Теория колец

МГУ имени М. В. Ломоносова, Москва

осень 2023

Версия от 6 октября 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 φ: $R \to S$ — гомоморфизм колец. Тогда φ осуществляет сохраняющее включения взаимно-однозначное соответствие между множеством правых идеалов R, содержащих $\ker\varphi$, и множеством всех правых идеалов кольца $\varphi(R)$.

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

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 собственных правых идеалов называют *максимальными правыми идеалами*. Аналогично определяются максимальные левые и двусторонние идеалы.

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

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

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

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

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

В нулевом кольце нет максимальных идеалов.

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

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

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

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

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

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

Задачи к лекции 1.

Задача 1. Докажите теорему о гомоморфизме для колец.

Задача 2. Докажите теорему о соответствии идеалов.

Задача 3. Найдите 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 ${}_R R$ модуль над собой. Такие модули называют *регулярными*.

4. Любой правый (левый) идеал кольца является правым (левым) модулем.

5. Представления группы G над полем $\mathbb{F}$ соответствуют модулям над групповым кольцом $\mathbb{F}G$.

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

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

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

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

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

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

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

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

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

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

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

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

Определение 1.47.

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

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

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

- *Свободный R-модуль* — модуль, обладающий базисом.

Пример 1.48. Приведем примеры свободных модулей.

1. Нулевой модуль 0 считается свободным, его базис — пустое множество.

2. Свободная абелева группа = свободный $\mathbb{Z}$-модуль.

3. Векторное пространство над полем.

4. Регулярный модуль R_R, его базис — это $\{1\}$.

5. Множество матриц $M_n(R)$ — свободный правый или левый R-модуль с базисом из матричных единиц.

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

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

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

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

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

Предложение 1.52. Все модули над телом свободны.

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

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

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

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

Нулевой модуль не считаем неприводимым.

Пример 1.54.

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

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

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

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 ${}_RR^n$.

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. □

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

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

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

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

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

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

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

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

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

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

2')–9') Левые аналоги условий 2)–9).

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

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

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

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

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

1) $\Rightarrow$ 6) Доказано ранее.

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

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

9) $\Rightarrow$ 3) Пусть M — свободный неприводимый модуль, в частности, $M \neq 0$. Выберем произвольный базис M и возьмём в нём любой элемент m. Тогда отображение

$r \mapsto mr$ задаёт изоморфизм модулей $R_R \cong mR$. С другой стороны, $M = mR$ ввиду неприводимости. Таким образом, $R_R \cong M$, а значит, R_R неприводим.

□

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

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

Определение 1.62. *Свободная n-порождённая алгебра* $K\langle x_1, \ldots, x_n\rangle$ над коммутативным кольцом K — множество конечных формальных K-линейных комбинаций $\sum\limits_I \lambda_I x_{i_1} \cdots x_{i_k}$, $\lambda_I \in K$, *слов* от x_i, где $I = (i_1, \ldots, i_k)$ — конечные упорядоченные наборы натуральных чисел от 1 до n (набор может быть пустым). Умножение слов $x_{i_1} \cdots x_{i_k} \cdot x_{j_1} \cdots x_{j_m}$ производится конкатенацией, элементы K перестановочны со словами; на всё кольцо умножение продолжается в соответствии с дистрибутивностью. Единица алгебры соответствует пустому слову и отождествляется с 1_K.

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

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

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

Кроме того, мы будем использовать записи вида 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: $r \mapsto m_r$ 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] $K + (L \cap N) = (K + L) \cap N$.

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, $m = k + l \in K + (L \cap N)$. □

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

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 $\left(\begin{smallmatrix} \mathbb{Z}_4 & \mathbb{Z}_2 \\ 0 & \mathbb{Z}_2 \end{smallmatrix}\right)$ 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 $(M_n(R))^{\mathrm{opp}} \cong M_n(R^{\mathrm{opp}})$.

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