hom}(P, A) \xrightarrow{f_*} \mathrm{Hom}(P, B) \xrightarrow{g_*} \mathrm{Hom}(P, P) \longrightarrow 0$. Ясно, что $\mathrm{id}_P \in \mathrm{Hom}(P, P)$. В силу точности, g_* сюръективно, значит, найдется гомоморфизм $\phi \in \mathrm{Hom}(P, B)$ такой, что $g_*(\phi) = \mathrm{id}_P$. Расписывая g_* по определению, получаем $g\phi = \mathrm{id}_P$, т.е. g обратим справа, это и требовалось. □

Следствие 11.17. Каждый свободный модуль проективен.

Доказательство. Свободный модуль F является сам для себя прямым слагаемым $F = F \oplus 0$ □

Следствие 11.18. Каждое прямое слагаемое проективного модуля проективно.

Доказательство. Пусть P проективный модуль, и K — его прямое слагаемое. По теореме P сам является прямым слагаемым некоторого свободного модуля F. Тогда K — тоже прямое слагаемое F. □

Следствие 11.19. Прямая сумма любого семейства проективных модулей проективна.

Доказательство. Пусть $\{P_\lambda\}_{\lambda \in \Lambda}$ — произвольное семейство проективных модулей. Тогда для каждого P_λ найдется свободный модуль F_λ и его подмодуль G_λ, так что $F_\lambda = P_\lambda \oplus G_\lambda$. Тогда $\bigoplus\limits_{\lambda \in \Lambda} F_\lambda$ — тоже свободный модуль, при этом

$$\bigoplus_{\lambda \in \Lambda} F_\lambda = \bigoplus_{\lambda \in \Lambda} (P_\lambda \oplus G_\lambda) = \bigoplus_{\lambda \in \Lambda} P_\lambda \oplus \bigoplus_{\lambda \in \Lambda} G_\lambda$$

□

Следствие 11.20. Пусть R — кольцо, e — идемпотент. Тогда правый идеал eR — проективный правый R-модуль.

Доказательство. Модуль R_R свободен, его базис $\{1_R\}$. При этом $R_R = eR \oplus (1-e)R$, значит, eR проективен. □

Напомним, что кольцо R полупросто, если R_R (эквивалентно, ${}_RR$) — полупростой модуль, т.е. изоморфен прямой сумме неприводимых.

Теорема 11.21. Следующие условия на кольцо R эквивалентны:

1) Кольцо R полупросто.

2) Все правые R-модули проективны.

2') Все левые R-модули проективны.

Доказательство. 1) $\Rightarrow$ 2) Пусть M — произвольный правый модуль над полупростым кольцом R. Любой модуль изоморфен фактормодулю свободного. Пусть $M \cong F/K$, где F — свободный модуль, K — некоторый его подмодуль. Вспомним, что над полупростым кольцом все модули полупросты, в частности, свободный модуль F полупрост. В полупростом модуле любой подмодуль выделяется прямым слагаемым, тогда $F = K \oplus K'$. Отсюда $K' \cong F/K \cong M$, следовательно M — прямое слагаемое свободного модуля, а значит, проективен.

2) $\Rightarrow$ 1) Пусть I — произвольный правый идеал R. По условию фактормодуль R/I проективен, тогда точная последовательность $0 \longrightarrow I \longrightarrow R_R \longrightarrow R/I \longrightarrow 0$ расщепляется. Так как отображение $I \longrightarrow R_R$ — это просто вложение, то I выделяется прямым сдагаемым в R_R. Мы показали, что любой подмодуль R_R выделяется прямым слагаемым, это одно из эквивалентных определений полупростого модуля.

1) $\Leftrightarrow$ 2') Симметрично. □

Определение 11.22. Кольцо R называется *наследственным справа*, если все его правые идеалы являются проективными правыми R-модулями. Аналогично определяется наследственность слева. Кольцо называется наследственным, если оно удовлетворяет и правому и левому условию.

Пример 11.23.

- Полупростое кольцо наследственно справа и слева в силу предыдущей теоремы.
- Любая область главных правых идеалов R является наследственным справа кольцом. Действительно, любой его правый идеал имеет вид $I = aR$. Заметим, что I — свободный R-модуль: равенство $ar = 0$ возможно только в случае $r = 0$, т.к. R — область. Отсюда I — проективный модуль.

Напомним, что произвольное множество с некоторым линейным порядком $\leqslant$ называется вполне упорядоченным, если любое его непустое подмножество содержит наименьший элемент. По теореме Цермело любое множество может быть вполне упорядочено.

Теорема 11.24 (Капланский)**.** Пусть R — наследственное справа кольцо. Тогда любой подмодуль свободного правого R-модуля изоморфен прямой сумме правых идеалов кольца R. В частности, любой подмодуль свободного правого R-модуля проективен.

Доказательство. Пусть F — свободный правый R-модуль, P — его подмодуль. Рассмотрим базис $\{e_\lambda\}_{\lambda\in\Lambda}$ модуля F. Тогда получаем разложение во внутреннюю прямую сумму $F = \bigoplus\limits_{\lambda\in\Lambda} e_\lambda R$. Пусть индексное множество Λ вполне упорядочено при помощи некоторого линейного порядка $\leqslant$. Для любого $\mu \in \Lambda$ рассмотрим следующие подмодули в F:

$$F_{\leqslant\mu} = \bigoplus_{\lambda\leqslant\mu} e_\lambda R \subseteq F, \quad F_{<\mu} = \bigoplus_{\lambda<\mu} e_\lambda R \subseteq F,$$

где обе прямые суммы внутренние. Отсюда $\{e_\lambda \mid \lambda \leqslant \mu\}$ — базис модуля $F_{\leqslant\mu}$, тогда как $\{e_\lambda \mid \lambda < \mu\}$ — базис для $F_{<\mu}$. Если μ — наименьший элемент Λ, то считаем, что $F_{<\mu} = 0$.

Для каждого $\mu \in \Lambda$ рассмотрим произвольный элемент $u \in P \cap F_{\leqslant\mu}$. Из разложения u по базису $\{e_\lambda \mid \lambda \leqslant \mu\}$ получаем, что существует единственное представление $u = v + e_\mu r_\mu$, где $v \in F_{<\mu}$, $r_\mu \in R$. Тогда мы можем сопоставить каждому u его коэффициент r_μ, получается функция, обозначим ее как ϕ. По определению ϕ отображает $P \cap F_{\leqslant\mu}$ в кольцо R. Функция ϕ определена корректно в силу единственности разложения по базису. Заметим, что ϕ — гомоморфизм правых R-модулей. Действительно, если даны два разложения $u = v + e_\mu r_\mu$ и $u' = v' + e_\mu r'_\mu$, то, складывая их, получим $u + u' = (v + v') + e_\mu(r_\mu + r'_\mu)$, откуда $\phi(u + u') = r_\mu + r'_\mu = \phi(u) + \phi(u')$. Также для любого $r \in R$ имеем $ur = vr + e_\mu r_\mu r$, поэтому $\phi(ur) = r_\mu r = \phi(u)r$.

Заметим, что ядро функции ϕ совпадает с $P \cap F_{<\mu}$. Заменяя ϕ на ее сужение на образ, мы можем записать следующую точную последовательность

$$0 \longrightarrow P \cap F_{<\mu} \xrightarrow{\iota} P \cap F_{\leqslant\mu} \xrightarrow{\phi} \mathrm{Im}\phi \longrightarrow 0,$$

где ι — тождественное вложение. Так как ϕ — гомоморфизм правых модулей, то $\mathrm{Im}\phi$ — подмодуль в R_R, т.е. $\mathrm{Im}\phi$ — правый идеал. В силу того, что R наследственное справа, $\mathrm{Im}\phi$ — проективный R-модуль, поэтому предыдущая точная последовательность расщепляется. Так как ι — тождественное вложение, то получаем разложение во внутреннюю прямую сумму $P \cap F_{\leqslant\mu} = (P \cap F_{<\mu}) \oplus B_\mu$, где правый модуль B_μ изоморфен правому идеалу $\mathrm{Im}\phi \subseteq R_R$.

Осталось показать, что $P = \bigoplus\limits_{\mu\in\Lambda} B_\mu$. Проверим, что $P = \sum\limits_{\mu\in\Lambda} B_\mu$. Включение $P \supseteq \sum\limits_{\mu\in\Lambda} B_\mu$ очевидно, так как $B_\mu \subseteq P$. Докажем обратное включение от противного, пусть $P \not\subseteq \sum\limits_{\mu\in\Lambda} B_\mu$. Так как $F = \bigcup_{\mu\in\Lambda} F_{\leqslant\mu}$, то имеем $P = P \cap F = \bigcup_{\mu\in\Lambda}(P \cap F_{\leqslant\mu})$. Все модули $P \cap F_{\leqslant\mu}$ не могут лежать в $\sum\limits_{\mu\in\Lambda} B_\mu$, ведь иначе мы бы получили, что и весь P там содержится. Выберем наименьший индекс μ_0 такой, что $P \cap F_{\leqslant\mu_0}$ не лежит в $\sum\limits_{\mu\in\Lambda} B_\mu$. Тогда найдется $x \in P \cap F_{\leqslant\mu_0}$, не лежащий в $\sum\limits_{\mu\in\Lambda} B_\mu$. По предыдущему $P \cap F_{\leqslant\mu_0} = P \cap F_{<\mu_0} \oplus B_{\mu_0}$, откуда $x = y + z$, где $y \in P \cap F_{<\mu_0}$, $z \in B_{\mu_0}$. Если μ_0

— наименьший элемент Λ, то $y = 0$, $x = z \in B_{\mu_0} \subseteq \sum\limits_{\mu\in\Lambda} B_\mu$, противоречие с выбором μ_0. Если же найдется $\lambda_0 < \mu_0$, то имеем $y \in P \cap F_{\leqslant\lambda_0}$. В силу минимальности μ_0 мы получаем, что $y \in \sum\limits_{\mu\in\Lambda} B_\mu$, откуда $x = y + z \in \sum\limits_{\mu\in\Lambda} B_\mu$, снова противоречие.

Теперь проверим, что сумма всех B_μ действительно прямая. Пусть $b_1+\ldots+b_k = 0$, где каждый b_i лежит в некотором B_{μ_i}. Без ограничения общности $\mu_1 < \ldots < \mu_k$. Тогда имеем $\{b_1, \ldots, b_{k-1}\} \subseteq B_{\mu_{k-1}} \subseteq P \cap F_{\leqslant\mu_{k-1}} \subseteq P \cap F_{<\mu_k}$, но $b_k \in B_{\mu_k}$. Отсюда

$$b_k = -(b_1 + \ldots + b_{k-1}) \in (P \cap F_{<\mu_k}) \cap B_{\mu_k} = 0,$$

в силу того, что сумма $(P \cap F_{<\mu}) \oplus B_\mu$ прямая для любого μ, как мы установили ранее. Значит, $b_k = 0$. Далее, рассуждая по индукции, получаем, что все $b_1 = \ldots = b_k = 0$. □

Следствие 11.25. Пусть R — наследственное справа кольцо. Тогда правый R-модуль проективен тогда и только тогда, когда он вкладывается как подмодуль в некоторый свободный модуль.

Доказательство. Если P — проективен, то он изоморфен прямому слагаемому свободного модуля. Обратно, если P — подмодуль свободного модуля, то по теореме он изоморфен прямой суммой проективных модулей, а значит, сам проективен. □

Следствие 11.26. Кольцо R является наследственным справа тогда и только тогда, когда любой помодуль любого проективного правого R-модуля проективен.

Доказательство. ($\Rightarrow$) Пусть P проективный модуль, K — его подмодуль. Тогда P вкладывается в некоторый свободный модуль F, откуда K тоже вкладывается в F, а значит, K проективный по предыдущему следствию.

($\Leftarrow$) Регулярный модуль R_R свободен, а значит, проективен. Все его подмодули — правые идеалы — тоже должны быть проективны. □

Следствие 11.27. Пусть R — область главных правых идеалов, тогда:

1. Любой подмодуль свободного правого R-модуля свободен.
2. Правый R-модуль проективен тогда и только тогда, когда он свободен.

Доказательство. Как отмечалось выше, R будет наследственным справа, и, более того, все его правые идеалы — свободные R-модули. Тогда по теореме любой подмодуль свободного R-модуля изоморфен прямой сумме свободных правых идеалов, а значит, сам тоже свободен.

Если P — правый проективный R-модуль, то он вкладывается как подмодуль в свободный модуль, а значит, сам свободен. □

12 Кольца регулярные по фон Нейману

Определение 12.1. Элемент x кольца R называется *регулярным по фон Нейману*, если он обладает *псевдообратным* элементом y, т.е. таким, что $xyx = x$. Кольцо R будем называть *регулярным по фон Нейману*, если все его элементы регулярны по фон Нейману.

В этой лекции для краткости вместо «регулярный по фон Нейману» часто будем говорить просто «регулярный».

Если элемент $x \in R$ обратим хотя бы с одной стороны, то он заведомо регулярен по фон Нейману: в качестве псевдообратного можно выбрать левый или правый обратный.

Класс регулярных колец замкнут относительно взятия гомоморфных образов и прямых произведений. Подкольцо регулярного кольца не обязано быть регулярным ($\mathbb{Z} \subseteq \mathbb{Q}$).

Предложение 12.2. Пусть R — произвольное кольцо, M — правый (или левый) полупростой R-модуль. Тогда кольцо эндоморфизмов $S = \operatorname{End} M$ будет регулярно по фон Нейману.

Доказательство. Пусть $f \in S$. В полупростом модуле M любой подмодуль выделяется прямым слагаемым, в частности, $\operatorname{Im} f$ и $\ker f$: пусть $M = \operatorname{Im} f \oplus N$, а также $M = \ker f \oplus K$. Заметим, что $f(K) = \operatorname{Im} f$. Более того, ограничение $f\Big|_K$ инъективно. Тогда существует обратное отображение $g' : \operatorname{Im} f \longrightarrow K$. Отображение обратное к гомоморфизму модулей автоматически тоже гомоморфизм. Далее fg' тождественно на $\operatorname{Im} f$, т.е. для любого $y \in \operatorname{Im} f$ выполнено $(fg')(y) = y$. Следовательно для любого $x \in M$ получаем $(fg'f)(x) = f(x)$. Наконец зададим эндоморфизм $g \in S$ через ограничения $g\Big|_{\operatorname{Im} f} = g'$, $g\Big|_N \equiv 0$, определение корректно в силу $M = \operatorname{Im} f \oplus N$. Тогда получаем, что $(fgf)(x) = f(x)$ для всех $x \in M$. □

Предложение 12.3. Для кольца R эквивалентны следующие условия:

1) R регулярно;

2) всякий главный правый идеал R порождается идемпотентом;

3) всякий правый идеал вида $xR + yR$ порождается идемпотентом;

4) всякий конечнопорождённый правый идеал R является главным, причём порождается идемпотентом;

2')–4') левые аналоги.

Доказательство. 1) $\Rightarrow$ 2) Если $xyx = x$, то xy — идемпотент. Для главного правого идеала xR имеем $xR = xyxR \subseteq xyR \subseteq xR$, откуда $xR = xyR$.

2) $\Rightarrow$ 3) В силу 2) найдётся идемпотент e такой, что $xR = eR$. Рассмотрим разность $y - ey$. Покажем, что выполнено $xR + yR = eR + (y - ey)R$. С одной стороны, имеем

$e, y - ey \in eR + yR = xR + yR$, откуда $xR + yR \supseteq eR + (y - ey)R$. С другой стороны, $x, y \in xR + eR + (y - ey)R = eR + (y - ey)R$ и получаем обратное включение. В силу пункта 2) главный правый идеал $(y - ey)R$ порождается некоторым идемпотентом, скажем, $f = (y - ey)r$. Заметим, что $ef = e(1 - e)yr = 0$. Теперь положим $g = f(1 - e)$. Тогда $g^2 = f(1 - e)f(1 - e) = f(f - ef)(1 - e) = f(1 - e) = g$, значит, g — тоже идемпотент. Причем по построению g ортогонален e, то есть $ge = eg = 0$. Более того, $fg = g$, а также $gf = f(1 - e)f = f - fef = f$. Следовательно $g \in fR$, $f \in gR$, откуда $gR = fR$. Таким образом, $xR + yR = eR + (y - ey)R = eR + gR = (e + g)R$. Однако $e + g$ — тоже идемпотент в силу ортогональности e и g. Мы нашли идемпотент, порождающий правый идеал $xR + yR$.

3) $\Rightarrow$ 4) Пусть N — произвольный конечнопорожденный правый идеал, скажем, $N = x_1R + \ldots + x_nR$. По индукции найдем идемпотент, порождающий N. База индукции $n = 1$ верна по пункту 3) при $y = 0$. Если $x_1R + \ldots x_{n-1}R = eR$ для некоторого идемпотента e, тогда мы можем применить пункт 3) к сумме $eR + x_nR$, что доказывает шаг индукции.

4) $\Rightarrow$ 1) Возьмем произвольный $x \in R$, тогда по пункту 4) найдётся идемпотент e такой, что $eR = xR$. Это значит, что $e \in xR$ и $x \in eR$, откуда найдутся такие $y, z \in R$, что $e = xy$, $x = ez$. Тогда получаем $x = ez = e(ez) = ex = xyx$, а значит y — псевдообратный элемент для x.

1) $\Rightarrow$ 2') $\Rightarrow$ 3') $\Rightarrow$ 4') $\Rightarrow$ 1) Симметрично.

□

Предложение 12.4. Регулярное кольцо R обладает следующими свойствами:

1) Каждый правый идеал N идемпотентен, т.е. $N^2 = N$.

2) Все двусторонние идеалы R полупервичны.

3) $J(R) = 0$.

4) Кольцо R *полунаследственно справа*, т.е. каждый конечнопорожденный правый идеал — проективный R-модуль.

1'), 4') Левые аналоги.

Доказательство. 1) Включение $N^2 \subseteq N$ выполнено всегда. Обратно, если $x \in N$, то $x = (xy)x \in (NR)N = N^2$.

2) Если квадрат идеала I_1 лежит в I_2, то и сам I_1 лежит в I_2 по предыдущему пункту.

3) Возьмем произвольный $a \in J(R)$, тогда aR порождается идемпотентом по предыдущему предложению, но в $J(R)$ нет ненулевых идемпотентов, откуда $a = 0$.

4) По предыдущему предложению конечнопорожденный правый идеал порождается идемпотентом, а значит, выделяется прямым слагаемым в R_R, следовательно он проективен.

□

Предложение 12.5. Следующие условия на кольцо R эквивалентны:

1) R полупросто;
2) R регулярно по фон Нейману и артиново справа;
3) R регулярно по фон Нейману и нётерово справа;
2'), 3') левые аналоги.

Доказательство. 1) $\Rightarrow$ 2) Артиновость R известна. Так как модуль R_R полупрост, то $\operatorname{End} R_R$ — регулярное кольцо, но $R \cong \operatorname{End} R_R$.

2) $\Rightarrow$ 3) Артиново справа кольцо всегда нётерово справа.

3) $\Rightarrow$ 1) В силу нётеровости всякий правый идеал I конечно порождён, а из-за регулярности является главным и порождён идемпотентом: $I = eR$. Тогда $R_R = I \oplus (1-e)R$, то есть произвольный правый идеал выделяется прямым слагаемым. Значит, R_R — полупростой модуль.

1) $\Rightarrow$ 2') $\Rightarrow$ 3') $\Rightarrow$ 1) Симметрично. $\square$

Лемма 12.6. Пусть $e_1, \ldots, e_n \in R$ — система ортогональных идемпотентов, причём $e_1 + \ldots + e_n = 1$. Тогда регулярность R равносильна тому, что для всякого $x \in e_i R e_j$ существует $y \in e_j R e_i$, такой что $xyx = x$.

Доказательство. ($\Rightarrow$) Пусть R регулярно и $x \in e_i R e_j$. Выберем $y' \in R$ таким, что $x = xy'x$. Тогда

$$x = xy'x = x\left(\sum_{k=1}^{n} e_k\right) y' \left(\sum_{l=1}^{n} e_l\right) x = \sum_{k,l=1}^{n} x(e_k y' e_l)x = x(e_j y' e_i)x,$$

так как $x \in e_i R e_j$. Отсюда искомое $y = e_i y' e_j$.

($\Leftarrow$) Индукция по n. Случай $n = 1$ тривиален. Нам понадобится отдельно рассмотреть случай $n = 2$. Сначала предположим, что $e_1 x e_2 = 0$. По условию найдутся $y \in e_1 R e_1$ и $z \in e_2 R e_2$ такие, что $(e_1 x e_1) y (e_1 x e_1) = e_1 x e_1$ и $(e_2 x e_2) z (e_2 x e_2) = e_2 x e_2$. Кроме того, $x = 1 \cdot x \cdot 1 = (e_1 + e_2)x(e_1 + e_2) = e_1 x e_1 + e_2 x e_1 + e_2 x e_2$ в силу нашего предположения, что $e_1 x e_2 = 0$. Тогда

$$x(y+z)x = (e_1 x e_1 + e_2 x e_1 + e_2 x e_2)(y+z)(e_1 x e_1 + e_2 x e_1 + e_2 x e_2)$$

Воспользуемся тем, что $y \in e_1 R e_1$ и $z \in e_2 R e_2$

$$x(y+z)x = (e_1 x e_1) y (e_1 x e_1) + (e_2 x e_1) y (e_1 x e_1) + (e_2 x e_2) z (e_2 x e_1) + (e_2 x e_2) z (e_2 x e_2).$$

Подставим соотношения $(e_1 x e_1) y (e_1 x e_1) = e_1 x e_1$ и $(e_2 x e_2) z (e_2 x e_2) = e_2 x e_2$ и снова воспользуемся тем, что $y \in e_1 R e_1$ и $z \in e_2 R e_2$, получаем

$$x(y+z)x = e_1 x e_1 + e_2 x e_2 + e_2 x (y+z) x e_1.$$

Вычтем это равенство из тождества $x = e_1 x e_1 + e_2 x e_1 + e_2 x e_2$. Тогда получаем, что $x' = x - x(y+z)x$ лежит в $e_2 R e_1$. По условию леммы найдется такой $w \in e_1 R e_2$, что

$x'wx' = x'$. Подставляя в это равенство $x' = x - x(y+z)x$, получаем выражение вида $x = x(\ldots)x$, откуда x регулярен по фон Нейману.

Пусть теперь e_1xe_2 может быть ненулевым. По условию найдется $y \in e_2Re_1$ такой, что $(e_1xe_2)y(e_1xe_2) = e_1xe_2$. Так как $y \in e_2Re_1$, то предыдущее равенство перепишется в виде $e_1xyxe_2 = e_1xe_2$, откуда $e_1(x-xyx)e_2 = 0$. В силу предыдущего, найдется такой $z \in R$, что $(x-xyx)z(x-xyx) = x-xyx$. После раскрытия скобок мы снова получаем выражение вида $x = x(\ldots)x$, откуда x регулярен по фон Нейману.

Наконец, пусть $n > 2$ и лемма верна для $n-1$. Рассмотрим идемпотенты $f = 1 - e_1 = e_2 + \ldots + e_n$, а также $g = 1 - e_2 = e_1 + e_3 + e_4 + \ldots + e_n$. По предположению индукции кольца fRf и gRg регулярны. Покажем, что идемпотенты e_1, f сами удовлетворяют условиям леммы. Рассмотрим любой элемент $x \in e_1Rf$, тогда $xe_2 \in e_1Re_2$. По условию леммы найдется $y \in e_2Re_1$ такой, что $(xe_2)y(xe_2) = xe_2$. В силу $y \in e_2Re_1$ это равенство переписывается в виде $xyxe_2 = xe_2$, откуда получаем $(x - xyx)e_2 = 0$. Кроме того, в виду $x \in e_1Rf$ имеем $e_2(x - xyx) = 0$. Тогда

$$(x - xyx) = 1 \cdot (x - xyx) \cdot 1 = (e_2 + g)(x - xyx)(e_2 + g) = g(x - xyx)g,$$

следовательно $x - xyx \in gRg$. В силу регулярности кольца gRg найдется такой $z \in gRg$, что $(x-xyx)z(x-xyx) = x-xyx$. Раскрывая скобки, получаем выражение вида $x = xwx$. Так как $x \in e_1Rf$, то $xwx = x(fwe_1)x$, а значит fwe_1 — это тоже псевдообратный для x. Итак, для произвольного $x \in e_1Rf$ мы нашли псевдообратный, лежащий в fRe_1. Симметричные рассуждения показывают, что для любого элемента из fRe_1 найдется псевдообратный, лежащий в e_1Rf. Применяя случай $n = 2$, получаем, что R регулярно. Шаг индукции доказан. □

Теорема 12.7. Следующие условия на кольцо R эквивалентны:

1) R регулярно по фон Нейману.

2) Кольцо матриц $M_n(R)$ регулярно по фон Нейману для всех n.

3) Кольцо матриц $M_n(R)$ регулярно по фон Нейману для хотя бы одного n.

Доказательство. Рассмотрим матричные единицы $E_{11}, \ldots, E_{nn}$.

1) $\Rightarrow$ 2) Произвольный $X \in E_{ii}M_n(R)E_{jj}$ имеет вид xE_{ij}, $x \in R$. Выберем $y \in R$ такой, что $xyx = x$ и положим $Y = yE_{ji} \in E_{jj}M_n(R)E_{ii}$. Тогда произведение $XYX = (xE_{ij})(yE_{ji})(xE_{ij}) = (xyx)E_{ij} = X$. Выполнены условия леммы для идемпотентов $\{E_{ii}\}_{i=1}^n$ в кольце $M_n(R)$.

2) $\Rightarrow$ 3) Частный случай.

3) $\Rightarrow$ 1) По лемме при $i = j = 1$ кольцо $E_{11}M_n(R)E_{11} \cong R$ будет регулярно. □

Следствие 12.8. Пусть R — регулярное кольцо, M — конечнопорожденный проективный правый (или левый) R-модуль. Тогда кольцо эндоморфизмов $\operatorname{End} M$ также будет регулярным.

Доказательство. Пусть M порождается n элементами. Тогда M — фактор свободного модуля $R_R^n = R_R \oplus \ldots \oplus R_R$ (n раз) по некоторому подмодулю N. Короткая последовательность $0 \longrightarrow N \longrightarrow R_R^n \longrightarrow M \longrightarrow 0$ точна, значит, она расщепляется в силу проективности M. Отсюда $R_R^n \cong M \oplus N$. Тогда

$$\operatorname{End} R_R^n \cong \begin{pmatrix} \operatorname{End} M & \operatorname{Hom}(M,N) \\ \operatorname{Hom}(N,M) & \operatorname{End} N \end{pmatrix}.$$

В кольце $\operatorname{End} R_R^n$ выберем идемпотент $e = \left(\begin{smallmatrix} \mathrm{id} & 0 \\ 0 & 0 \end{smallmatrix}\right)$, значит, $\operatorname{End} M \cong e(\operatorname{End} R_R^n)e$. В то же время $\operatorname{End} R_R^n \cong M_n(R)$ регулярно по теореме. Теперь, применяя лемму к идемпотентам $e, 1-e$, получаем, что кольцо $e(\operatorname{End} R_R^n)e$ тоже будет регулярным. $\square$

Напомним, что если $a_1, \ldots, a_n$ — элементы правого R-модуля M, то $\langle a_1, \ldots, a_n \rangle$ — это подмодуль, порожденный $a_1, \ldots, a_n$, т.е. множество всех возможных правых линейных комбинаций $\sum a_i r_i$.

Теорема 12.9. Пусть кольцо R регулярно по фон Нейману, M — проективный правый (или левый) R-модуль. Тогда любой конечнопорожденный подмодуль в M выделяется прямым слагаемым.

Доказательство. Так как M проективен, то он изоморфен прямому слагаемому некоторого свободного модуля F. С точностью до изоморфизма модулей можно считать, что $M \subseteq F$ и найдется подмодуль $N \subseteq F$ такой, что $F = M \oplus N$ — внутренняя прямая сумма.

Пусть $K \subseteq M$ — конечно порожденный подмодуль, скажем, $K = \langle a_1, \ldots, a_n \rangle$. Пусть $\{e_\lambda\}_{\lambda \in \Lambda}$ — базис модуля F. Каждый a_i выражается как линейная комбинация некоторого конечного числа элементов базиса. Значит, все $a_1, \ldots, a_n$ также выражаются как линейная комбинация некоторого конечного числа элементов базиса, скажем, $e_{\lambda_1}, \ldots, e_{\lambda_m}$. Множество $e_{\lambda_1}, \ldots, e_{\lambda_m}$ линейно независимо, как подмножество линейно независимого множества, поэтому модуль $G = \langle e_{\lambda_1}, \ldots, e_{\lambda_m} \rangle$ свободен. Аналогично модуль $G' = \langle e_\lambda \mid \lambda \in \Lambda \setminus \{\lambda_1, \ldots, \lambda_m\} \rangle$ свободен, причём $F = G \oplus G'$ — внутренняя прямая сумма.

По построению $K \subseteq G$. Покажем, что K выделяется в G прямым слагаемым. Положим $t = \max\{m, n\}$. Тогда существует естественное вложение $\phi : G \longrightarrow R_R^t$, каждый базисный элемент e_{λ_i} отправляется в вектор $(0, \ldots, 1, \ldots, 0)$, где единица стоит на i-м месте, а затем ϕ продолжается по линейности на всё G. При этом ϕ — инъекция, в силу единственности разложения по базису. Обозначим $\overline{G} = \phi(G)$, $\overline{K} = \phi(K)$, $\phi(a_i) = \overline{a}_i$. Рассмотрим следующий эндоморфизм $f \in \operatorname{End}(R_R^t)$, положим образ i-го базисного вектора равным $\overline{a}_i$ при $i \leqslant n$ и нулю при $i > n$, а затем продолжим f по линейности на всё R_R^t. Так как $a_1, \ldots, a_n$ порождали K, то $\overline{a}_1, \ldots, \overline{a}_n$ порождают $\overline{K}$. Следовательно $\operatorname{Im} f = \overline{K}$. При этом кольцо $\operatorname{End}(R_R^t) \cong M_t(R)$ регулярно по предыдущей теореме, значит, найдется $g \in \operatorname{End}(R_R^t)$ такой, что $fgf = f$.

Тогда элемент fg — идемпотент. Покажем, что его образ равен $\overline{K}$. С одной стороны, $(fg)(R_R^t) \subseteq f(R_R^t) = \overline{K}$. С другой стороны, в силу $fgf = f$ имеем $(fg)(R_R^t) \supseteq (fg)(\mathrm{Im}f) = (fgf)(R_R^t) = f(R_R^t) = \overline{K}$.

Итак, образ идемпотента fg равен $\overline{K}$, тогда для любого $u \in R_R^t$ имеем $u = (fg)(u) + (1-fg)(u)$. Полагая $\overline{X} = \mathrm{Im}(1-fg)$, получаем разложение $R_R^t = \overline{K} \oplus \overline{X}$. Из свойства модулярности вытекает, что $\overline{G} = R_R^t \cap \overline{G} = \overline{K} \oplus (\overline{X} \cap \overline{G})$. Наконец рассмотрим полный прообраз $Y = \phi^{-1}(\overline{X} \cap \overline{G})$, это подмодуль в G. Так как ϕ осуществляла изоморфизм G и $\overline{G}$, то получаем $G = K \oplus Y$.

Возвращаясь к свободному модулю F, получаем $F = G \oplus G' = K \oplus Y \oplus G'$. Теперь вспоминаем, что $K \subseteq M \subseteq F$, откуда, снова пользуясь модулярностью, получаем $M = F \cap M = K \oplus ((Y \oplus G') \cap M)$, т.е. K выделяется прямым слагаемым в M, это и требовалось. □

Следствие 12.10. Пусть кольцо R регулярно по фон Нейману, M — произвольный конечнопорожденный правый (или левый) R-модуль. Если M порождается некоторыми своими n элементами, то и любой конечнопорожденный подмодуль $N \subseteq M$ также может быть порожден некоторыми своими n элементами.

Доказательство. Построим сюръективный гомоморфизм $\phi : R_R^n \longrightarrow M$ стандартным образом: отобразим элементы базиса в порождающие элементы модуля M и продолжим ϕ по линейности. Пусть $N = \langle a_1, \ldots, a_m \rangle$. В каждом прообразе $\phi^{-1}(a_i)$ выберем произвольный элемент b_i. Положим $G = \langle b_1, \ldots, b_m \rangle$, это подмодуль в R_R^n, причем $\phi(G) = N$. По предыдущей теореме G выделяется прямым слагаемым в R_R^n, скажем, $R_R^n = G \oplus G'$. Тогда $G \cong R_R^n/G'$, откуда G может быть порожден n элементами $g_1, \ldots, g_n$ — образами базисных элементов R_R^n при естественной проекции $R_R^n \longrightarrow R_R^n/G'$. Следовательно $\phi(g_1), \ldots, \phi(g_n)$ порождают N. □

Задачи к лекции 11.

Задача 1. Приведите пример 1) эпиморфизма модулей, не обратимого справа 2) мономорфизма модулей, не обратимого слева. *Указание:* Примеры можно найти среди гомоморфизмов абелевых групп.

Задача 2. Приведите пример конечнопорожденного модуля, не являющегося проективным.

Задача 3. Приведите пример проективного модуля, не являющегося свободным.

Задача 4. Покажите, что бесконечное прямое произведение проективных модулей может не быть проективным. *Указание:* Рассмотреть счётное произведение копий $\mathbb{Z}_\mathbb{Z}$, найти в нём не свободную подгруппу, затем воспользоваться тем, что $\mathbb{Z}$ — область главных идеалов.

Задача 5. Приведите пример точной последовательности $0 \longrightarrow A \longrightarrow A \oplus B \longrightarrow B \longrightarrow 0$, которая не расщепляется. *Указание:* Пример можно найти среди абелевых групп.

Задача 6. Покажите, что кольцо формальных матриц $\begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$ является наследственным справа, но не слева.

Задача 7. Докажите, что область R регулярна по фон Нейману тогда и только тогда, когда R — тело.

Задача 8. Докажите, что если элемент $axa-a$ обладает псевдообратным, то a также обладает псевдообратным.

Задача 9. Пусть R — регулярное по фон Нейману кольцо без единицы, в котором для всякого ненулевого a псевдообратный к нему элемент единственен. Докажите, что R — тело. *Указание*: докажите, что в R нет делителей нуля, и постройте единицу R.

Задача 10. Докажите, что если кольцо R регулярно по фон Нейману, то его центр — это тоже регулярное по фон Нейману кольцо.

Задача 11. Приведите пример регулярного кольца R и его правого идеала, который не может быть порожден конечным числом элементов.