Теория колец

МГУ имени М. В. Ломоносова, Москва

осень 2023

Версия от 20 декабря 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 $M \subseteq R$ — некоторое 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. Также мы будем считать, что пустое множество $\varnothing$ порождает нулевой идеал (0).

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 $\pi\colon \varphi(R) \longrightarrow R/\ker\varphi$, $\varphi(r) \mapsto \varphi^{-1}(\varphi(r))$, 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 $\varphi\colon R \to S$ — 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.

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.

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 в общем случае 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 <u>собственных</u> 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 $aR = \{ar : r \in R\}$ 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 обратимые элементы в групповом кольце а) $\mathbb{F}_2\mathbb{Z}_2$, б) $\mathbb{F}_2\mathbb{Z}_3$, в) $\mathbb{F}_2\mathbb{Z}_6$.

Задача 4. Найдите обратимые элементы в кольце $R[[t]]$ формальных степенных рядов над коммутативным кольцом R.

Задача 5. 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 6. Найдите центр кольца матриц $M_n(R)$, $n > 1$, если а) R — поле, б) R — некоммутативное тело, в) R — произвольное кольцо.

Задача 7. Покажите, что если H — подгруппа группы G, то групповое кольцо RH является подкольцом кольца RG.

Задача 8. Найдите центр группового кольца RG. Когда оно является коммутативным?

Задача 9. Опишите идеалы в кольце $\mathbb{F}[[t]]$ формальных степенных рядов над полем.

Задача 10. 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 ${}_RM$.

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 ${}_RR$ 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 $f\colon I \to \coprod\limits_{i\in I} M_i$, 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 $m \in M$. $\square$

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 — $\mathbb{Z}$).

Задачи к лекции 2.

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

Задача 2. Докажите теорему о гомоморфизме для модулей.

Задача 3. Докажите теорему о соответствии подмодулей.

Задача 4. Предъявите взаимно-однозначное соответствие левых идеалов матричного кольца над кольцом R с подмодулями в ${}_R R^n$.

Задача 5. Покажите, что у конечно порождённого правого модуля над телом все базисы содержат одинаковое количество элементов.

Задача 6. Приведите пример модуля, не имеющего базиса.

Задача 7. Приведите пример свободного модуля, имеющего два базиса разных мощностей.

Задача 8. Верно ли, что подмодуль свободного модуля является свободным?

Задача 9. Приведите примеры конечно порождённого не свободного и свободного не конечно порождённого модулей.

Задача 10. Пусть D — тело. Множество строк $M = \{(d_1, \ldots, d_n) \mid d_i \in D\}$ можно понимать как правый $M_n(D)$-модуль. Покажите, что этот модуль неприводим.

Лекция 3. Неприводимые модули.

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. $\square$

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. $\square$

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

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

Доказательство. Пусть M порождён элементами $m_1, \ldots, m_n$. Зададим Ω — множество собственных подмодулей M, содержащих N. Заметим, что подмодуль $L \leqslant M$ является собственным тогда и только тогда, когда он не содержит одновременно все элементы $m_1, \ldots, m_n$. Отсюда

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

Если $\{L_\lambda\}_{\lambda\in\Lambda}$ — произвольная цепь в Ω, то положим $L = \bigcup_{\lambda\in\Lambda} L_\lambda$. Тогда для произвольных $m_1, m_2 \in L_\lambda$, найдутся индексы $\lambda_1, \lambda_2 \in \Lambda$, что $m_1 \in L_{\lambda_1}$, $m_2 \in L_{\lambda_2}$. Так как $\{L_\lambda\}_{\lambda\in\Lambda}$ — это цепь, то без ограничения общности можно считать, что $L_{\lambda_2} \subseteq L_{\lambda_1}$. Отсюда $m_1, m_2 \in L_{\lambda_1}$, но L_{λ_1} — подмодуль в M. Значит, $m_1 - m_2 \in L_{\lambda_1} \subseteq L$, откуда L — аддитивная подгруппа в M. Также для любого $r \in R$ выполнено $rm_1 \in L_{\lambda_1} \subseteq L$. Значит, L — подмодуль в M.

Так как для всех $\lambda \in \Lambda$ выполнено $\{m_i\}_{i=1}^n \not\subseteq L_\lambda$, то получаем $\{m_i\}_{i=1}^n \not\subseteq L$.

Итак, $L \in \Omega$, а значит, выполнены условия леммы Цорна и в M существует максимальный подмодуль. □

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 φmr, $\varphi \in \operatorname{End} M_R$, $m \in M$, $r \in R$, 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. $\operatorname{End} N_R^n \cong M_n(\operatorname{End} N_R)$.

Теорема 1.67. $\operatorname{End} R_R \cong R$, $\operatorname{End} {}_R R \cong R$.

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

Определение 1.69. 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 1.70. Если бы мы писали гомоморфизмы левых модулей слева, то в предыдущей теореме $\operatorname{End} {}_R R$ оказалось бы изоморфно R^{opp}.

Предложение 1.71 (модулярность)**.** Пусть K, L, N — подмодули правого R-модуля M_R такие, что $K \subseteq N$. Тогда выполнено[4] $K + (L \cap N) = (K + L) \cap N$.

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

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, $m = k + l \in K + (L \cap N)$. $\square$

Задачи к лекции 3.

Задача 1. Приведите пример ненулевого модуля, у которого нет неприводимого подмодуля.

Задача 2. Пусть N_R — неприводимый R-модуль. Найдите все неприводимые подмодули модуля $M_R = N_R^3$.

Задача 3. Пусть V — векторное пространство над полем $\mathbb{F}$ со счётным базисом. Положим $R = \operatorname{End}_{\mathbb{F}}(V)$. Покажите, что $R \cong M_n(R)$ для всех $n \in \mathbb{N}$.

Задача 4. Докажите, что кольцо $\left(\begin{smallmatrix} \mathbb{Z}_4 & \mathbb{Z}_4 \\ 0 & \mathbb{Z}_2 \end{smallmatrix}\right)$ не изоморфно своему противоположному. Найдите кольцо без единицы наименьшей мощности, не изоморфное своему противоположному.

Задача 5. Покажите, что правый (левый) модуль над кольцом R является левым (правым) модулем над кольцом R^{opp}.

Задача 6. Найдите противоположное к кольцу матриц $M_n(R)$. Проверьте, верно ли, что $(M_n(R))^{\text{opp}} \cong M_n(R^{\text{opp}})$.

Задача 7. Покажите, что в утверждении о модулярности условие $K \subseteq N$ является существенным.

2 Артиновы и нётеровы модули и кольца. Теорема Жордана — Гёльдера.

Лекция 4. Артиновы и нётеровы модули и кольца.

Определение 2.1. 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.

$\square$

Определение 2.2. 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 2.3. 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 $M_n = M_n \cap (M_n + N) = M_n \cap (M_i + N) = M_i + (M_n \cap N) = M_i + (M_i \cap N) = M_i$. $\square$

Доказательство нётерова случая двойственно вышеприведённому.

Следствие 2.4. 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. $\square$

Предложение 2.5. 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 2.6. 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 2.7 (лемма Фиттинга)**.** Пусть модуль M одновеременно 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 2.8. 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 2.9. Кольцо R нётерово справа тогда и только тогда, когда каждый его правый идеал конечно порождён.

Следствие 2.10. Если в кольце все правые идеалы главные, т.е. порождены одним элементом, то кольцо нётерово справа.

Пример 2.11. $\mathbb{Z}$ 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 2.12. 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 2.13. 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 2.4, F_R артинов (нётеров) как сумма модулей с таким же свойством. Поэтому и его фактормодуль M артинов (нётеров) по предложению 2.3. $\square$

Следствие 2.14. Подмодуль конечно порождённого правого модуля M_R над нётеровым справа кольцом конечно порождён.

Доказательство. Все подмодули нётерова модуля M_R конечно порождены. $\square$

Теорема 2.15 (Гильберт, о базисе)**.** Пусть R — нётерово справа кольцо. Тогда $R[x]$ также нётерово справа.

Без доказательства. Если успеем, докажем более общий результат. $\square$

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

Предложение 2.16 (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. $\square$

Предложение 2.17 (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 2.18 (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. □

Задачи к лекции 4.

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. Докажите, что кольцо R артиново справа тогда и только тогда, когда каждый конечно порождённый правый R-модуль артинов.

Задача 5. Докажите предложение 2.6 для артиновых модулей: эндоморфизм φ артинова модуля является изоморфизмом тогда и только тогда, когда он инъективен.

Задача 6. Покажите, что подкольцо артинова (нётерова) кольца не обязательно артиново (нётерово).

Задача 7. 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 8. 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 9. 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.

Лекция 5. Композиционные ряды. Теорема Жордана — Гёльдера. Теорема плотности. Примитивные кольца.

Определение 2.19. 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 $(M_i)_{i=0}^n$ является подпоследовательностью в $(M_j')_{j=0}^{n'}$.

Теорема 2.20 (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 2.21. *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 2.22 (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 2.23. 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 2.24. 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 2.25. Пусть V — конечномерное векторное пространство над полем $\mathbb{F}$. Тогда композиционная длина V совпадает с размерностью.

Лемма 2.26. Пусть M — левый или правый модуль над кольцом R и $S = \operatorname{End}_R(M)$. Тогда существует канонический гомоморфизм колец $\varphi : R \to \operatorname{End}_S(M)$.

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

$$\varphi(r_1r_2)(x) = r_1r_2x = \varphi(r_1)(r_2x) = \varphi(r_1)\varphi(r_2)(x),$$

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 2.27 (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 2.28. 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 $x_is = y_i$ 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 2.29 (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 ${}_DM$, 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 2.30. 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 2.31. Кольцо R называется *примитивным (справа)*, если существует точный правый простой R-модуль.

Следствие 2.32. 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 2.33. 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 $I = \mathrm{Ann}\,_R(M)$, 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 2.34. Простое кольцо примитивно справа и слева.

Определение 2.35. 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 5.

Задача 1. Найдите все неприводимые правые модули над кольцом верхнетреугольных 2×2-матриц над полем.

Задача 2. Верно ли, что всякий неприводимый правый R-модуль изоморфен некоторому (минимальному) подмодулю R_R?

Задача 3. Пусть модуль M имеет композиционную длину n. Покажите, что любой его собственный подмодуль N также обладает композиционным рядом и $l(N) < n$.

Задача 4. Пусть R_R обладает композиционным рядом. Докажите, что всякий неприводимый R-модуль содержится среди факторов этого ряда.

Задача 5. Найдите композиционную длину кольца вычетов $\mathbb{Z}_n$ как $\mathbb{Z}$-модуля.

Задача 6. Докажите, что если S— плотное подкольцо кольца линейных преобразований левого векторного пространства V над телом D, то $D \cong \mathrm{End}\,_S(V)$.

Задача 7. Докажите, что если R — примитивное (справа) кольцо, то кольцо матриц $M_n(R)$ примитивно (справа).

Задача 8. Покажите, что коммутативное примитивное (справа) кольцо R является полем.

Задача 9. (Отсутсвие обращения следствия 2.34): Пусть R — кольцо линейных преобразований пространства V над телом, причём $\dim D(V) = \infty$. Покажите, что кольцо R примитивно справа, но не является простым.

3 Полупростые модули и кольца. Теорема Веддербёрна — Артина.

Лекция 6. Полупростые модули. Цоколь. Изотипные компоненты.

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

Отметим, что эта сумма может быть как конечной так и бесконечной. Причём в бесконечном случае она необязательно счётна.

Пример 3.2.

- Нулевой модуль полупрост, он раскладывается в пустую сумму неприводимых.
- Всякое (в т.ч. бесконечномерное) векторное пространство над полем 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.

Далее как обычно M обозначает правый R-модуль.

Предложение 3.3. Пусть M раскладывается в прямую сумму $M = \bigoplus\limits_{i \in I} S_i$, где каждый модуль S_i неприводим. Тогда эта прямая сумма содержит лишь конечное число слагаемых в том и только в том случае, когда M конечно порожден.

Доказательство. Пусть сумма конечна, тогда можно считать, что индексное множество $I = \{1, \ldots, n\}$. В силу неприводимости каждый модуль S_i порожден любым своим ненулевым элементом. Для всех $i = 1, \ldots, n$ выберем произвольный $s_i \in S_i \setminus \{0\}$. Рассмотрим модуль $\langle s_1, \ldots, s_n \rangle_R$, порождённый элементами $s_1, \ldots, s_n$. Тогда имеем $S_i \subseteq \langle s_1, \ldots, s_n \rangle_R$ для всех $i = 1, \ldots, n$. Следовательно, $M = \langle s_1, \ldots, s_n \rangle_R$.

Обратно, пусть модуль M конечно порожден, т.е. $M = \langle m_1, \ldots, m_r \rangle_R$. В силу равенства $M = \bigoplus\limits_{i \in I} S_i$ можно записать

$$\begin{aligned} m_1 &= s_{i_{1,1}} + s_{i_{1,2}} + \ldots + s_{i_{1,k_1}}, \\ m_2 &= s_{i_{2,1}} + s_{i_{2,2}} + \ldots + s_{i_{2,k_2}}, \\ &\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\ m_r &= s_{i_{r,1}} + s_{i_{r,2}} + \ldots + s_{i_{r,k_r}}, \end{aligned}$$

где каждый $s_{i_{\alpha,\beta}} \in S_{i_{\alpha,\beta}}$. Отсюда индексы $i_{\alpha,\beta}$ пробегают некоторое конечное множество в I. Среди модулей $S_{i_{\alpha,\beta}}$ уберем повторяющиеся и рассмотрим подмодуль в M, равный их сумме $\bigoplus S_{i_{\alpha,\beta}}$. Этот подмодуль содержит элементы $m_1, \ldots, m_r$, а значит, совпадает со всем модулем M. Причем все прямые слагаемые $S_{i_{\alpha,\beta}}$ разложения $M = \bigoplus S_{i_{\alpha,\beta}}$ взяты из разложения $M = \bigoplus\limits_{i \in I} S_i$. Это возможно только в случае, когда оба этих разложения совпадают. □

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 <u>всех</u> модулей в выражении $N + \sum\limits_{j \in J} S_j$ является прямой. Тогда $\Omega \neq \varnothing$, в силу $\varnothing \in \Omega$ (сумма N и нулевого модуля, очевидно, 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. Так как F — это объединение цепи $\{F_\lambda\}_{\lambda \in \Lambda}$, то найдётся индекс $\lambda \in \Lambda$, такой что F_λ содержит все $j_1, \ldots, j_k$. Сумма $N + \sum\limits_{j \in F_\lambda} S_j$ является прямой в силу $F_\lambda \in \Omega$. Однако мы получили нетривиальное разложение нуля $0 = n + s_{j_1} + \ldots + s_{j_k}$, соответствующее этой сумме модулей, противоречие. Таким образом, $F \in \Omega$.

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. Докажем, что тогда сумма всех модулей в выражении $N + \sum\limits_{j \in J \cup \{i_0\}} S_j$ будет прямой. Действительно,

$$
\begin{aligned}
&0 = n + s_{j_1} + \ldots + s_{j_k} + s_0, \quad n \in N,\ s_0 \in S_{i_0},\ s_{j_i} \in S_{j_i},\ j_i \in J; \\
&-n - s_{j_1} - \ldots - s_{j_k} = s_0 \in P \cap S_{i_0},
\end{aligned}
$$

откуда $0 = s_0 = -n - s_{j_1} - \ldots - s_{j_k}$. Тогда n и все $s_{j_1}, \ldots, s_{j_k}$ тоже равны нулю, т.к. сумма $N + \sum\limits_{j \in J} S_j$ прямая. Таким образом, сумма $N + \sum\limits_{j \in J \cup \{i_0\}} S_j$ является прямой. Это означает, что $J \cup \{i_0\} \in \Omega$, что противоречит максимальности J.

Итак, мы показали, что для всех $i \in I$ выполнено $P \cap S_i = S_i$. Другими словами, $S_i \subseteq P$. В то же время $M = \sum\limits_{i \in I} S_i$ по условию леммы. Поэтому $P = M$, что и требовалось доказать. $\square$

Отметим, что разложение модуля в сумму неприводимых $M = \sum\limits_{i \in I} S_i$ всегда можно превратить в прямую сумму, убрав часть слагаемых. Это сразу следует из предыдущей леммы при $N = 0$.

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

Дополнение определено неоднозначно, но как R-модули все дополнения изоморфны фактормодулю 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. Пусть $M = N \oplus N'$. Воспользуемся модулярностью: $P = M \cap P = (N + N') \cap P = N + (N' \cap P)$. Причем сумма $P = N + (N' \cap P)$ окажется прямой, т.к. $N \cap (N' \cap P) \subseteq N \cap N' = 0$. $\square$

Теорема 3.7 (критерий полупростоты модуля)**.** 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) $\Rightarrow$ 1) Если $M = 0$, то доказывать нечего, далее предполагаем $M \neq 0$. Пусть S — сумма[5] всех неприводимых подмодулей модуля M. Предположим, что $S \neq M$, тогда $M = S \oplus T$, $T \neq 0$. Рассмотрим произвольный ненулевой циклический подмодуль $N \leqslant T$. Так как N конечно порожден, то можно найти в нем максимальный собственный подмодуль N' (теорема 1.58). Но N' — это подмодуль не только в N, но и в M. Значит, по пункту 3) N' выделяется прямым слагаемым в M. По лемме 3.6 N' выделяется прямым слагаемым и в модуле N тоже, т.е. $N = N' \oplus P$. Следовательно, $P \cong N/N'$. Тогда из максимальности N' следует, что модуль P неприводим. По определению модуля S получаем, что $P \subseteq S$. В то же время по построению $P \subseteq T$. Однако $M = S \oplus T$, а значит, $S \cap T = 0$, откуда $P = 0$, что противоречит неприводимости модуля P. Значит, наше исходное предположение $S \neq M$ оказалось неверным. Поэтому модуль M совпадает с суммой всех своих неприводимых подмодулей. $\square$

[5] Если неприводимых подмодулей нет, то полагаем стандартным образом $S = 0$. Однако дальше мы увидим, что этот случай не реализуется.

Следствие 3.8. Пусть $M = \bigoplus_{i\in I} S_i$, все S_i — неприводимые модули, $N \leqslant M$. Тогда у модуля N есть дополнение вида $\bigoplus_{k\in K} S_k$, где $K \subseteq I$, причем N изоморфен (но не обязательно равен) модулю $\bigoplus_{k\in I\setminus K} S_k$. В частности, если N неприводимый, то найдётся такое $i \in I$, что $N \cong S_i$, и при этом $N \oplus \bigoplus_{j\neq i} S_j = M$.

Доказательство. Из леммы 3.4 получаем, что $M = N \oplus \bigoplus_{k\in K} S_k$. Непосредственно по определению прямой суммы проверяется, что

$$N \cong M/\bigoplus_{k\in K} S_k = \bigoplus_{i\in I} S_i \Big/ \bigoplus_{k\in K} S_k \cong \bigoplus_{k\in I\setminus K} S_k.$$

Если N неприводим, то он не может быть изоморфен прямой сумме, в которой есть хотя бы два ненулевых слагаемых. Ведь тогда прямые слагаемые были бы нетривиальными подмодулями в N. Значит, $N \cong S_i$ для некоторого $i \in I$. □

Следствие 3.9. Подмодули и фактормодули полупростого модуля полупросты. Гомоморфный образ полупростого модуля полупрост.

Доказательство. По предыдущему следствию подмодули и фактормодули окажутся изоморфны прямой сумме модулей S_i, где i пробегает некоторое подмножество в I. Но все S_i неприводимы.

Пусть $\phi : M \to N$ — сюръективный гомоморфизм модулей, M полупрост. Тогда по теореме о гомоморфизме $N \cong M/\ker\phi$, т.е. N изоморфен фактормодулю модуля M, а значит, полупрост по предыдущему. □

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. Так как $P_1 \leqslant M = Q_1 \oplus \ldots \oplus Q_m$, то P_1 изоморфен одному из модулей Q_j в силу следствия 3.8. С точностью до перенумерации можно считать, что $P_1 \cong Q_1$. Это позволяет удалить эти слагаемые и осуществить индукцию по n. База индукции $n = 0$ соответствует $M = 0$ и пустой сумме модулей, для которой всё выполнено тривиальным образом. □

Пусть $\{N_\lambda\}_{\lambda\in\Lambda}$ — семейство всех максимальных правых идеалов кольца R. По теореме Крулля это семейство непусто при $R \neq 0$. Вспомним, что любой неприводимый правый R-модуль M изоморфен фактормодулю R/N_λ для некоторого[6] N_λ (предложение 1.55). Тогда семейство $\{R/N_\lambda\}_{\lambda\in\Lambda}$ заведомо включает в себя все неприводимые правые R-модули с точностью до изоморфизма. Введём на множестве $\{R/N_\lambda\}_{\lambda\in\Lambda}$ отношение эквивалентности как изоморфизм модулей. Выберем по одному представителю из каждого класса эквивалентности. Получится множество неприводимых модулей $\{M_\gamma\}_{\gamma\in\Gamma}$ такое, что произвольный неприводимый правый R-модуль M изоморфен в точности одному модулю M_γ из этого множества[7]. В этом случае будем говорить, что M — это *модуль класса изоморфизма* γ.

Пример 3.11. В некоторых случаях классы изоморфизма неприводимых модулей можно описать более явно.

- Пусть R — это тело. Тогда 0 — единственный максимальный правый идеал. Значит, все неприводимые правые R-модули изоморфны правому регулярному модулю R_R. Получается, что множество $\{M_\gamma\}_{\gamma\in\Gamma}$ состоит из одного модуля R_R.
- Пусть $R = \mathbb{Z}$. Как уже отмечалось, неприводимые $\mathbb{Z}$-модули — это конечные циклические группы простого порядка. Ясно, что две такие группы $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/q\mathbb{Z}$ не изоморфны при $p \neq q$ из соображений мощности. Поэтому в качестве множества $\{M_\gamma\}_{\gamma\in\Gamma}$ можно выбрать $\{\mathbb{Z}/p\mathbb{Z} \mid p \text{ простое}\}$.

Определение 3.12. Пусть M — произвольный правый R-модуль, $\{M_\gamma\}_{\gamma\in\Gamma}$ — все неприводимые правые R-модули с точностью до изоморфизма.

- *Цоколь* модуля M — это сумма всех его неприводимых подмодулей:
$$\operatorname{soc} M = \sum\{N \leqslant M \mid N \text{ — неприводим}\}.$$
- Для каждого $\gamma \in \Gamma$ можно определить *изотипную (однородную) компоненту* модуля M как сумму всех неприводимых подмодулей класса γ:
$$\operatorname{soc}_\gamma M = \sum\{N \leqslant M \mid N \cong M_\gamma\}.$$
Изотипную компоненту также называют *γ-цоколем.*

[6]Для нулевого кольца мы считаем, что $1 = 0$, откуда в силу унитарности $1 \cdot m = m$ получаем, что над нулевым кольцом существует только нулевой модуль. Он не является неприводимым. Поэтому над нулевым кольцом пустым является как множество максимальных правых идеалов, так и множество неприводимых правых модулей.

[7]Отметим, что если заменить неприводимость на другое свойство модулей, то такого множества может и не быть. В общем случае получится не множество, а класс. Например, два векторных пространства над полем изоморфны тогда и только тогда, когда их базисы равномощны. Однако множества всех кардиналов не существует.

В обоих случаях суммирование по пустому множеству будем считать нулевым подмодулем.

Из пунктов 1,2 критерия полупростоты получаем, что и цоколь, и каждая изотипная компонента заведомо являются полупростыми модулями. Более того, $\operatorname{soc} M$ — это наибольший полупростой подмодуль модуля M. В частности, верно следующее.

Замечание 3.13. Модуль M полупрост тогда и только тогда, когда $M = \operatorname{soc} M$.

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 $\dim V \geqslant 2$. Тем не менее, цоколь можно представить в виде прямой суммы неприводимых модулей, убрав часть слагаемых (лемма 3.4 при $N = 0$). То же верно и для изотипных компонент.

Определение 3.14. *Вполне инвариантный* подмодуль $N \leqslant M$ — это такой подмодуль, что $\varphi(N) \subseteq N$ для всех $\varphi \in \operatorname{End} M$.

На правом 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 3.15. Пусть M — произвольный правый R-модуль, $\{M_\gamma\}_{\gamma\in\Gamma}$ — все неприводимые правые R-модули с точностью до изоморфизма. Тогда выполнено следующее.

1) Цоколь раскладывается в прямую сумму изотипных компонент[8]:

$$\operatorname{soc} M = \bigoplus_{\gamma\in\Gamma} \operatorname{soc}_\gamma M.$$

2) Всякая сумма некоторых изотипных компонент вполне инвариантна. Другими словами, для любого подмножества $\widetilde{\Gamma} \subseteq \Gamma$ и для произвольного эндоморфизма ϕ всего модуля M выполнено

$$\phi\left(\bigoplus_{\gamma\in\widetilde{\Gamma}} \operatorname{soc}_\gamma M\right) \subseteq \bigoplus_{\gamma\in\widetilde{\Gamma}} \operatorname{soc}_\gamma M.$$

3) Пусть M — полупростой модуль, $N \leqslant M$ — вполне инвариантный подмодуль. Тогда найдётся такое подмножество $\widetilde{\Gamma} \subseteq \Gamma$, что

$$N = \bigoplus_{\gamma\in\widetilde{\Gamma}} \operatorname{soc}_\gamma M.$$

[8]Некоторые из них могут быть нулевыми

Доказательство. 1) Из определения цоколя сразу получаем, что $\operatorname{soc} M = \sum\limits_{\gamma\in\Gamma} \operatorname{soc}_\gamma M$. Выберем произвольное $\gamma_0 \in \Gamma$ и обозначим $P = \sum\limits_{\gamma\in\Gamma\setminus\{\gamma_0\}} \operatorname{soc}_\gamma M$. Для доказательства первого пункта достаточно показать, что модуль $K = P \cap \operatorname{soc}_{\gamma_0} M$ является нулевым. Предположим, что $K \neq 0$.

Модуль $\operatorname{soc}_{\gamma_0} M$ является суммой неприводимых модулей класса γ_0. Убирая часть слагаемых, можно добиться того, чтобы эта сумма стала прямой (лемма 3.4 при $N = 0$). Однако K — подмодуль в $\operatorname{soc}_{\gamma_0} M$, а значит, K изоморфен прямой сумме некоторых неприводимых модулей класса γ_0 (следствие 3.8). Выберем какой-нибудь неприводимый подмодуль $K' \leqslant K$ класса γ_0. Тогда $K' \leqslant K \leqslant P$.

Далее по определению $\operatorname{soc}_\gamma M$ модуль $P = \sum\limits_{\gamma\in\Gamma\setminus\{\gamma_0\}} \operatorname{soc}_\gamma M$ можно представить в виде суммы неприводимых модулей. Снова убирая часть слагаемых, можно получить разложение $P = \bigoplus\limits_{i\in I} N_i$, где каждый модуль N_i является неприводимым какого-то класса $\gamma \in \Gamma \setminus \{\gamma_0\}$. Однако модуль K' тоже неприводим, и при этом $K' \leqslant P$. Тогда K' должен быть изоморфен одному из модулей N_i (следствие 3.8). Однако эти модули заведомо разных классов изоморфизма, противоречие.

2) Пусть $\operatorname{soc}_\gamma M = \sum S_i$, где S_i — все неприводимые модули класса γ. Рассмотрим произвольный эндоморфизм $\varphi \in \operatorname{End} M_R$. Тогда $\varphi(\operatorname{soc}_\gamma M) = \sum \varphi(S_i)$. Так как $\ker\phi \cap S_i$ является подмодулем в неприводимом модуле S_i, то либо $\ker\phi \cap S_i = S_i$, либо $\ker\phi \cap S_i = 0$. Следовательно, либо $\phi(S_i) = 0$, либо $\phi(S_i)$ изоморфен S_i. Поэтому образ $\varphi(\operatorname{soc}_\gamma M)$ снова является суммой неприводимых модулей класса γ, т.е. $\varphi(\operatorname{soc}_\gamma M) \subseteq \operatorname{soc}_\gamma M$. Таким образом, каждая изотипная компонента является вполне инвариантным подмодулем. Но любая сумма вполне инвариантных подмодулей снова вполне инвариантна.

3) Пусть $N \leqslant M$ вполне инвариантен, и M полупрост. Тогда N тоже полупрост, а значит, N раскладывается в сумму неприводимых модулей. Поэтому

$$N \subseteq \bigoplus_{\gamma\in\widetilde{\Gamma}} \operatorname{soc}_\gamma M, \quad \widetilde{\Gamma} = \{\gamma \in \Gamma \mid \exists P \leqslant N :\ P \cong M_\gamma\}.$$

Для доказательства обратного включения достаточно показать, что вместе с каждым неприводимым подмодулем $P \leqslant N$ класса γ модуль N содержит и всю изотипную компоненту $\operatorname{soc}_\gamma M$. Другими словами, мы должны проверить, что если P, Q — изоморфные неприводимые модули, причем $P \leqslant N$, $Q \leqslant M$, то выполнено $Q \leqslant N$.

Так как $P \cap Q$ является подмодулем и в P, и в Q, то либо $P = Q$, либо сумма $P + Q$ прямая. Первый случай нам точно подходит, разберём второй. По критерию полупростоты подмодуль $P \oplus Q \leqslant M$ выделяется прямым слагаемым, а значит, $M = P \oplus Q \oplus U$ для некоторого подмодуля $U \leqslant M$. Пусть $f\colon P \to Q$ — изоморфизм модулей. Рассмотрим отображение

$$\theta : M = P \oplus Q \oplus U \to M, \quad p + q + u \mapsto f(p) + f^{-1}(q) + u.$$

Тогда θ — эндоморфизм модуля M, причём $\theta(P) = Q$, а также $\theta(Q) = P$. Однако модуль N вполне инвариантен и содержит P, а значит, $N \supseteq \theta(P) = Q$, что и требовалось.

$\square$

Задачи к лекции 6.

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

Задача 3. Покажите, что $\operatorname{soc} M$ является наибольшим полупростым подмодулем модуля M.

Задача 4. Приведите пример ненулевого модуля с нулевым цоколем.

Задача 5. Покажите, что $\operatorname{soc}(\operatorname{soc} M) = \operatorname{soc} M$ для произвольного R-модуля M.

Задача 6. Для кольца R можно рассмотреть два цоколя: $S_1 = \operatorname{soc}(R_R)$ для правого регулярного модуля, и $S_2 = \operatorname{soc}({}_RR)$ — для левого. Покажите, что
1) S_1 и S_2 являются идеалами кольца R;
2) S_1 и S_2 не обязательно равны.

Задача 7. Верно ли, что цоколь циклического модуля является циклическим?

Задача 8. Пусть модуль M раскладывается в сумму подмодулей $M = M_1 + M_2$. Верно ли, что $\operatorname{soc} M = \operatorname{soc} M_1 + \operatorname{soc} M_2$?

Задача 9. Найдите цоколь $\mathbb{Z}_n$ как $\mathbb{Z}$-модуля.

Лекция 7. Изотипные компоненты. Полупростые кольца. Теорема Веддербёрна-Артина.

Предложение 3.16. Пусть $\{M_\gamma\}_{\gamma\in\Gamma}$ — все неприводимые правые R-модули с точностью до изоморфизма. Рассмотрим полупростой модуль $M = \bigoplus\limits_{i\in I} S_i$, где S_i неприводимы. Для $\gamma \in \Gamma$ положим $I_\gamma = \{i \in I \mid S_i \cong M_\gamma\}$. Тогда

$$\mathrm{soc}_\gamma\, M = \bigoplus_{i\in I_\gamma} S_i.$$

Доказательство. Для любого $i \in I_\gamma$ модуль S_i принадлежит классу изоморфизма γ, а значит, $S_i \subseteq \mathrm{soc}_\gamma\, M$ по определению изотипной компоненты. Тогда выполнено $\bigoplus\limits_{i\in I_\gamma} S_i \subseteq \mathrm{soc}_\gamma\, M$, и остаётся доказать обратное включение.

Пусть $N \leqslant M$ — произвольный неприводимый подмодуль класса γ. Так как $M = \bigoplus\limits_{i\in I} S_i$, то каждый $a \in N$ единственным образом раскладывается в сумму элементов $s_i \in S_i$, в которой лишь конечное число слагаемых отлично от нуля. Для каждого $i \in I$ построим гомоморфизм $\phi_i : N \longrightarrow S_i$, который ставит в соответствие элементу $a \in N$ его проекцию s_i на прямое слагаемое S_i. Тогда ядро ϕ_i — это подмодуль в неприводимом модуле N, а образ — подмодуль в неприводимом модуле S_i. Значит, ϕ_i является либо изоморфизмом, либо нулевым гомоморфизмом. Тогда

$$N \subseteq \bigoplus_{i\in I\colon\ S_i\cong N} S_i.$$

В то же время N — это модуль класса γ, поэтому $\{i \in I \mid S_i \cong N\} = I_\gamma$. Таким образом, $N \subseteq \bigoplus\limits_{i\in I_\gamma} S_i$. Однако $N \leqslant M$ — произвольный неприводимый подмодуль класса γ. Значит, $\mathrm{soc}_\gamma\, M \subseteq \bigoplus\limits_{i\in I_\gamma} S_i$. □

Вспомним, что если $\{R_\gamma\}_{\gamma\in\Gamma}$ — произвольное семейство колец, индексированное множеством Γ, то прямое произведение колец этого семейства определяется как множество отображений

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

с поточечными операциями сложения и умножения. Отображение f часто удобно записывать в виде $f = \prod\limits_{\gamma\in\Gamma} f(\gamma)$.

Предложение 3.17. Пусть $\{M_\gamma\}_{\gamma\in\Gamma}$ — все неприводимые правые R-модули с точностью до изоморфизма. Рассмотрим полупростой правый R-модуль M. Тогда[9]

$$\operatorname{End} M \cong \prod_{\gamma\in\Gamma} \operatorname{End}(\operatorname{soc}_\gamma M).$$

Доказательство. Зададим отображение $\Phi : \operatorname{End} M \longrightarrow \prod\limits_{\gamma\in\Gamma} \operatorname{End}(\operatorname{soc}_\gamma M)$. Каждому эндоморфизму $f \in \operatorname{End} M$ сопоставим $\prod\limits_{\gamma\in\Gamma} f_\gamma$, где f_γ полагаем равным ограничению $f\Big|_{\operatorname{soc}_\gamma M}$. Так как изотипная компонента $\operatorname{soc}_\gamma M$ — это вполне инвариантный подмодуль в M, то f_γ является её эндоморфизмом. При этом

$$(f+g)_\gamma = (f+g)\Big|_{\operatorname{soc}_\gamma M} = f\Big|_{\operatorname{soc}_\gamma M} + g\Big|_{\operatorname{soc}_\gamma M} = f_\gamma + g_\gamma.$$

Снова пользуясь тем, что $\operatorname{soc}_\gamma M$ вполне инвариантен, получим

$$(f\circ g)_\gamma = (f\circ g)\Big|_{\operatorname{soc}_\gamma M} = f\Big|_{\operatorname{soc}_\gamma M} \circ g\Big|_{\operatorname{soc}_\gamma M} = f_\gamma \circ g_\gamma.$$

Далее, учитывая что на прямом произведение операции заданы поточечно, имеем

$$\prod_{\gamma\in\Gamma}(f+g)_\gamma = \prod_{\gamma\in\Gamma}(f_\gamma+g_\gamma) = \prod_{\gamma\in\Gamma} f_\gamma + \prod_{\gamma\in\Gamma} g_\gamma; \quad \prod_{\gamma\in\Gamma}(f\circ g)_\gamma = \prod_{\gamma\in\Gamma}(f_\gamma\circ g_\gamma) = \prod_{\gamma\in\Gamma} f_\gamma \circ \prod_{\gamma\in\Gamma} g_\gamma.$$

Также $\Phi(\mathrm{id}) = \mathrm{id}$. Таким образом, построенное отображение Φ действительно является гомоморфизмом.

Так как M полупрост, то он совпадает со своим цоколем, а значит, раскладывается в сумму изотипных компонент: $M = \bigoplus\limits_{\gamma\in\Gamma} \operatorname{soc}_\gamma M$. Поэтому если ограничение f на каждую изотипную компоненту $\operatorname{soc}_\gamma M$ равно нулю, то сам f — это тоже нулевой эндоморфизм. Отсюда гомоморфизм Φ инъективен.

Пусть $f_\gamma \in \operatorname{End}(\operatorname{soc}_\gamma M)$, $\gamma \in \Gamma$ — произвольное семейство эндоморфизмов. Так как $M = \bigoplus\limits_{\gamma\in\Gamma} \operatorname{soc}_\gamma M$, то каждый $m \in M$ единственным образом представим в виде $m = \sum\limits_{\gamma\in\Gamma} m_\gamma$, где $m_\gamma \in \operatorname{soc}_\gamma M$, и лишь конечное число элементов m_γ отлично от нуля. Определим эндоморфизм f модуля M по правилу $f(m) = \bigoplus\limits_{\gamma\in\Gamma} f_\gamma(m_\gamma)$. Тогда $\Phi(f) = \prod\limits_{\gamma\in\Gamma} f_\gamma$, откуда следует сюръективность Φ. $\square$

[9]Некоторые изотипные компоненты могут быть нулевыми, тогда их кольца эндоморфизмов тоже будут нулевыми. Поэтому в этом прямом произведение возможны нулевые множители, которые можно отбросить с точностью до изоморфизма.

Предложение 3.18. Пусть D — произвольное тело, $n \in \mathbb{N}$. Рассмотрим множество $D^n = \{(d_1, \ldots, d_n) \mid d_i \in D\}$, элементы которого мы будем считать строками с покоординатной операцией сложения. Зададим на D^n структуру правого модуля над кольцом матриц $R = M_n(D)$ посредством умножения строки на матрицу[10] справа. Тогда D^n является неприводимым R-модулем, и при этом его кольцо эндоморфизмов

$$\mathrm{End}\,(D^n_R) \cong D.$$

Доказательство. Рассмотрим произвольную ненулевую строку $v = (v_1, \ldots, v_n) \in D^n$, пусть $v_i \neq 0$ для некоторого $i \in \{1, \ldots, n\}$. Покажем, что подмодуль $vR \leqslant D^n$, порождённый v, совпадает со всем D^n. Для каждого $j \in \{1, \ldots, n\}$ рассмотрим матричную единицу E_{ij}, тогда

$$v \cdot E_{ij} \cdot (v_i^{-1}E) = (0, \ldots, \underset{j\text{-я позиция}}{1}, \ldots, 0).$$

Значит vR содержит все стандартные базисные векторы, складывая их и умножая на скалярные матрицы, можно получить любой вектор из D^n.

Зададим на D^n структуру левого D-модуля при помощи операции умножения всех элементов произвольной строки $v \in D^n$ на $d \in D$ слева. Определим отображение[11] $\phi : D \longrightarrow \mathrm{End}\,(D^n_R)$ по правилу $\phi(d)v = d \cdot v$, для всех $d \in D$, $v \in D^n$. Тогда для всех $d \in D$, $v_1, v_2 \in D^n$, $A_1, A_2 \in M_n(D)$ выполнено

$$\phi(d)(v_1A_1 + v_2A_2) = dv_1A_1 + dv_2A_2 = (\phi(d)v_1)A_1 + (\phi(d)v_2)A_2,$$

а значит, $\phi(d)$ действительно является эндоморфизмом D^n как правого R-модуля. При этом тривиальным образом $\phi(d_1 + d_2) = \phi(d_1) + \phi(d_2)$, $\phi(d_1d_2) = \phi(d_1)\phi(d_2)$, $\phi(1) = \mathrm{id}$, следовательно, ϕ — гомоморфизм колец.

Ядро $\ker\phi$ является идеалом в D, но D — тело. Причём $\phi(1) = \mathrm{id}$, поэтому $\ker\phi \neq D$, откуда $\ker\phi = 0$ и ϕ инъективен. Осталось проверить сюръективность. Рассмотрим произвольный $f \in \mathrm{End}\,(D^n_R)$. Пусть

$$f(1, 0 \ldots, 0) = (d, *, \ldots, *).$$

Тогда для произвольной строки $(d_1, \ldots, d_n) \in D^n$ выполнено

$$f(d_1, \ldots, d_n) = f\left((1, 0, \ldots, 0) \cdot \begin{pmatrix} d_1 & \ldots & d_n \\ 0 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & 0 \end{pmatrix}\right) = f(1, 0 \ldots, 0) \cdot \begin{pmatrix} d_1 & \ldots & d_n \\ 0 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & 0 \end{pmatrix} =$$

[10] В этом случае $M_n(D)$ можно естественным образом отождествить с кольцом эндоморфизмов D^n как левого D-модуля, см. следствие 1.66. Тогда умножение строки на матрицу окажется не чем иным, как действие соответствующего эндоморфизма на строку.

[11] Это гомоморфизм колец из теоремы плотности.

$$= (d, *, \ldots, *) \cdot \begin{pmatrix} d_1 & \ldots & d_n \\ 0 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & 0 \end{pmatrix} = (dd_1, \ldots, dd_n) = d \cdot (d_1, \ldots, d_n),$$

откуда следует сюръективность. □

Вспомним, что правый идеал N кольца R называется минимальным, если $N \neq 0$ и он не содержит в себе никаких других правых идеалов кроме нуля и самого себя. Неприводимые подмодули кольца как правого модуля над собой R_R — это в точности минимальные правые идеалы.

Следствие 3.19. Пусть $R = M_n(D)$ — кольцо матриц над телом D. Для каждого $i = 1, \ldots, n$ рассмотрим подмножество

$$V_i^{(n)} = \left\{ \begin{pmatrix} 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{pmatrix} \;\middle|\; a_{i1}, \ldots, a_{in} \in D \right\} \subseteq M_n(D),$$

состоящее из всех матриц, у которых строки с номерами $1, \ldots, i-1, i+1, \ldots, n$ нулевые. Тогда $V_i^{(n)}$ — минимальный правый идеал кольца R. Причём его кольцо эндоморфизмов как правого R-модуля $\operatorname{End} V_i^{(n)} \cong D$.

Доказательство. Из правил матричного произведения сразу получаем, что $V_i^{(n)}$ — правый идеал. Причем $V_i^{(n)}$ изоморфен D^n как правому модулю над $R = M_n(D)$. Осталось применить предыдущее предложение. □

Теорема 3.20 (Молин, Веддербёрн, Артин)**.** Следующие условия эквивалентны.

1) Модуль R_R полупрост.

1') Модуль ${}_RR$ полупрост.

2) Кольцо R раскладывается в конечное прямое произведение колец матриц над телами:

$$R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k),$$

где число k определено единственным образом и пары $(n_1, D_1), \ldots, (n_k, D_k)$ тоже определены однозначно с точностью до перенумерации и замены тел на изоморфные.

Доказательство (единственность разложения покажем позднее). В силу симметричности условия 2) достаточно показать, что 1) $\Leftrightarrow$ 2).

1) $\Rightarrow$ 2) Регулярный модуль R_R заведомо конечно порождён, т.к. порождается одной лишь единицей. Одновременно R_R полупрост, а значит, он раскладывается в

конечную прямую сумму неприводимых подмодулей $R_R = \bigoplus_{i=1}^{d} I_i$ (предложение 3.3). Неприводимые подмодули в R_R — это в точности минимальные правые идеалы кольца R.

Введём на множестве $\{I_1, \ldots, I_d\}$ отношение эквивалентности как изоморфизм модулей. Обозначим через k количество классов эквивалентности. С точностью до перенумерации можно считать, что $I_1, \ldots, I_k$ — представители всех этих классов. Для каждого $j = 1, \ldots, k$ положим n_j равным мощности j-го класса. Тогда, группируя изоморфные слагаемые, можно записать $R_R \cong I_1^{n_1} \oplus \ldots \oplus I_k^{n_k}$, где полагаем $I_j^{n_j} = I_j \oplus \ldots \oplus I_j$ (n_j раз). В силу предложения 3.16 мы получили разложение полупростого модуля R_R на его однородные компоненты $I_j^{n_j}$ с точностью до изоморфизма. По теореме 1.67 $R \cong \operatorname{End} R_R$. По предложению 3.17 $\operatorname{End} R_R \cong \operatorname{End} I_1^{n_1} \times \ldots \times \operatorname{End} I_k^{n_k}$. 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, $R \cong \prod_{j=1}^{k} M_{n_j}(D_j)$.

2) $\Rightarrow$ 1) Для $j = 1, \ldots, k$ обозначим $R_j = M_{n_j}(D_j)$. Применим следствие 3.19. Тогда $R_j = V_1^{(n_j)} \oplus V_2^{(n_j)} \oplus \ldots \oplus V_{n_j}^{(n_j)}$ — прямая сумма правых R_j -модулей, причём все $V_1^{(n_j)}, \ldots, V_{n_j}^{(n_j)}$ неприводимы. Значит, R_j — полупростой правый модуль над собой.

По условию $R = R_1 \times \ldots \times R_k$. Обозначим,

$$W_{ij} = (O_{n_1}, \ldots, O_{n_{j-1}}, V_i^{(n_j)}, O_{n_{j+1}}, \ldots, O_{n_k}) \subseteq R, \quad j = 1, \ldots, k;\ i = 1, \ldots n_j.$$

Тогда W_{ij} — правый идеал кольца R. Так как $V_i^{(n_j)}$ — неприводимый правый R_j-модуль, то W_{ij} — неприводимый правый R-модуль. Тогда

$$R_R = \bigoplus_{j=1}^{k} (O, \ldots, O, R_j, O, \ldots, O) = \bigoplus_{j=1}^{k} \bigoplus_{i=1}^{n_j} W_{ij}$$

является разложением в сумму неприводимых R-модулей, откуда R_R полупрост. $\square$

Определение 3.21. Кольцо R называется *полупростым*[12], если R_R (эквивалентно ${}_R R$) является полупростым модулем. Для таких колец также используются термины *классически полупростое кольцо* и *вполне приводимое кольцо.*

По теореме Веддербёрна-Артина, полупростое кольцо всегда изоморфно конечному прямому произведению колец матриц над телами.

Предложение 3.22. Полупростое кольцо является артиновым и нётеровым как справа, так и слева.

[12]Иногда этот термин используется в другом значении. Дальше мы встретимся с полупростыми кольцами в смысле Джекобсона.

Доказательство. Модуль R_R раскладывается в конечную прямую сумму неприводимых подмодулей. Каждый неприводимый модуль является и артиновым, и нётеровым тривиальным образом. Однако конечная прямая сумма артиновых (нётеровых) модулей снова артинов (нётеров) модуль (следствие 2.4). Для ${}_RR$ рассуждения аналогичны. □

Предложение 3.23. Пусть R — полупростое кольцо. Тогда все правые и все левые модули над ним являются полупростыми.

Доказательство. Каждый модуль M является фактормодулем некоторого свободного модуля F, т.е. $M \cong F/K$ для подходящего подмодуля $K \leqslant F$ (предложение 1.51). В то же время свободный модуль изоморфен прямой сумме некоторого количества копий регулярного модуля: $F \cong \bigoplus\limits_{i \in I} R_R$ (предложение 1.49). Однако модуль R_R полупрост, т.е. является суммой неприводимых подмодулей. Но тогда F тоже окажется суммой неприводимых, следовательно, F полупрост. При этом M — фактормодуль модуля F, а значит, тоже полупрост. □

Задачи к лекции 7.

Задача 1. Пусть M — конечно порождённый модуль над полупростым кольцом. Докажите, что кольцо $\operatorname{End}(M)$ полупросто.

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

Задача 3. Покажите, что любое поле является полупростым кольцом.

Задача 4. Покажите, что ни для какой конечной группы G групповое кольцо $\mathbb{Z}G$ не полупросто.

Задача 5. Является ли полупростым кольцо $M_n(\mathbb{Z})$?

Задача 6. Покажите, что прямое произведение колец $R = R_1 \times R_2$ полупросто тогда и только тогда, когда полупросты сомножители R_1 и R_2.

Задача 7. Покажите, что произвольнго идеала I полупростого кольца R фактор кольцо R/I тоже полупросто.

Лекция 8. Описание неприводимых модулей над полупростым кольцом. Теорема Веддербёрна-Артина для простых колец и для алгебр над полем. Пример простого не полупростого кольца.

Теорема 3.24 (Описание неприводимых модулей над полупростым кольцом)**.** Пусть R — полупростое кольцо. Тогда любой неприводимый правый R-модуль изоморфен некоторому минимальному правому идеалу кольца R. Далее пусть известно разложение $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$. Обозначим

$$V_i^{(n_j)} = \left\{ \begin{pmatrix} 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{i1} & a_{i2} & \ldots & a_{in_j} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{pmatrix} \middle| \; a_{i1}, \ldots, a_{in_j} \in D_j \right\} \subseteq M_{n_j}(D_j),$$

$$W_{ij} = (O_{n_1}, \ldots, O_{n_{j-1}}, V_i^{(n_j)}, O_{n_{j+1}}, \ldots, O_{n_k}) \subseteq R, \quad j = 1, \ldots, k;\; i = 1, \ldots n_j.$$

Тогда для каждого $j = 1, \ldots, k$ имеется изоморфизм правых R-модулей:

$$W_{1j} \cong W_{2j} \cong ... \cong W_{n_j j}.$$

При этом их кольца эндоморфизмов

$$\operatorname{End} W_{ij} \cong D_j, \quad i = 1, \ldots n_j.$$

Модули $W_{11}, W_{12}, \ldots, W_{1k}$ попрано не изоморфны. Произвольный неприводимый правый[13] R-модуль изоморфен одному из $W_{11}, W_{12}, \ldots, W_{1k}$. В частности, существует ровно k неприводимых правых R-модулей с точностью до изоморфизма.

Доказательство. Всякий неприводимый правый R-модуль M изоморфен R_R/N, где $N \leqslant R_R$ — максимальный правый идеал. По критерию полупростоты N выделяется в R_R прямым слагаемым, т.е. $R_R = N \oplus N'$ для некоторого подмодуля $N' \leqslant R_R$. Но тогда $N' \cong R_R/N \cong M$, а значит, N' неприводим. Но неприводимые подмодули в R_R — это в точности минимальные правые идеалы.

Пусть $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$. Из доказательства теоремы Веддербёрна-Артина мы знаем, что $R_R = \bigoplus W_{ij}$ — разложение в сумму неприводимых модулей. По предыдущему, произвольный неприводимый правый R-модуль изоморфен некоторому минимальному правому идеалу $N' \leqslant R_R = \bigoplus W_{ij}$. Тогда N' должен быть изоморфен одному из W_{ij} в силу следствия 3.8.

Зафиксируем $j \in \{1, \ldots, k\}$ и выберем произвольные $\alpha, \beta \in \{1, \ldots, n_j\}$. Покажем, что $W_{\alpha j} \cong W_{\beta j}$ как R-модули. Рассмотрим матричную единицу $E_{\alpha\beta}$ размера $n_j \times n_j$ и положим

$$F_{\alpha\beta} = (O_{n_1}, \ldots, O_{n_{j-1}}, E_{\alpha\beta}, O_{n_{j+1}}, \ldots, O_{n_k}) \in R.$$

Определим отображение $W_{\beta j} \longrightarrow W_{\alpha j}$ как умножение на $F_{\alpha\beta}$ <u>слева</u>. Так как модули <u>правые</u>, то такое отображение действительно будет гомоморфизмом модулей. Кроме

[13]Для левых модулей нужно будет вместо $V_i^{(n_j)}$ рассмотреть аналогичные левые идеалы, где вместо ненулевой строки берется ненулевой столбец.

того, ограничение этого отображения на j-й прямой множитель $M_{n_j}(D_j)$ переносит строку с номером α на место строки с номером β. Отсюда следует инъективность и сюръективность.

Теперь зафиксируем $\alpha, \beta \in \{1, \ldots, k\}$ и покажем, что $W_{1\alpha} \ncong W_{1\beta}$. Рассмотрим единичную матрицу E размера $n_\alpha \times n_\alpha$ и положим

$$F = (O_{n_1}, \ldots, O_{n_{\alpha-1}}, E, O_{n_{\alpha+1}}, \ldots, O_{n_k}) \in R.$$

Тогда $w \cdot F = w$ для всех $w \in W_{1\alpha}$, но $W_{1\beta} \cdot F = O$. Рассмотрим произвольный гомоморфизм $\phi : W_{1\alpha} \longrightarrow W_{1\beta}$, тогда $\phi(w) = \phi(w \cdot F) = \phi(w) \cdot F = O$. Значит, ϕ может быть только нулевым, отсюда $W_{1\alpha} \ncong W_{1\beta}$.

Покажем, что $\operatorname{End} W_{ij} \cong D_j$. В силу следствия 3.19 достаточно поверить, что кольцо эндоморфизмов правого R-модуля W_{ij} изоморфно кольцу эндоморфизмов правого модуля $V_i^{(n_j)}$ над кольцом $M_{n_j}(D_j)$. Действительно, если $\phi \in \operatorname{End} V_i^{(n_j)}$, тогда определим $\widetilde{\phi} \in \operatorname{End} W_{ij}$ по правилу

$$\widetilde{\phi}(O, \ldots, A, \ldots, O) = (O, \ldots, \phi(A), \ldots, O), \quad A \in V_i^{(n_j)}.$$

Тогда

$$\begin{aligned}
\widetilde{\phi}((O, \ldots, A, \ldots, O) + (O, \ldots, A', \ldots, O)) = \widetilde{\phi}(O, \ldots, A + A', \ldots, O) = \\
= (O, \ldots, \phi(A + A'), \ldots, O) = (O, \ldots, \phi(A) + \phi(A'), \ldots, O) = \\
= (O, \ldots, \phi(A), \ldots, O) + (O, \ldots, \phi(A'), \ldots, O) = \\
= \widetilde{\phi}(O, \ldots, A, \ldots, O) + \widetilde{\phi}(O, \ldots, A', \ldots, O).
\end{aligned}$$

Для любого $(B_1, \ldots, B_k) \in R$ имеем

$$\begin{aligned}
\widetilde{\phi}((O, \ldots, A, \ldots, O) \cdot (B_1, \ldots, B_k)) = \widetilde{\phi}(O, \ldots, AB_j, \ldots O) = \\
= (O, \ldots, \phi(AB_j), \ldots, O) = (O, \ldots, \phi(A)B_j, \ldots, O) = \\
= (O, \ldots, \phi(A), \ldots, O) \cdot (B_1, \ldots, B_k) = \\
= \widetilde{\phi}(O, \ldots, A, \ldots, O) \cdot (B_1, \ldots, B_k),
\end{aligned}$$

откуда $\widetilde{\phi}$ действительно является эндоморфизмом правого R-модуля W_{ij}. В силу того, что операции на прямом произведении заданы покомпонентно, то сразу из определения $\widetilde{\phi}$ получаем $\widetilde{\phi_1 + \phi_2} = \widetilde{\phi_1} + \widetilde{\phi_2}$, а также $\widetilde{\phi_1 \circ \phi_2} = \widetilde{\phi_1} \circ \widetilde{\phi_2}$ и $\widetilde{\mathrm{id}} = \mathrm{id}$. Кроме того, тоже по определению отображение $\phi \mapsto \widetilde{\phi}$ инъективно.

Осталось проверить сюръективность построенного гомоморфизма колец эндоморфизмов $\operatorname{End} V_i^{(n_j)} \longrightarrow \operatorname{End} W_{ij}$, $\phi \mapsto \widetilde{\phi}$. Выберем произвольный $f \in \operatorname{End} W_{ij}$. Тогда для каждого $A \in V_i^{(n_j)}$ найдётся $B \in V_i^{(n_j)}$, что $f(O, \ldots, A, \ldots, O) = (O, \ldots, B, \ldots, O)$. Положим $\psi(A) = B$. Непосредственные проверки аналогичные тем, что проводились для $\widetilde{\phi}$, показывают, что ψ — эндоморфизм модуля $V_i^{(n_j)}$, причём $\widetilde{\psi} = f$. $\square$

Доказательство единственности в теореме Молина-Веддербёрна-Артина. Сначала отметим, что число k определено однозначно как количество попарно неизоморфных неприводимых правых R-модулей. Далее пусть имеется изоморфизм колец

$$R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k) \cong M_{\widetilde{n}_1}(\widetilde{D}_1) \times \ldots \times M_{\widetilde{n}_{\widetilde{k}}}(\widetilde{D}_k).$$

Тогда найдутся два разложения модуля R_R в сумму неприводимых:

$$\bigoplus_{j=1}^{k} \bigoplus_{i=1}^{n_j} W_{ij} \cong R_R \cong \bigoplus_{j=1}^{k} \bigoplus_{i=1}^{\widetilde{n}_j} \widetilde{W}_{ij}.$$

По предложению 3.10 прямые слагаемые в обоих суммах можно упорядочить так, чтобы они оказались попарно изоморфны. Пусть W_{11} оказался изоморфен $\widetilde{W}_{ij}$. Однако $W_{11} \cong W_{21} \cong ... \cong W_{n_1 1}$ и остальные слагаемые им не изоморфны. Точно так же $\widetilde{W}_{1j} \cong \widetilde{W}_{2j} \cong ... \cong \widetilde{W}_{\widetilde{n}_j j}$ и остальные слагаемые им не изоморфны. Снова по предложению 3.10 получаем, что $n_1 = \widetilde{n}_j$. Далее убираем все слагаемые $\{W_{11}, W_{21}, ..., W_{n_1 1}\}$ в первой сумме и все слагаемые $\{\widetilde{W}_{1j}, \widetilde{W}_{2j}, ..., \widetilde{W}_{\widetilde{n}_j j}\}$ во второй сумме. Теперь мы можем осуществить индукцию по k. База индукции $k = 0$ соответствует пустой сумме неприводимых R-модулей, этот случай тривиален.

Итак, можно считать, что $n_j = \widetilde{n}_j$, $W_{ij} \cong \widetilde{W}_{ij}$ для всех i, j. Тогда

$$D_j \cong \operatorname{End} W_{1j} \cong \operatorname{End} \widetilde{W}_{1j} \cong \widetilde{D}_j, \quad j = 1, \ldots, k,$$

откуда получаем, что тела тоже определены однозначно. □

Определение 3.25 (напоминание)**.** *Простое кольцо* — это кольцо, в котором ровно два собственных идеала: $\{0\}$, R.

Как мы увидим дальше простое кольцо необязательно полупросто. Однако при условии артиновости эти классы колец действительно оказываются связаны между собой.

Теорема 3.26 (Строение простых артиновых колец)**.** Следующие условия на кольцо R эквивалентны:

1) R простое и артиново справа;
2) R полупростое и все неприводимые правые R-модули изоморфны;
3) $R \cong M_n(D)$, D — тело;
1'), 2') левые аналоги 1), 2).

Натуральное n определено единственным образом и тело D определено однозначно с точностью до изоморфизма.

Доказательство. В силу симметричности 3) достаточно доказать эквивалентность условий 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 теоремы 3.24.

2) $\Rightarrow$ 3) По теореме о строении неприводимых модулей над полупростым кольцом получаем $k = 1$.

3) $\Rightarrow$ 1) Простота кольца $R = M_n(D)$ доказана ранее (следствие 1.24). Так как кольцо $M_n(D)$ полупросто, то оно артиново (предложение 3.22). $\square$

Пусть теперь $\mathbb{F}$ — произвольное поле, R — ассоциативная алгебра с единицей над $\mathbb{F}$. Тогда можно отождествить $\mathbb{F}$ с множеством скалярных элементов алгебры $\{\lambda \cdot 1_R \mid \lambda \in \mathbb{F}\}$. Поэтому далее считаем, что $\mathbb{F} \subseteq R$.

Каждый R-модуль M является также и модулем над $\mathbb{F}$, т.к. $\mathbb{F} \subseteq R$. Другими словами, M является одновременно и линейным пространством над полем $\mathbb{F}$.

Для каждого $\lambda \in \mathbb{F}$ определён эндоморфизм модуля $\phi_\lambda : M \longrightarrow M$, $\phi_\lambda(m) = m\lambda$. Это корректно определённый эндоморфизм т.к. все элементы поля лежат в центре кольца. Причём для любого эндоморфизма $\phi \in \operatorname{End} M$ выполнено

$$\phi_\lambda(\phi(m)) = \phi(m)\lambda = \phi(m\lambda) = \phi(\phi_\lambda(m)), \quad m \in M.$$

Таким образом, все ϕ_λ лежат в центре кольца эндоморфизмов. В дальнейшем вместо ϕ_λ будем писать просто λ. Получается, что $\operatorname{End} M$ естественным образом тоже является алгеброй над полем $\mathbb{F}$.

Лемма 3.27. 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. Каждый R-эндоморфизм $\varphi \in \operatorname{End} M_R$ является одновременно $\mathbb{F}$-линейным оператором на $M_\mathbb{F}$. В силу алгебраической замкнутости поля он обладает собственным значением $\lambda \in \mathbb{F}$. Значит, 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 $\operatorname{End} M_R \cong \mathbb{F}$. $\square$

Теорема 3.28 (Молин, Веддербёрн, Артин, об алгебрах)**.** Пусть R — ассоциативная алгебра с единицей над полем $\mathbb{F}$. Следующие условия эквивалентны.

1) Модуль R_R полупрост.

1') Модуль ${}_RR$ полупрост.

2) Алгебра R раскладывается в конечную прямую сумму $\mathbb{F}$-алгебр матриц:

$$R \cong M_{n_1}(D_1) \oplus \ldots \oplus M_{n_k}(D_k),$$

где D_j являются алгебрами с делением над полем $\mathbb{F}$. Число k определено единственным образом и пары $(n_1, D_1), \ldots, (n_k, D_k)$ тоже определены однозначно с точностью до перенумерации и алгебр с делением на изоморфные.

В случае $\dim_{\mathbb{F}} R < \infty$, выполнено $\dim_{\mathbb{F}} D_j < \infty$ для всех j. Если $\dim_{\mathbb{F}} R < \infty$ и поле $\mathbb{F}$ алгебраически замкнуто то $D_j \cong \mathbb{F}$ для всех j.

Доказательство. Доказательство точно такое же как в теореме Молина-Веддербёрна-Артина для колец. Непосредственно проверяется, что все используемые в доказательстве изоморфизмы колец являются также изоморфизмами алгебр. Мы опустим эти технические проверки. Полное доказательство можно найти, например, в книге Ричарда Пирса «Ассоциативные алгебры», Мир, 1986.

Пусть $\dim_{\mathbb{F}} R < \infty$. Если для хотя бы одного j выполнено $\dim_{\mathbb{F}} D_j = \infty$, то тогда $\dim_{\mathbb{F}}(M_{n_1}(D_1) \oplus \ldots \oplus M_{n_k}(D_k)) = \infty$, противоречие. Значит, $\dim_{\mathbb{F}} D_j < \infty$ для всех j. Пусть при этом $\mathbb{F}$ алгебраически замкнуто. В доказательстве теоремы Молина-Веддербёрна-Артина тела D_j являются кольцами эндоморфизмов неприводимых R-модулей. Тогда по предыдущей лемме $D_j \cong \mathbb{F}$. $\square$

Далее мы приведём классический пример простого, но не полупростого кольца.

Определение 3.29. Первая *алгебра Вейля* над полем $\mathbb{F}$ определяется как как фактор свободной алгебры $A_1(\mathbb{F}) = \mathbb{F}\langle x, y\rangle / (yx - xy - 1)$ по идеалу порождённому элементом $yx - xy - 1$.

Зададим на алгебре многочленов $\mathbb{F}[x]$ 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.

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

Предложение 3.30. 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. $\square$

Следствие 3.31. Существует простое, но не артиново кольцо. В частности, существует простое, но не полупростое кольцо.

Задачи к лекции 8.

Задача 1. 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 2. Покажите, что если в группе G содержится больше одного элемнта, то групповая алгебра $\mathbb{F}G$ не является простой.

Задача 3. Изоморфны ли групповые кольца $\mathbb{R}\mathbb{Z}_4$ и $\mathbb{R}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$?

Задача 4. Найдите разложение в прямое произведение матричных колец кольца $\mathbb{R}Q_8$.

Задача 5. Пусть A— конечномерная алгебра над полем. Докажите, что кольцо $M_n(A)$— полупросто тогда и только тогда, когда A— полупроста.

Задача 6. При каких n кольцо вычетов $\mathbb{Z}_n$ полупросто?

4 Радикал Джекобсона

Лекция 9. Радикал модуля. Радикал Джекобсона 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 подмодулей. □

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 2.4).

($\Leftarrow$) 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 $\varphi\colon M \to (M/M_{i_1}) \oplus \ldots \oplus (M/M_{i_n})$, $m \mapsto (m + M_{i_1}, \ldots, m + M_{i_n})$ — 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.

Доказательство. Радикал Джекобсона является пересечением правых идеалов, поэтому он сам окажется правым идеалом. Однако радикал еще и совпадает с пересечением левых идеалов. □

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 $\mathrm{Ann}\, M = \{r \in R \mid mr = 0 \ \ \forall m \in M\}$.

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

Доказательство. Переформулировка пунктов 1), 1') теоремы. $\square$

Для правого R-модуля M и некоторого подмножества $S \subseteq R$ положим $\mathrm{Ann}\,_M(S) = \{m \in M \mid ms = 0 \; \forall s \in S\}$. 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 $\mathrm{soc}\, M \subseteq \mathrm{Ann}\,_M(J(R))$. Если же факторкольцо $R/J(R)$ полупросто, то $\mathrm{soc}\, M = \mathrm{Ann}\,_M(J(R))$.

Доказательство. По определению цоколь является суммой всех неприводимых подмодулей, поэтому включение $\mathrm{soc}\, M \subseteq \mathrm{Ann}\,_M(J(R))$ вытекает из пункта 1) теоремы. Пусть $R/J(R)$ полупросто. Обозначим $N = \mathrm{Ann}\,_M(J(R))$, $\overline{R} = R/J(R)$. Надо доказать, что $N \subseteq \mathrm{soc}\, M$. На N естественным образом вводится струтура $\overline{R}$-модуля: $m(r + J(R)) = mr$. Так как 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. Но отсюда для всех $n \in N_i \setminus \{0\}$ выполнено $nR = n\overline{R} = N_i$. Значит, каждый модуль N_i является неприводимым и над кольцом R тоже. Итак, $N_R = \bigoplus_{i\in I}(N_i)_R$, и все $(N_i)_R$ неприводимы. Поэтому $N_i \subseteq \mathrm{soc}\, M$ для всех i, откуда $N \subseteq \mathrm{soc}\, M$, что и требовалось. $\square$

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. $\square$

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 (применим лемму 4.3 к модулю R_R),
- 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 правых идеалов, применённой к максимальным правым идеалам кольца R.

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). $\square$

Нам понадобится следующее вспомогательное утверждение.

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

Доказательство. Если модуль R_R артинов, то R/I — артинов правый R-модуль (предложение 2.3). 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. $\square$

Аналогичное утверждение для подколец неверно.

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

Доказательство. По предыдущему предложению факторкольцо $R/J(R)$ артиново справа. При этом, как уже отмечалось в примерах, $J(R/J(R)) = 0$. Остаётся применить предыдущее следствие. $\square$

Задачи к лекции 9.

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

Задача 2. 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 3. Для любого $n > 1$ и кольца R покажите, что $J(M_n(R)) = M_n(J(R))$.

Задача 4. Найдите $J(R[x])$ для коммутативного кольца коэффициентов R.

Задача 5. Пусть R — полупримитивное кольцо и F — свободный правый R-модуль. Покажите, что $\operatorname{rad} F = 0$.

Задача 6. 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 7. Докажите, что если в правом идеале I все элементы квазирегулярны справа, то I квазирегулярен.

Лекция 10. Нильпотентность радикала артинова кольца. Лемма Накаямы. Теорема Акидзуки–Хопкинса–Левицкого.

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. Рассмотрим кольцо многочленов от счётного числа коммутирующих переменных $\mathbb{Q}[x_2, \ldots, x_n, \ldots]$, где для удобства нумерация переменных начинается с двойки. Обозначим через I идеал, порождённый 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 J, порождённый множеством $\{x_2 + I, \ldots, x_n + I, \ldots\}$, является нильидеалом, но не нильпотентен. Более того, индексы нильпотентности элементов идеала J не ограничены.

Доказательство. Рассмотрим произвольный многочлен $f \in \mathbb{Q}[x_2, \ldots, x_n, \ldots]$ без свободного члена. Пусть n — это наибольший номер переменной, от которой многочлен f зависит нетривиально. Тогда

$$f(x_2, \ldots, x_n) = \sum_{k_2, \ldots, k_n = 0}^{\infty} a_{k_2, \ldots, k_n} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n},$$

где лишь конечное число коэффициентов $a_{k_2, \ldots, k_n}$ отлично от нуля. Пусть $m \in \mathbb{N}$ равно числу ненулевых слагаемы в этой сумме. Тогда f можно переписать в виде суммы мономов $f = g_1 + \ldots + g_m$. Если моном g_i делится на переменную x_j, то, возводя в степень n, получаем, что g_i^n делится на $x_j^n = x_j^{n-j} \cdot x_j^j \in I$. Поэтому все $g_1^n, \ldots, g_m^n$ лежат в идеале I.

Теперь возведём многочлен f в степень mn:

$$f^{mn} = (g_1 + \ldots + g_m)^{mn}.$$

Раскрывая скобки, получим, что каждое слагаемое имеет вид $g_1^{\ell_1} \cdot \ldots \cdot g_m^{\ell_m}$, где $\ell_1 + \ldots + \ell_m = mn$. По принципу Дирихе для хотя бы одного ℓ_i выполнено $\ell_i \geqslant n$. Значит, все слагаемые лежат в идеале I, откуда и сам многочлен f^{mn} лежит в идеале I.

Наконец перейдём в факторкольцо $R = \mathbb{Q}[x_2, \ldots, x_n, \ldots]/I$. Произвольный элемент идеала J имеет вид $f(x_2 + I, \ldots, x_n + I)$. Тогда

$$(f(x_2 + I, \ldots, x_n + I))^{mn} = (f(x_2, \ldots, x_n) + I)^{mn} = f^{mn} + I = 0 + I,$$

откуда вытекает, что J является нильидеалом.

С другой стороны, элемент $x_k + I$ имеет индекс нильпотентности k. Рассматривая все возможные натуральные $k \geqslant 2$, получаем, что индексы нильпотентности элементов идеала J не ограничены. В частности, этот идеал не может быть нильпотентен. $\square$

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. $\square$

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 $L \in \Omega$. $\square$

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. $\square$

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 $(M/N)r = 0$ для всех $r \in J(R)$, 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: $M/N = (MI + N)/N$. Заметим, что $(MI+N)/N$ совпадает с аддитивной подгруппой в M/N, порождённой всеми элементами вида $\{mr + N \mid m \in M,\ r \in I\}$. Это множество можно переписать как $\{(m + N)r \mid m \in M,\ r \in I\}$. Однако аддитивная подгруппа, порождённая таким множеством совпадает с $(M/N)I$. Таким образом, $M/N = (M/N)I$, откуда $M/N \subseteq (M/N)J(R)$. Обратное включение очевидно. Значит, $M/N = (M/N)J(R)$ и $M/N = 0$ по предыдущей лемме. □

Предложение 4.31. Пусть M — полупростой R-модуль. Тогда следующие условия эквивалентны:

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

Доказательство. 1) $\Rightarrow$ 2) Пусть $M = \bigoplus\limits_{i \in I} S_i$ — разложение в сумму неприводимых модулей. Покажем, что в силу артиновости эта сумма может содержать лишь конечное число слагаемых. От противного, пусть I бесконечно. Выберем счётное подмножество $\{i_1, i_2, \ldots\} \subseteq I$. Тогда цепь подмодулей

$$\bigoplus_{j=1}^{\infty} S_{i_j} \supsetneq \bigoplus_{j=2}^{\infty} S_{i_j} \supsetneq \bigoplus_{j=3}^{\infty} S_{i_j} \supsetneq \ldots$$

является бесконечной строго убывающей, что противоречит артиновости. Итак, $M = S_1 \oplus \ldots \oplus S_n$ — конечная сумма неприводимых, а значит, нётеровых модулей. Отсюда M нётеров (следствие 2.4).

2) $\Rightarrow$ 3) Любой подмодуль нётерова модуля конечно порождён.

3) $\Rightarrow$ 4) Так как полупростой модуль M конечно порождён, то он раскладывается в конечную прямую сумму неприводимых $M = S_1 \oplus \ldots \oplus S_n$, см. предложение 3.3. Тогда

$$0 \subseteq S_1 \subseteq S_1 \oplus S_2 \subseteq S_1 \oplus S_2 \oplus S_3 \subseteq \ldots \subseteq S_1 \oplus \ldots \oplus S_n = M$$

является композиционным рядом, т.к. все его факторы изоморфны модулям S_i, а значит, неприводимы.

4) $\Rightarrow$ 1) Модуль, обладающий композиционным рядом, одновременно и артинов, и нётеров (следствие 2.24). □

Теорема 4.32 (Акидзуки, Хопкинс, Левицкий)**.** Пусть кольцо R *полупримарно*, т.е. радикал Джекобсона $J(R)$ нильпотентен, а фактор по нему $\overline{R} = R/J(R)$ является полупростым кольцом. Тогда для произвольного правого R-модуля M следующие условия эквивалентны:

1) M артинов;

2) M нётеров;

3) M обладает композиционным рядом.

Доказательство. Обозначим $J = J(R)$. Выберем натуральное n таким, что $J^n = 0$, но $J^{n-1} \neq 0$. Построим конечную цепь подмодулей

$$M \supseteq MJ \supseteq MJ^2 \supseteq \ldots \supseteq MJ^{n-1} \supseteq MJ^n = 0.$$

Рассмотрим факторы этой цепи $F_i = MJ^{i-1}/MJ^i$, где $i = 1, 2, \ldots n$ и формально полагаем $J^0 = R$. Тогда $F_i J = 0$ при любом i. Значит, на F_i можно задать структуру модуля над кольцом $\overline{R} = R/J$ по правилу $f(r + J) = fr$ для всех $f \in F_i$, $r \in R$.

Заметим, что произвольное подмножество $X \subseteq F_i$ является подмодулем над R тогда и только тогда, когда X является подмодулем над $\overline{R}$. Следовательно, F_i — артинов (нётеров) R-модуль в том и только в том случае, когда F_i — артинов (нётеров) $\overline{R}$-модуль.

1) $\Rightarrow$ 2) Пусть R-модуль M артинов, тогда его подмодуль MJ^{i-1} тоже артинов. Однако F_i — это фактормодуль модуля MJ^{i-1}, поэтому F_i — артинов R-модуль. Тогда по предыдущему F_i — артинов модуль над кольцом $\overline{R}$. По условию $\overline{R}$ — полупростое кольцо, а значит, все модули над ним полупросты. В частности, F_i — полупростой $\overline{R}$-модуль. В этом случае из артиновости следует нётеровость (предложение 4.31). Итак, все $F_1, \ldots, F_n$ являются нётеровыми $\overline{R}$-модулям. Значит, $F_1, \ldots, F_n$ — нётеровы R-модули.

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 2.3). Продолжая таким же образом, получаем, что все модули $MJ^{n-1}, MJ^{n-2}, MJ^{n-3}, \ldots, MJ, M$ нётеровы. В частности, исходный модуль M нётеров, что и требовалось.

2) $\Rightarrow$ 1) Достаточно в предыдущем рассуждении всюду поменять местами артиновость и нётеровость.

3) $\Leftrightarrow$ 1) & 2) Верно для любого модуля (следствие 2.24). □

Следствие 4.33. Для кольца R следующие условия эквивалентны:

1) R артиново справа;

2) R нётерово справа, радикал Джекобсона $J(R)$ нильпотентен, а фактор по нему $\overline{R} = R/J(R)$ — полупростое кольцо.

Доказательство. 1) $\Rightarrow$ 2) Радикал Джекобсона артинова справа кольца всегда нильпотентен (теорема 4.25). Также фактор артинова справа кольца по радикалу Джекобсона — полупростое кольцо (следствие 4.19). Применяя предыдущую теорему к модулю R_R, получаем что из его артиновости следует нётеровость.

2) $\Rightarrow$ 1) Снова применяем предыдущую теорему к модулю R_R. $\square$

Следствие 4.34. Артиново справа кольцо (напомним: с единицей!) нётерово справа.

Доказательство. Частный случай предыдущего следствия. $\square$

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).

Следствие 4.35. Конечно порождённый правый модуль над артиновым справа кольцом является нётеровым.

Доказательство. Конечно порождённый правый модуль над артиновым справа кольцом сам является артиновым, см. предложение 2.13. Поэтому снова применима теорема Акидзуки–Хопкинса–Левицкого. $\square$

Определение 4.36. 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 4.37. 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 $a = 0$. $\square$

Пример 4.38. 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 10.

Задача 1. Постройте коммутативное кольцо R, радикал Джекобсона $J(R)$ которого имеет индекс нильпотентности 3, но все элементы $J(R)$ имеют нулевые квадраты.

Задача 2. Найдите $J(\mathbb{F}_2 Q_8)$, укажите его индекс нильпотентности.

Задача 3. 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 4. Докажите, что для произвольного семейства колец $\{R_i\}_{i\in I}$ выполнено равенство $J(\prod_{i\in I} R_i) = \prod_{i\in I} J(R_i)$.

Задача 5. Докажите, что в коммутативном кольце сумма обратимого элемента и нильпотента обратима. Верно ли это для некоммутативных колец?

Задача 6. Докажите, что сумма двух ниль-идеалов является ниль-идеалом. Аналогичный вопрос о сумме двух правых ниль-идеалов — это известная проблема Кёте (1930 г.).

5 Локальные, полулокальные и полусовершенные кольца. Поднятие идемпотентов.

Лекция 11. Локальные кольца. Идемпотенты кольца и их связь с разложением в прямую сумму. Критерий локальности артинова кольца

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. $R = R^\times \cup J(R)$;
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) Так как $J(R)$ — 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. Тогда r лежит в некотором максимальном правом идеале (предложение 1.36). Но $J(R)$ — единственный максимальный правый идеал, откуда $r \in J(R)$. Если r необратим слева, то рассуждения аналогичны.

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 $a \notin J(R)$. Так как $J(R)$ совпадает с пересечением максимальных правых идеалов, то 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 $1 = n + ar$. Так как 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, но это одно из эквивалентных определений тела (теорема 1.59).

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

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.

Нулевое кольцо не является локальным по определению.

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 $(1 + x + \ldots + x^{n-1})$. $\square$

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. Элемент необратим справа (слева) тогда и только тогда, когда он лежит в некотором максимальном правом (левом) идеале, см. предложение 1.36. Так как кольцо локально, то этот правый (левый) идеал совпадает с $J(R)$. Однако $J(R)$ — собственный идеал, поэтому указанный элемент необратим с двух сторон. $\square$

Пример 5.7.

- Любое тело (в том числе любое поле) — тривиальный пример локального кольца. В этом случае, радикал Джекобсона равен нулю.

- Кольцо вычетов $\mathbb{Z}_n$ локально тогда и только тогда, когда $n = p^k$ для некоторого простого p. Действительно, в этом случае все необратимые элементы — это в точности элементы идеала $p\mathbb{Z}_{p^k}$. Обратно, если предположить, что n делится на два различных простых числа p, q, то, выбирая $m, \ell \in \mathbb{Z}$ такими, что $pm+q\ell = 1$, получаем $p\mathbb{Z}_n + q\mathbb{Z}_n = \mathbb{Z}_n$, откуда вычеты $\overline{p}, \overline{q}$ не лежат в одном собственном идеале, но они необратимы.

- Для простого[14] числа p рассмотрим множество $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$, состоящее из дробей, у которых в несократимом виде знаменатель не делится на p. Тогда необратимые элементы в $\mathbb{Z}_{(p)}$ имеют вид $\frac{m}{n}$, где m делится на p, но n не делится на p. Все такие дроби образуют собственный идеал, а значит, $\mathbb{Z}_{(p)}$ является локальным.

- Если D — тело, то локальным является кольцо R, состоящее из таких верхнетреугольных $n \times n$ матриц A над телом D, что $a_{11} = a_{22} = \ldots = a_{nn}$. Такая матрица необратима тогда и только тогда, когда её диагональные элементы равны нулю. Но треугольные матрицы с нулевой диагональю нильпотенты, откуда кольцо R локально. В частности, $J(R)$ совпадает с множеством матриц с нулевой диагональю, и $R/J(R) \cong D$.

Определение 5.8. Элемент e кольца R называется *идемпотентом*, если $e^2 = e$.

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

Если $e \in R$ — идемпотент, тогда $f = 1 - e$ — это тоже идемпотент, т.к.

$$f^2 = (1 - e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e = f.$$

[14]Если p не простое, то указанное множество не будет замкнуто относительно умножения. Приведённая конструкция является примером локализации коммутативного кольца (в данном случае кольца $\mathbb{Z}$).

Иногда f называют *дополнением* идемпотента e. Отметим, что идемпотенты e, f всегда *ортогональны*, т.е.

$$fe = (1-e)e = e - e^2 = 0, \qquad ef = e(1-e) = e - e^2 = 0.$$

Определение 5.9. Множество идемпотентов $\{e_1, \ldots, e_n\} \subseteq R$ называется *ортогональным*, если $e_i e_j = e_j e_i = 0$ для любых $i \neq j$.

Определение 5.10. Множество идемпотентов $\{e_1, \ldots, e_n\} \subseteq R$ называется *полным*, если $e_1 + \ldots + e_n = 1$.

Пример 5.11. Приведём примеры полных ортогональных множеств идемпотентов:

- Множество всех диагональных матричных единиц $\{E_{ii} \mid i = 1, \ldots, n\}$ в кольце матриц $M_n(R)$.
- Если e — произвольный идемпотент кольца R, то пара $\{e, f\}$, где $f = 1 - e$, является полным ортогональным множеством из двух идемпотентов.

Для каждого идемпотента e можно рассмотреть порождённые им правый eR и левый Re идеалы, а также множество

$$eRe = \{ere \mid r \in R\}.$$

Тогда

$$ere + ese = e(re + es)e \in eRe, \quad (ere) \cdot (ese) = e(res)e \in eRe, \quad e(ere) = ere = (ere)e,$$

а значит, $\underline{eRe \text{ — это кольцо с единицей } e}$. Отметим, что в рамках наших определений нельзя назвать eRe подкольцом в R, т.к. у него другая единица.

Предложение 5.12 (Разложение Пирса)**.** Пусть $\{e_1, \ldots, e_n\} \subseteq R$ — полное ортогональное множество идемпотентов. Тогда правый и левый регулярные модули раскладываются во (внутреннюю) прямую сумму:

1) $R_R = e_1 R \oplus \ldots \oplus e_n R$,

1') ${}_R R = Re_1 \oplus \ldots \oplus Re_n$.

Кроме того, имеется разложение кольца R во (внутреннюю) прямую сумму аддитивных подгрупп:

2) $R = \bigoplus\limits_{i,j=1}^{n} e_i R e_j$.

Причём отображение $r \mapsto (e_i r e_j)_{i,j=1}^n$, $r \in R$ задаёт изоморфизм между кольцом R и кольцом матриц:

$$R \cong \begin{pmatrix} e_1Re_1 & e_1Re_2 & \ldots & e_1Re_n \\ e_2Re_1 & e_2Re_2 & \ldots & e_2Re_n \\ \ldots & \ldots & \ldots & \ldots \\ e_nRe_1 & e_nRe_2 & \ldots & e_nRe_n \end{pmatrix} \subseteq M_n(R).$$

Доказательство. 1) Для каждого $r \in R$ имеем $1 \cdot r = (\sum_{i=1}^n e_i)r = \sum_{i=1}^n e_i r$, откуда $R_R = \sum_{i=1}^n e_i R$. Теперь рассмотрим произвольное разложение нуля $0 = \sum_{i=1}^n e_i r_i$. Домножим слева на e_k, получим $0 = \sum_{i=1}^n e_k e_i r_i = e_k r_k$. В силу произвольности номера k получаем, что все слагаемые в разложении нуля сами равны нулю[15] Значит, разложение нуля может быть только тривиальным, отсюда сумма прямая.

Доказательство 1') проводится аналогично.

2) Каждый $r \in R$ можно представить в виде

$$r = 1 \cdot r \cdot 1 = \left(\sum_{i=1}^n e_i\right) \cdot r \cdot \left(\sum_{j=1}^n e_j\right) = \sum_{i,j=1}^n e_i r e_j.$$

Значит, $R = \sum\limits_{i,j=1}^n e_i R e_j$. Далее в произвольном разложении нуля $0 = \sum_{i,j=1}^n e_i r_{ij} e_j$ можно домножить слева на e_k и справа на e_ℓ. Тогда получим $0 = e_k r_{k\ell} e_\ell$ для всех $k, \ell = 1, \ldots, n$, откуда вытекает, что указанная сумма прямая.

Изоморфизм колец $\phi : R \longrightarrow (e_i R e_j)_{i,j=1}^n$ определим как

$$\phi(r) = \begin{pmatrix} e_1 r e_1 & e_1 r e_2 & \ldots & e_1 r e_n \\ e_2 r e_1 & e_2 r e_2 & \ldots & e_2 r e_n \\ \ldots & \ldots & \ldots & \ldots \\ e_n r e_1 & e_n r e_2 & \ldots & e_n r e_n \end{pmatrix}.$$

Тогда по построению $\phi(r+s) = \phi(r) + \phi(s)$. Рассмотрим элемент на позиции (i,j) у матрицы $\phi(r \cdot s)$:

$$(\phi(r \cdot s))_{ij} = e_i r s e_j = e_i r \cdot 1 \cdot s e_j = e_i r \left(\sum_{k=1}^n e_k\right) s e_j =$$
$$= \sum_{k=1}^n e_i r e_k s e_j = \sum_{k=1}^n e_i r e_k^2 s e_j = \sum_{k=1}^n (e_i r e_k)(e_k s e_j) = \sum_{k=1}^n (\phi(r))_{ik} \cdot (\phi(s))_{kj},$$

откуда $\phi(r \cdot s) = \phi(r) \cdot \phi(s)$. Также

$$\phi(1) = \begin{pmatrix} e_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & e_n \end{pmatrix} \text{ — единица указанного кольца.}$$

Инъективность ϕ следует из того, что сумма в пункте 2) прямая. Наконец для произвольных $r_{ij} \in R$, $i, j = 1, \ldots, n$ прообраз матрицы $(e_i r_{ij} e_j)_{i,j=1}^n$ непуст, т.к. содержит $r = \sum_{i,j=1}^n e_i r_{ij} e_j$, откуда получаем сюръективность ϕ. $\square$

[15] При этом коэффициенты r_i могут быть определены неоднозначно, однозначными окажутся только произведения $r_i e_i$.

Предложение 5.13. Правый идеал I кольца R выделяется прямым слагаемым в R_R тогда и только тогда, когда он порождается некоторым идемпотентом.

Доказательство. ($\Rightarrow$) Пусть $R_R = I \oplus L$, тогда $1 = e + f$ для некоторых $e \in I$, $f \in L$. Домножая на e справа и слева, получим

$$e = e^2 + ef, \quad e = e^2 + fe.$$

Тогда разность $e - e^2$, с одной стороны, равна ef, а значит, лежит в правом идеале I. Одновременно $e - e^2 = fe \in L$. Значит, $e - e^2 \in I \cap L$, но сумма идеалов I, L прямая, откуда $e - e^2 = 0$, т.е. e — идемпотент.

Далее если a — произвольный элемент идеала I, то $a = ea + fa$, где $fa \in L$. Но сумма $R_R = I \oplus L$ прямая и $a = a + 0$ — другое разложение элемента a. Значит, $fa = 0$, $ea = a$. Поэтому $I = eR$.

($\Leftarrow$) Если $I = eR$, $e^2 = e$, то достаточно рассмотреть разложение Пирса $R_R = eR \oplus fR$, где $f = 1 - e$. □

Предложение 5.14. Для правого R-модуля M следующие условия эквивалентны:

1) M раскладывается во (внутреннюю) прямую сумму некоторых своих подмодулей $M = M_1 \oplus \ldots \oplus M_n$.

2) Кольцо эндоморфизмов $S = \operatorname{End} M$ содержит полное ортогональное множество идемпотентов $\{e_1, \ldots, e_n\}$, причём $e_i(M) = M_i$, $i = 1, \ldots, n$.

Доказательство. 1) $\Rightarrow$ 2) Каждый элемент $m \in M$ единственным образом представим в виде $m = m_1 + \ldots + m_n$, где $m_i \in M_i$. Определим эндоморфизм e_i по правилу $e_i(m) = m_i$. Тогда $e_i^2(m) = e_i(m_i) = m_i = e_i(m)$, откуда e_i — идемпотент. Кроме того, $\sum_{i=1}^n e_i(m) = \sum_{i=1}^n m_i = m$, т.е. множество идемпотентов $\{e_i\}_{i=1}^n$ является полным. Наконец $e_i e_j(m) = e_i(m_j) = 0$, а значит, семейство $\{e_i\}_{i=1}^n$ ортогонально.

2) $\Rightarrow$ 1) Имеем $M = \mathrm{id}(M) = \sum e_i(M) = \sum M_i$. Причём в силу идемпотентности e_i его ограничение на свой образ M_i является тождественным отображением. Если $0 = m_1 + \ldots + m_n$ — разложение нуля, $m_i \in M_i$, то для всех i выполнено

$$0 = e_i(0) = e_i(m_1 + \ldots + m_n) = e_i(e_1(m_1) + \ldots + e_n(m_n)) = e_i(m_i) = m_i.$$

□