**Московский государственный технический университет
имени Н.Э. Баумана**

Факультет «Фундаментальные науки»
Кафедра «Математическое моделирование»

А.Н. Канатников

ИЗБРАННЫЕ ЛЕКЦИИ ПО АЛГЕБРЕ

Конспект лекций

Для студентов факультета ФН

Москва
2009

16. КОЛЬЦА И ПОЛЯ

16.1. Кольца

Определение: а) $(K,+)$ — группа, б) $(K,\cdot)$ — полугруппа, в) дистрибутивность умножения. Неассоциативные кольца. Аддитивная группа и мультипликативная полугруппа кольца. Кольцо с единицей. Коммутативное кольцо. Понятие подкольца. Подкольцо, порожденное множеством элементов. Примеры: $\mathbb{Z}$; $M_n(\mathbb{R})$; кольцо функций (отображений) $f\colon X \to K$, где K — кольцо; кольцо линейных операторов в ЛП. Свойства: 1) $a0 = 0a = 0$; 2) $0 \neq 1$, если в кольце более одного элемента; 3) $(-a)b = a(-b) = -ab$; 4) $(-1)a = -a$ в кольце с единицей; 5) $(a-b)c = ac - bc$, $c(a-b) = ca - cb$; 4) бином Ньютона в коммутативном кольце. Подкольца в $\mathbb{Z}$.

16.2. Специальные типы колец

Тело — кольцо с делением (все ненулевые элементы обратимы). Поле — коммутативное тело. Мультипликативная группа поля. Проблема расширения полугруппы до группы и кольца до тела (поля). Коммутативное кольцо без делителей нуля — целостное кольцо. Теорема: конечное целостное кольцо есть поле. Пример: $\mathbb{Z}$ есть коммутативное кольцо без делителей нуля, но не поле.

16.3. Гомоморфизмы колец и факторизация

Определение. Ядро и образ. Изоморфизм колец. Идеалы. В $\mathbb{Z}$ все подкольца являются идеалами. В $M_n(\mathbb{Z})$ множество верхних треугольных матриц — подкольцо, но не идеал. Идеалы, порожденные множеством элементов. Главные идеалы (с одним образующим). Понятие факторкольца и канонический гомоморфизм. Пример: факторкольцо $\mathbb{Z}/m\mathbb{Z}$ — кольцо $\mathbb{Z}_m$ вычетов по модулю m. Теорема: $\mathbb{Z}_m$ является полем тогда и только тогда, когда m — простое число. Мультипликативная группа вычетов по простому модулю. Теорема Ферма. Примеры: а) факторкольцо $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ есть поле, изоморфное полю комплексных чисел; б) кольцо фундаментальных рациональных последовательностей, факторизованное подкольцом б.м. последовательностей.

16.4. Модули и алгебры

Определение 16.1. Пусть K — кольцо, а M — абелева группа, для которой будем использовать аддитивную запись. Эта группа называется ***левым K-модулем*** (левым модулем над кольцом K), если задано левое умножение элементов группы на элементы кольца, т.е. отображение $\varphi\colon K \times M \to M$, удовлетворяющее аксиомам ($\alpha,\ \beta \in K$, $u,\ v \in M$):

M_1) $\varphi(\alpha, u+v) = \varphi(\alpha,u) + \varphi(\alpha,v)$;
M_2) $\varphi(\alpha+\beta, u) = \varphi(\alpha,u) + \varphi(\beta,u)$;
M_3) $\varphi(\alpha\beta, u) = \varphi(\alpha, \varphi(\beta,v))$.

Умножение элементов модуля на элементы кольца представляет собой многосортную операцию. Под многосортной n-арной операцией понимают отображение $\varphi\colon A_1 \times A_2 \times \ldots \times A_n \to A_0$, элементы множеств A_i называют сортами. Мы видим, что аргументы многосортной операции являются объектами разной природы. Многосортные операции обозначают общепринятым способом — точкой по центру или вообще опускают знак операции, если для операндов используются однобуквенные обозначения. При таком обозначении аксиомы левого умножения имеют следующий вид:

M_1^*) $\alpha(u+v) = \alpha u + \alpha v$;
M_2^*) $(\alpha+\beta)u = \alpha u + \beta u$;

M_3^*) $(\alpha\beta)u = \alpha(\beta u)$.

Наряду с понятием левого модуля существует понятие и правого модуля. ***Правым K-модулем*** над кольцом K называется абелева группа, в которой введено ***правое умножение*** на элементы кольца. Правое умножение отличается от левого третьей аксиомой:

$$u(\beta\alpha) = (u\beta)\alpha.$$

Можно сказать, что при левом умножении внешним (вторым) множителем является левый, а при правом умножении — правый. Если кольцо K коммутативно, то понятия левого и правого K-модулей совпадают

Пример. а. Первым примером модуля является действительное или комплексное линейное пространство. Анализ аксиом линейного пространства показывает, что в них используются только две основные арифметические операции (сложение и умножение), выполняемые над числами. Поэтому не представляет трудностей ввести общее понятие ***линейного пространства над*** произвольным ***полем*** P. Это понятие — частный случай модуля над коммутативным кольцом.

б. Любая абелева группа G имеет структуру $\mathbb{Z}$-модуля, в котором произведение na есть вычисление n-кратного для элемента $a \in G$:

$$na = \underbrace{a + a + \ldots + a}_{n \text{ раз}}.$$

Действительно, вычисление n-кратного можно рассматривать как бинарную многосортную операцию. Не составляет труда проверить выполнение аксиом модуля.

в. Множество E_G „автогомоморфизмов“ (они называются ***эндоморфизмами***) заданной абелевой группы G, т.е. гоморфизмов G в себя, есть кольцо относительно операций поточечного сложения и композиции как умножения, а сама группа G является E_G-модулем, если под умножением эндоморфизма φ на элемент группы a понимать значение $\varphi(a)$.

г. Любое кольцо K является K-модулем (сравните: $\mathbb{R}$ есть ЛП над $\mathbb{R}$). Пример можно обобщить: n-я декартова степень K^n кольца K с операциями покомпонентного сложения и покомпонентного умножения на „скаляр“ есть K-модуль.

д. В кольце K структуру левого (правого) K-модуля имеет любой левый (правый) идеал. В этом примере умножение произвольного элемента кольца справа (слева) на элемент идеала можно рассматривать как многосортную операцию. #

Отметим, что если алгебраическая система $K = (K_0, \{+, \cdot\})$ есть кольцо, то и алгебраическая система $\widetilde{K} = (K_0, \{+, *\})$ с операцией $a * b = ba$ тоже будет кольцом. Любой левый K-модуль является правым $\widetilde{K}$-модулем, а правый K-модуль — левым $\widetilde{K}$-модулем. Таким образом, двойственные понятия „правый“ и „левый“ взаимозаменяемы. Вернемся к примеру ***в***. В зависимости от интерпретации композиции (под $f \circ g$ можно понимать и $f(g(x))$, и $g(f(x))$, т.е. отображения могут применяться и справа налево, так и слева направо) абелева группа будет или левым E_G-модулем, или правым.

Если K — кольцо с единицей, то к трем аксиомам модуля уместно добавить аксиому

M_1^*) $1 \cdot a = a$ (умножение любого элемента на единицу кольца не изменяет этого элемента).

Модуль над кольцом с единицей, удовлетворяющий этой аксиоме, называется ***унитарным модулем***. Модули, рассмотренные в примерах **а**–**в**, **д** являются унитарными. Модуль в примере **г** является унитарным в случае кольца с единицей и неунитарным, если кольцо не имеет единицы. Эти примеры показывают, что требование унитарности естественное, но автоматически не выполняется: несложно привести пример неунитарного модуля над кольцом с единицей, например, взяв унитарный модуль и заменив исходное умножение αu на элементы кольца другим умножением $\alpha * u = (\alpha + \alpha)u$. Если единица кольца имеет порядок (по сложению), отличный от 2, то получим неунитарный модуль.

Подмодули

Пусть K — кольцо и M есть K-модуль. Множество $H \subset M$ называется ***подмодулем*** модуля K, если H замкнуто относительно групповых операций и относительно умножения на элементы кольца, т.е.

1) $u,\, v \in H \Rightarrow u + v \in H$;
2) $u \in H \Rightarrow -u \in H$;
3) $u \in H,\, \alpha \in K \Rightarrow \alpha u \in H$.

Из второго условия вытекает, что подмодуль всегда включает нуль (нейтральный элемент по операции сложения). Само второе условие вытекает из первого и третьего, если кольцо имеет единицу. В этом случае верно равенство $(-u) = (-1)u$, поскольку

$$u + (-1)u = 1 \cdot u + (-1)u = (1 - 1)u = 0 \cdot u,$$

а в силу свойств умножения на элементы кольца

$$0 \cdot u + 0 \cdot u = (0 + 0)u = 0 \cdot u,$$

откуда $0 \cdot u = 0$.

Как и в случае линейных пространств, можно утверждать, что пересечение двух подмодулей, как, впрочем, и пересечение любого числа подмодулей, является подмодулем. Это позволяет ввести понятие подмодуля порожденного заданным множеством элементов. В частности, если H_1 и H_2 — подмодули, то их объединение не является подмодулем, однако определен минимальный подмодуль, содержащий и H_1, и H_2. Этот подмодуль называется суммой подмодулей H_1 и H_2 и обозначается $H_1 + H_2$. Несложно показать, что

$$H_1 + H_2 = \{x \in M\colon x = h_1 + h_2,\ h_1 \in H_1,\ h_2 \in H_2\},$$

т.е., как и в случае линейных пространств, сумма подмодулей — это множество всевозможных сумм элементов двух подмодулей. Сумма подмодулей является ***прямой***, если для любого элемента $u \in H_1 + H_2$ разложение $u = h_1 + h_2$, $h_1 \in H_1$, $h_2 \in H_2$, единственно. Сумма двух подмодулей прямая тогда и только тогда, когда пересечение этих подмодулей нулевое (доказательство повторяет соответствующее доказательство из линейной алгебры).

Понятие прямой суммы можно перенести на любое конечное число подмодулей. Сумма n подмодулей H_i, $i = \overline{1, n}$, представляет собой множество всевозмозможных сумм вида $\sum\limits_{i=1}^{n} h_i$, где $h_i \in H_i$, $i = \overline{1, n}$. Такая сумма называется прямой, если указанное представление любого элемента суммы единственно. Сумма n подмодулей является прямой тогда и тогда, когда пересечение любого из n подмодулей с суммой остальных нулевое.

Среди подмодулей выделим так называемые ***конечно порожденные подмодули***, т.е. подмодули, порожденные конечным множеством, и ***циклические подмодули***, порожденные одним элементом. В унитарном левом модуле M циклический подмодуль, порожденный элементом u имеет вид Ku. Действительно, любой подмодуль, содержащий u, содержит и любой элемент вида αu, т.е. любой подмодуль, содержащий u, включает в себя множество Ku. Само множество Ku является подмодулем, поскольку для элементов $\alpha_1 u$ и $\alpha_2 u$ их сумма есть $(\alpha_1 + \alpha_2)u \in Ku$. Для любого $\beta \in K$ и $v = \alpha u \in Ku$ имеем $\beta v = (\beta\alpha)u \in Ku$. Если $v = \alpha u \in Ku$, то $-v = (-\alpha)u \in Ku$. Наконец, в унитарном модуле $u \in Ku$. Поэтому Ku — минимальный подмодуль, содержащий u, или, иначе, подмодуль, порожденный элементом u.

Аналогично в унитарном модуле подмодуль, порожденный элементами $u_1, \ldots, u_n$, представляет собой сумму $Ku_1 + \ldots + Ku_n$. Проверка этого аналогично случаю циклического подмодуля.

Гомоморфизмы модулей

Пусть K — кольцо и M, N — модули над K. Отображение $\varphi\colon M \to N$ называется ***гомоморфизмом K-модулей***, если оно сохраняет операции K-модулей, т.е.

$$\varphi(u+v) = \varphi(u) + \varphi(v), \quad \varphi(\alpha u) = \alpha\varphi(u).$$

Если K — поле, то K-модуль представляет собой линейное пространство над полем K, а понятие гомоморфизма K-модулей сводится к понятию *линейного оператора*. Как и в случае линейного оператора множество $\operatorname{Im}\varphi = \varphi(M)$ есть подмодуль в N, называемый ***образом гомоморфизма*** φ, а множество $\operatorname{Ker}\varphi = \varphi^{-1}(0) = \{u \in M\colon \varphi(x) = 0\}$ — подмодуль, называемый ***ядром гомоморфизма*** φ.

Пусть M — K-модуль и $H \subset M$ — его подмодуль. Тогда H есть подгруппа в абелевой группе M. Возможна факторизация. Оказывается, что фактор-группа G/H имеет естественную структуру K-модуля. В самом деле, факторизация аддитивной группы K-модуля определяется отношением эквивалентности $u \sim v \Leftrightarrow u - v \in H$. Легко убедиться в том, что если $u \sim v$, то для любого $\alpha \in K$ будет $\alpha u \sim \alpha v$. Значит, на фактор-группе G/H можно задать умножение на элементы кольца в соответствии с равенством

$$\alpha(u + H) = \alpha u + H$$

(т.е. для умножения класса смежности $a + H$ на элемент α достаточно в этом классе взять произвольный элемент u и умножить на элемент α; результат определит класс смежности, который и будет произведением $a + H$ на α).

Подчеркнем, что в то время как в теории групп и теории колец факторизация требует дополнительного условия на „знаменатель“ факторизации, в теории модулей фактоизация возможна по любому подмодулю.

Характеристики модуля и его элементов

Аннулятором (кручением) ***элемента модуля*** называется множество $\operatorname{Ann}_K(u)$ элементов кольца, аннулирующих элемент модуля, т.е.

$$\operatorname{Ann}_K(u) = \{\alpha \in K\colon \alpha v = 0\}.$$

Аннулятор элемента в левом K-модуле — левосторонний идеал в K. В самом деле, если $\alpha \in \operatorname{Ann}_K(u)$ и $\beta \in K$, то $\alpha u = 0$ и $\beta\alpha u = \beta \cdot 0 = 0$, т.е. $\beta\alpha \in \operatorname{Ann}_K(u)$. Коротко результат этого рассуждения можно записать так: $\beta \operatorname{Ann}_K(u) \subset \operatorname{Ann}_K(u)$. А это и означает, что $\operatorname{Ann}_K(u)$ есть левосторонний идеал

У элемента аннулятор может состоять из единственного элемента — нуля кольца. Другой крайний случай, когда $\operatorname{Ann}_K(u) = K$. Это означает, что $\alpha u = 0$ для любого элемента $\alpha \in K$. Отметим, что такое невозможно в унитарном модуле.

Элемент K-модуля, имеющий ненулевой аннулятор, называется ***периодическим***. Если в K-модуле все элементы периодические, то модкль называется ***периодическим***. Пример периодического модуля — конечная абелева группа как $\mathbb{Z}$ — модуль. В этом случае периодический элемент есть элемент конечного порядка.

Аннулятор $\operatorname{Ann}(M)$ ***K-модуля*** M — пересечение аннуляторов всех элементов модуля. Если $\operatorname{Ann}(G) = 0$, то ***модуль точный***. Аннулятор K-модуля — двусторонний идеал в K. Поэтому можно рассмотреть фактор-кольцо $K/\operatorname{Ann}(M)$. При этом K-модуль M можно наделить структурой модуля над фактор-кольцом $K/\operatorname{Ann}(M)$, если ввести левое умножение $\big(a + \operatorname{Ann}(M)\big)u = au$. Это определение корректно, поскольку для эквивалентных элементов a и b имеем $a - b \in \operatorname{Ann}(M)$ и для любого элемента $u \in M$ верно $au - bu = (a - b)u = 0$, или $au = bu$. Полученный при этом модуль над фактор-кольцом будет точным. В самом деле, если $\big(a + \operatorname{Ann}(M)\big)u = 0$ для любого $u \in M$, то элемент $a \in K$ аннулирует любой элемент модуля, а потому принадлежит аннулятору модуля, т.е. $a + \operatorname{Ann}(M) = \operatorname{Ann}(M)$ и является нулем фактор-кольца.

Свободные модули

Говорят, что множество $\{u_1, \ldots, u_m\}$ порождает K-модуль M свободно, если оно порождает этот K-модуль и, кроме того, для любого K-модуля N и любого множества $\{v_1, \ldots, v_m\} \subset N$ существует K-гомоморфизм φ: $M \to N$, для которого $\varphi(u_i) = v_i$, $i = \overline{1, m}$. При этом модуль M называют ***свободным***, а совокупность его элементов $\{u_1, \ldots, u_m\}$ — его базисом.

Понятие системы, порождающей модуль свободно, тесно связано с понятием линейной независимости (зависимости). Фактически это понятие позволяет перенести на произвольные модули основную часть аппарата линейной алгебры, опирающегося на понятие линейной независимости и базиса. Этот тезис вытекает из следующей теоремы.

Теорема 16.1. Пусть K — кольцо с единицей и M — левый унитарный модуль. Тогда следующие утверждения эквивалентны:

а) множество $\{u_1, \ldots, u_m\}$ порождает M свободно;

б) множество $\{u_1, \ldots, u_m\}$ порождает M и элементы $u_1, \ldots, u_m$ линейно независимы;

в) любой элемент $u \in M$ представим в виде $u = \alpha_1 u_1 + \ldots + \alpha_m u_M$, и притом единственным образом.

г) модули Ku_i образуют прямую сумму;

д) $M \cong K^m$.

◀ Пусть верно утверждение а). Выберем в качестве K-модуля N „стандартный“ модуль K^n и гомоморфизм φ, для которого $\varphi(u_i) = e_i$, где $e_1, \ldots, e_n$ — ***стандартный базис*** в K^n. Тогда для любых $\alpha_i \in K$ имеем

$$\varphi\Big(\sum_{i=1}^{n} \alpha_i u_i\Big) = \sum_{i=1}^{n} \alpha_i \varphi(u_i) = (\alpha_1, \ldots, \alpha_n).$$

Равенство $u = \alpha_1 u_1 + \ldots + \alpha_n u_n = 0$ влечет за собой $\varphi(u) = 0$. Но это возможно только тогда, когда $\alpha_i = 0$, $i = \overline{1, n}$. Таким образом, заключаем, что система $u_1, \ldots, u_n$ линейно независима.

Пункт б) следует из пункта в) как частный случай $u = 0$. С другой стороны, если элементы $u_1, \ldots, u_n$ линейно независимы, то так же, как и в линейной алгебре, нетрудно показать, что разложение любого элемента модуля по этой системе единственно. Существование такого разложения вытекает из условия, что элементы $u_1, \ldots, u_n$ порождают модуль.

Единственность представления $u = \alpha_1 u_1 + \ldots + \alpha_n u_n$ можно переформулировать как утверждение, что сумма $Ku_1 + \ldots + Ku_n$ является прямой. Это равносильно эквивалентности пунктов в) и г). Наконец, единственность разложения позволяет построить отображение, которое каждому элементу ставит в соответствие коэффициенты его разложения по системе $u_1, \ldots, u_n$. Это отображение, как легко убедиться, есть изоморфизм между рассматриваемы модулем и модулем K^n. Если $M \cong K^n$, то изоморфизм устанавливает соответствие между стандартным базисом в K^n и некоторым набором $u_1, u_2, \ldots, u_n$ элементов модуля M. Нетрудно показать, что $u_1, u_2, \ldots, u_n$ порождают M свободно (как стандартный базис порождает свободно K^n). Таким образом, из д) следует а). ▶

16.5. Алгебры на полем

Алгебра над полем P — это линейное пространство L над P с дополнительной бинарной операцией, называемой умножением, которая в совокупности со сложением превращает L в кольцо, в общем случае неассоциативное, и связана с операцией умножения на элементы поля законом ассоциативности $(\alpha u)v = \alpha(uv)$.

Структура кольца предполагает, что умножение ассоциативно. Однако, вспоминая, что могут рассматриваться неассоциативные кольца, заключаем, что могут быть ***неассоциативные алгебры***. В этом случае закон ассоциативности заменяется некоторым более слабым

законом. Например, в линейном пространстве V_3 существует операция векторного произведения, связанная со сложением законом дистрибутивности, а с умножением на число законом ассоциативности. Таким образом, V_3 есть алгебра над $\mathbb{R}$. Однако, векторное умножение неассоциативно, хотя удовлетворяет тождеству

$$(\boldsymbol{a} \times \boldsymbol{b}) \times \boldsymbol{c} + (\boldsymbol{b} \times \boldsymbol{c}) \times \boldsymbol{a} + (\boldsymbol{c} \times \boldsymbol{a}) \times \boldsymbol{b},$$

называемому ***тождеством Якоби***. Неассоциативная алгебра, удовлетворяющая тождеству Якоби, называется ***алгеброй Ли***.

Примеры алгебр:

1) кольцо многочленов над полем P;
2) кольцо матриц $M_n(P)$ над полем P;
3) алгебра линейных операторов в линейном пространстве над полем P;
4) любое расширение поля P, т.е. поле P', включающее в себя поле P.

Как и для других алгебраических структур, вводится понятие ***подалгебры*** — подмножества алгебры, которое замкнуто относительно всех операций алгебры (включая операцию вычитания, обратную к операции сложения). Пересечение любого подмножества подалгебр данной алгебры снова является подалгеброй. Отсюда приходим к понятию подалгебры, порожденной данным множеством элементов A: это пересечение всех подалгебр, содержащих множество A, или минимальная подалгебра, содержащая множество A. На алгебры и их подалгебры, как линейные пространства, распространяется понятие размерности.

Гомоморфизм алгебры A_1 над полем P в алгебру A_2 над P — это отображение $\varphi\colon A_1 \to A_2$, сохраняющее три операции алгебры. Если гомоморфизм является биективным отображением, то между элементами двух алгебр, а также между операциями в этих алгебрах, устанавливается взаимно однозначное соответствие. Такое соответствие означает, что две алгебры идентичны по своей внутренней структуре. Такие алгебры называются ***изоморфными***.

Для ассоциативных алгебр гомоморфизм есть, с одной стороны, линейный оператор, действующий из A_1 в A_2, а с другой, — гомоморфизм соответствующих колец. Следовательно, ***ядро гомоморфизма алгебр*** обладает свойствами двустороннего идеала, как ядро гомоморфизма колец. Понятие левостороннего (правостороннего, двустороннего) идеала переносится на алгебры. Таким образом, ядро гомоморфизма алгебр есть двусторонний идеал. ***Факторизация в алгебрах*** строится также, как и в других алгебраических структурах. Любой гомоморфизм $\varphi\colon A_1 \to A_2$ алгебр переносит структуру алгебры со своего образа A_2 (или подалгебры в A_2) на множество классов смежности $\dfrac{A_1}{H}$ (относительно сложения) по своему ядру $H = \operatorname{Ker}\varphi$. Множество классов смежности с перенесенной структурой называется ***факторалгеброй*** $\dfrac{A_1}{H}$ алгебры A_1 по подалгебре H. Операции факторалгебры записываются аналогично операциям фактормодулей и факторколец:

$$(a+H)+(b+H)=(a+b)+H, \quad (a+H)(b+H)=ab+H, \quad \lambda(a+H)=(\lambda a)+H.$$

Ядро гомоморфизма — двусторонний идеал. С другой стороны, для любого двустороннего идеала H на множестве классов смежности можно построить структуру алгебры, используя приведенные выше операции. Это означает, что факторалгебру можно построить по любому двустороннему идеалу. В частности, любой двусторонний идеал есть ядро некоторого гомоморфизма. В качестве примера можно рассмотреть ***канонический гомоморфизм алгебр***, который каждому элементу алгебры ставит в соответствие класс смежности, порожденный этим элементом.

Теорема 16.2. Всякая n-мерная ассоциативная алгебра над полем P изоморфна некоторой подалгебре в $M_k(P)$, где $k \leqslant n+1$.

◀ Доказательство близко к доказательству теоремы Кэли. Алгебра с 1 вкладывается в $M_n(P)$, которое можно интерпретировать как алгебру эндоморфизмов, а вложение имеет вид $\varphi_x(u) =$

xu. Алгебру размерности n без единицы можно расширить до $(n+1)$-мерной алгебры вводя на $P \otimes A$ умножение

$$(\alpha_1,\ a_1)(\alpha_2,\ a_2) = (\alpha_1\alpha_2,\ \alpha_1 a_2 + \alpha_2 a_1 + a_1 a_2). \qquad \blacktriangleright$$

Алгебра с делением — алгебра, являющееся телом относительно операций сложения и умножения.

Теорема 16.3 (Фробениус). Существует лишь три ассоциативные конечномерные алгебры с делением над $\mathbb{R}$: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, имеющие размерность 1, 2, 4.

Кроме указанных в теореме Фробениуса, существует еще одна неассоциативная конечномерная алгебра с делением размерности 8, называемая алгеброй октав. Четырехмерная алгебра с делением — это ***алгебра кватернионов***.

ОГЛАВЛЕНИЕ

4. Псевдорешения и псевдообратная матрица 1
4.1. Метод наименьших квадратов . . . 1
4.2. Псевдорешения . . . 3
4.3. Скелетное разложение . . . 4
4.4. Псевдообратная матрица . . . 6
4.5. Проектирование на подпространство . . . 10

9. Жорданова нормальная форма 12
9.1. Корневые подпространства . . . 12
9.2. Жорданова нормальная форма . . . 14
9.3. Комплексные корни . . . 19
9.4. Теорема Кэли — Гамильтона . . . 20

13. Операции над тензорами 22
13.1. Понятие тензора . . . 22
13.2. Матричная запись тензоров . . . 23
13.3. Преобразование тензоров, записанных в матричной форме . . . 24

14. Множества и отношения 26
14.1. Алгебра множеств . . . 26
14.2. Отображения и соответствия . . . 30
14.3. Отношения и операции . . . 32
14.4. Элементы математической логики . . . 34
14.5. Мощность множеств . . . 35

16. Кольца и поля 36
16.1. Кольца . . . 36
16.2. Специальные типы колец . . . 36
16.3. Гомоморфизмы колец и факторизация . . . 36
16.4. Модули и алгебры . . . 36
16.5. Алгебры на полем . . . 40

17. Кольцо многочленов 43
17.1. Определение кольца многочленов . . . 43
17.2. Деление с остатком и его свойства . . . 45
17.3. Разложение на неприводимые множители . . . 49
17.4. Использование делимости в теории шифрования . . . 49
17.5. Кватернионы . . . 50

19. Полукольца и булевы алгебры 51
19.1. Определение полукольца . . . 51
19.2. Ряды в полукольцах . . . 53
19.3. Замкнутые полукольца . . . 57
19.4. Системы линейных уравнений в полукольцах . . . 58
19.5. Симметричные полукольца . . . 63
19.6. Решетки . . . 67