

УДК 511.82

Разложение на простые множители невырожденных полиномиальных матриц^{*}

А.Н. КОРЮКИН¹

¹ 630090, РФ, г. Новосибирск, проспект академика Коптюга, 4, Институт математики им. Соболева, с. н. с., к. ф.-м. н., e-mail: koryukin@sibmail.ru

Предмет исследования. В алгебре полиномиальных матриц (над алгеброй K полиномов от одной буквы) размер n на n изучается вопрос единственности разложения на простые множители. **Актуальность.** Теория делимости является классической частью математики, вошедшей в процесс обучения в высших учебных заведениях. Автору неизвестно, изучался ли вопрос о единственности разложения на простые множители. Между тем в линейной теории автоматического управления (многоканальные системы) давно и успешно используются понятия наибольшего левого и правого делителей полиномиальных матриц, что может служить основой теории делимости для полиномиальных матриц. Важнейший вопрос теории делимости – существование и единственность разложения на простые множители. Вопрос единственности разложения на простые множители затруднён тем, что в кольце матриц нет коммутативности. **Результаты.** Показано, что в кольце полиномиальных матриц левые и правые идеалы главные (матрицы над алгеброй полиномов от одной буквы). Отсюда следует, что для любого числа невырожденных матриц существуют наибольший левый делитель, наибольший правый делитель, наименьшее левое кратное, наименьшее правое кратное. Показано, что для любой невырожденной матрицы существует разложение на простые множители. Охарактеризованы неразложимые матрицы: это в точности матрицы с простым (неразложимым) определителем. Проблема единственности разложения на простые множители решается так: для произвольной невырожденной матрицы A описаны все простые правые делители (простые матрицы B , для которых существует матрица C такая, что $A = BC$). Это описание сделано в терминах решётки K -подмодулей n -ок (модуля последовательности полиномов из K длины n). Разложение же $A = BC$ позволяет найти все разложения невырожденной матрицы A на простые множители. Эти поиски записаны в виде двух алгоритмов (для математиков и для инженеров). Описаны некоторые инварианты разложения матрицы на простые множители. Описаны некоторые частные случаи разложения. Приведён один пример разложения. **Методика и инструментарий.** Теория колец. Теория делимости.

Ключевые слова: полиномиальные матрицы, простые множители, неразложимые элементы, разложение на простые множители, единственность разложения на простые множители, теорема об единственности разложения на простые множители, наибольший общий левый делитель, наибольший общий правый делитель

ВВЕДЕНИЕ

Каждое натуральное число может быть представлено в виде произведения простых одним и только одним способом. Эту теорему называют основной теоремой арифметики [1].

В трудах Евклида [2] она ещё не встречается, но в предложении 31 книги VII было установлено, что любое целое число может быть представлено в виде произведения простых множителей, где некоторые множители могут быть одинаковыми; в предложении 14 книги IX доказано, что если все сомножители различны, то это представление однозначно [3].

Существование наибольшего общего делителя доказывается в самом начале VII книги Евклида [2] с помощью процесса, известного под названием «алгоритма Евклида». Этот алгоритм является основой всех последующих рассуждений (свойства простых чисел,

^{*} Статья получена 01 июля 2013 г.

существование и нахождение наименьшего общего кратного и т. д.). Однако существование и единственность разложения на простые множители не было доказано в общем виде. Но, во всяком случае, Евклид явно доказывает, что каждое целое делится на простое число (предложение 31 книги VII) [4].

По-видимому, Евклид потому не формулирует общую теорему, что у него не хватает адекватной терминологии и символики для произвольных степеней целого числа. К тому же все свидетельства согласуются с тем, что начиная с этой эпохи разложение заданного числа на простые множители было хорошо известно и им свободно пользовались [4].

Основная теорема арифметики не формулируется точно даже во «Введении в теорию чисел», написанном в 1798 году Лежандром. Вероятно, из-за отсутствия этой теоремы у Евклида она принимается без доказательства во многих школьных учебниках [1].

Первую точную формулировку этой теоремы и её доказательство дал Гаусс в 1801 году в своих знаменитых «Арифметических исследованиях» [5] (во втором разделе этих исследований в п. 16 доказывается однозначность разложения натурального числа на простые множители). По этому поводу Гаусс говорит: «То, что каждое составное число может быть разложено на простые множители, известно из основ; однако то, что этого нельзя сделать несколькими различными способами, совершенно необоснованно по большей части считается само собой разумеющимся».

Вопрос о делении многочленов как об операции обратной умножению, естественно, должен был быть поставлен в самом начале развития алгебры. Ясно, однако, что едва ли возможно решить эту проблему до тех пор, пока не создана последовательная система обозначений для различных степеней переменного. Действительно, до середины XVI века не появляется ни одного примера «евклидова» деления многочленов, и, видимо, Стевин [6] (который, в сущности, использовал обозначение показателя) был первым, кто пришёл к мысли применить «алгоритм Евклида» для отыскания наибольшего общего делителя двух многочленов [7, стр. 113]. В остальном понятие делимости до середины XVIII века считалось присущим только целым числам [4].

В XIX веке в теории делимости был достигнут значительный прогресс. Она была развита для кольца целых чисел, колец полиномов, областей целостности (ассоциативных коммутативных колец без делителей нуля). Были введены евклидовы кольца (кольца с алгоритмом Евклида), кольца главных идеалов, факториальные кольца (области целостности с единственным разложением на простые множители). Показано, что евклидовы кольца являются кольцами главных идеалов, а кольца главных идеалов являются факториальными; что кольцо полиномов над факториальным кольцом факториально [7, 8]. Значительный вклад в развитие теории делимости внёс Гаусс.

Теория делимости стала небольшой и классической частью основ математики, и её стали преподавать студентам высших учебных заведений [9–12].

Но в теории делимости математики ограничились изучением коммутативных колец, причём не имеющих делителей нуля. Между тем в линейной теории автоматического управления (многоканальные системы) по необходимости давно и успешно используются наибольший общий левый, правый делитель полиномиальных матриц [13–18] (полиномы от одной буквы). Понятия наибольшего левого и правого делителей полиномиальных матриц являются стандартными и классическими элементами инструментария теории многоканальных систем, и это преподают студентам высших учебных заведений [19], [20].

Впрочем, оказалось, что понятия наибольшего общего левого и правого делителя полиномиальных матриц были математикам известны [21], [22].

Очевидно, что алгебра матриц над алгеброй полиномов от одной буквы нётерова (как слева, так и справа). Поэтому в ней можно говорить о простых левых и правых делителях, и существует разложение на простые множители (по крайней мере, для невырожденных матриц). Но как быть с единственностью разложения на простые множители? Этот вопрос и исследуется в данной работе.

1. ЛЕВЫЙ/ПРАВЫЙ НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ И ЛЕВОЕ/ПРАВОЕ НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

Далее k – произвольное поле; s – символ; $K = k[s]$ – алгебра (векторное пространство с умножением) полиномов над полем k ; $n \geq 1$ – произвольное целое положительное число; $M = M_n(K)$ – алгебра матриц размера $n \times n$ над алгеброй K ; $U(M)$ – множество невырожденных матриц, у которых определитель лежит в k .

$U(M)$ – это в точности множество матриц из M , обратимых в M .

Элементы алгебры M называем просто матрицами. Множество $\{1, \dots, n\}$ обозначим через $\bar{n}$. Для $i, j \in \bar{n}$ обозначим через $e_{i,j}$ матрицу, у которой в i -ой строке и j -ом столбце единица, а остальные нули. Такие матрицы будем называть, как это обычно принято, матричными единицами.

Введём обозначения: K^n – K -модуль столбцов высоты n полиномов из K ; K_n – K -модуль строк длины n полиномов из K .

Напомним, что левый идеал, порождённый одним элементом, называется *главным*.

Лемма 1. Для $n \geq 1$, произвольный подмодуль любого n -порождённого K -модуля порождён не более чем n элементами.

Действительно, алгебра K коммутативна и нётерова (т. е. любая возрастающая цепочка идеалов алгебры K обрывается). Значит, любой конечнопорождённый K -модуль N нётеров. Поэтому все его подмодули конечнопорождены.

Достаточно рассматривать случай, когда K -модуль N свободно порождён своими n элементами. В этом случае элементы K -модуля N можно рассматривать как n -ки полиномов из K .

Рассмотрим произвольный подмодуль P K -модуля N . Он конечнопорождён. Рассмотрим любое конечное множество n -ок, порождающее K -модуль P , и следующую «элементарную операцию» над такими множествами n -ок: к одной n -ке можем прибавить другую, помноженную на произвольный полином из K .

Понятно, что в результате этих элементарных операций K -модуль, порождённый множеством n -ок, не изменится.

Будем обращать внимание только на первый элемент n -ок. Вспомним об алгоритме деления с остатком в алгебре K . Теперь элементарными операциями множество n -ок может быть преобразовано так, что только один из элементов этого множества может иметь ненулевую первую координату.

После этого исключим из множества n -ок имеющую ненулевую первую координату. В оставшихся n -ках первая координата нулевая. Исключим первую координату и продолжим процесс.

Теперь индукцией по числу n нетрудно показать, что произвольный подмодуль любого n -порождённого K -модуля порождён не более чем n элементами.

Лемма 2. Любой левый идеал алгебры матриц M главный.

Обозначим через μ произвольный левый идеал алгебры M . Так как $K \cdot E \subseteq M$ (E – единичная матрица), то μ является K -модулем.

Пространство K_n является K -модулем. Этот модуль порождается своими n элементами. Пространство $K_n \mu$ является его подмодулем. Значит, согласно лемме *podmodul-n-poroid*, K -модуль $K_n \mu$ порождён не более чем n элементами.

Возьмём эти n элементов и составим из них матрицу. Если элементов меньше, чем n , то допишем пустые строки. Эта матрица порождает исходный левый идеал μ . Таким образом, левый идеал μ главный.

Следствие 3. Правый идеал алгебры M главный.

(Из леммы 2 – транспонированием).

Следствие 4. Для любого множества матриц из M существует их правый (левый) наибольший общий делитель и правое (левое) наименьшее общее кратное.

Для $A, B \in M$, правые идеалы $AM \cap BM$, $AM + BM$ главные, т. е. $CM = AM \cap BM$, $DM = AM + BM$ для некоторых C, D из M . Тогда C будет наименьшим общим левым кратным матриц A, B ; D будет наибольшим общим левым делителем матриц A, B .

Для правых делителей и кратных Утверждение получается аналогично, или транспонированием (из Утверждения для левых делителей и кратных).

2. СУЩЕСТВОВАНИЕ РАЗЛОЖЕНИЯ НА ПРОСТЫЕ МНОЖИТЕЛИ НЕВЫРОЖДЕННЫХ ПОЛИНОМИАЛЬНЫХ МАТРИЦ

Лемма 5. Любая возрастающая цепочка левых (правых) идеалов алгебры M обрывается.

Алгебра K нётерова; K -модуль M конечно порождён. Поэтому M является нётеровым K -модулем.

Рассмотрим произвольную возрастающую цепочку $\rho_1 \subset \dots \subset \rho_n \subset \dots$ левых (правых) идеалов алгебры M . Элементы этой цепочки являются K -модулями. Это возрастающая цепочка подмодулей K -модуля M .

Из изложенного выше следует, что любая возрастающая цепочка левых (правых) идеалов алгебры M обрывается.

Напомним, что квадратная матрица над ассоциативным коммутативным кольцом называется невырожденной, если её определитель не ноль.

Обратимыми элементами алгебры M являются матрицы, определитель которых лежит в поле k и отличен от нуля.

Определение 6. В алгебре M простыми (неразложимыми) назовём невырожденные необратимые элементы, у которых при любом разложении в произведение двух сомножителей один из сомножителей будет обратим.

Лемма 7. В алгебре M для любой невырожденной необратимой матрицы любой процесс разложения в произведение необратимых сомножителей можно довести до конца.

Рассмотрим элемент $A \in M$ из условия Леммы. Если он простой, то он раскладывается в произведение простых сомножителей.

Далее элемент A не простой. Тогда он разлагается в произведение двух сомножителей $A = BC$.

Для произвольной матрицы Q через $\det(Q)$ будем, как это общепринято, обозначать определитель матрицы Q .

Матрицы B, C не вырождены (ведь $A = BC$ и матрица A невырождена). Матрицы B, C необратимы (ведь $A = BC$ и невырожденная матрица A неразложима). Поэтому полиномы $\det(B)$, $\det(C)$ не являются константами. Значит, эти полиномы являются собственными делителями полинома $\det(A)$.

Доказательство завершается индукцией по степени полинома $\det(A)$.

Следствие 8. В алгебре M любая невырожденная необратимая матрица раскладывается в произведение простых сомножителей.

3. К ЕДИНСТВЕННОСТИ РАЗЛОЖЕНИЯ НА ПРОСТЫЕ МНОЖИТЕЛИ – ДЛЯ НЕВЫРОЖДЕННЫХ МАТРИЦ. ДИАГОНАЛЬНОЕ РАЗЛОЖЕНИЕ НЕВЫРОЖДЕННЫХ МАТРИЦ НА ПРОСТЫЕ МНОЖИТЕЛИ

В алгебре $K = k[x]$:

- 1) обратимые элементы – это отличные от нуля константы;
- 2) выполнена теорема о единственности разложения на простые множители.

В алгебре M любую матрицу A можно разложить так: $A = UDV$, где U, V – обратимые матрицы из M ; D – диагональная матрица из M [19, § 2, пункты 16, 17]. Её называют *формой Смита*.

Для невырожденной матрицы A по диагонали матрицы D расположены отличные от нуля полиномы. Разложим их на множители. После этого разложим матрицу D (в произведение наибольшего числа необратимых сомножителей): $D = D_1 \cdot \dots \cdot D_m$, где $m \geq 1$. Понятно, что сомножители D_i , где $i \in \overline{m}$, имеют простой определитель.

Теперь понятно, что A разлагается в произведение m сомножителей, имеющих простые определители: $A = UD_1 \cdot \dots \cdot D_i \cdot \dots \cdot D_m V$.

Следствие 9. В алгебре M любая невырожденная простая матрица имеет простой определитель.

Так как матрица A простая, то из диагонального разложения следует $m=1$, т. е. $A = UDV$, где матрицы U, V обратимы, а определитель матрицы D простой. Значит, определитель матрицы A простой.

При этом очевидно, что матрицы из M с простым (неразложимым в K) определителем простые (неразложимые в M). Поэтому:

Лемма 10. Пусть A – невырожденная матрица из M . Тогда матрица A простая (неразложимая) $\Leftrightarrow$ её определитель простой.

4. ОТ ЕДИНСТВЕННОСТИ РАЗЛОЖЕНИЯ К ЖОРДАНОВОЙ ФОРМЕ

Рассмотрим произвольную невырожденную матрицу A из M и произвольное разложение $A = P_1 \cdot \dots \cdot P_m$ матрицы A на простые множители.

1. Разложения устойчивы при умножении на матрицы из $U(M)$ и справа, и слева: $AQ = P_1 \cdot \dots \cdot P_m Q$ есть разложение матрицы AQ в последовательность m простых множителей $P_1, \dots, P_m Q$ ($Q \in U(M)$); $TA = TP_1 \cdot \dots \cdot P_m$ есть разложение матрицы Q в последовательность m простых множителей $TP_1, \dots, P_m$ ($T \in U(M)$).

2. Для любой матрицы разложений на простые множители много. Например, равенство $P_1 \cdot P_2 = P_1 Q \cdot Q^{-1} P_2$ даёт бесконечно много разложений матрицы $P_1 \cdot P_2$ в произведение. Поэтому хотелось бы найти в этих разложениях что-то более устойчивое и инвариантное.

3. Рассмотрим цепочку правых идеалов $P_1 M \supseteq P_1 P_2 M \supseteq \dots \supseteq P_1 \dots P_m M$:

1) эта цепочка конечна (из m элементов) и заканчивается правым идеалом $AM = P_1 \cdot \dots \cdot P_m M$;

2) так как матрицы $P_1, \dots, P_m$ невырожденные и не обратимы в M , то во всех звеньях цепочки нет равенства: $P_1 M \supset P_1 P_2 M \supset \dots \supset AM$;

3) так как матрицы $P_1, \dots, P_m$ простые, то эта цепочка правых идеалов плотная.

Так как матрица P_1 простая, то фактор-модуль $M / P_1 M$ простой. Поэтому цепочка правых идеалов $M \supset P_1 M \supset P_1 P_2 M \supset \dots \supset AM$ будет плотной.

4. Теперь понятно, что для единственности разложения матрицы A полезно изучить решётку правых идеалов ρ алгебры M таких, что $\rho \supseteq AM$. Как устроена эта решётка? Она конечна? Дистрибутивна?

5. Обозначим через K^n множество всех столбцов из K высоты n .

Понятно, что K^n является левым M -модулем (при умножении матрицы на столбец получаем столбец). В частности, K^n также является K -модулем (ведь поле K вкладывается в M с помощью скалярных матриц: $K \cdot E \subseteq M$).

6. Для любой матрицы B рассмотрим её образ BK^n (при действии матриц слева на столбцы из K^n). Понятно, что BK^n есть подмодуль K -модуля K^n ; если V – некоторый подмодуль K -модуля M , то VK^n является подмодулем K -модуля K^n .

7. Каждому правому идеалу ρ сопоставим ρK^n :

1) ρK^n является подмодулем K -модуля K^n ;

2) рассмотрим произвольный подмодуль V K -модуля K^n . Он порождён не более чем n элементами (лемма 1). Составим из этих элементов-столбцов матрицу. Если столбцов меньше, чем n , то в матрицу добавим пустые столбы и сделаем матрицу квадратной. Обозначим её B ;

3) $BMK^n = BK^n = V$, т. е. образ ρK^n правого идеала $\rho = BM$ алгебры M , порождённого матрицей B , совпадает с произвольно выбранным подмодулем K -модуля K^n .

8.1. Решётка правых идеалов алгебры M изоморфна решётке подмодулей K -модуля K^n .

8.2. Отображение $f: \rho \mapsto \rho K^n$, сопоставляющее произвольному правому идеалу ρ алгебры M подмодуль ρK^n K -модуля K^n , является изоморфизмом решёток.

8.3. Рассмотрим отображение $g: V \mapsto \mu$, сопоставляющее любому подмодулю V K -модуля K^n множество μ матриц B из M таких, что $BK^n \subseteq V$. Так как $BMK^n \subseteq BK^n \subseteq V$, то μ является правым идеалом. Поэтому отображение g можно рассматривать как отображение решётки подмодулей K -модуля K^n в решётку правых идеалов алгебры M .

Отображение g будет обратно отображению f . Поэтому g будет изоморфизмом решёток.

8.4. Пусть ρ – произвольный правый идеал алгебры M ; $W = \rho K^n$.

Обозначим через $R(M, \rho)$ решётку правых идеалов алгебры M , содержащих ρ ; через $R(K^n, W)$ – решётку подмодулей K -модуля K^n , содержащих W .

При ограничении отображения f на правые идеалы, содержащие ρ , и при ограничении отображения g на подмодули K -модуля K^n , содержащие W , получим: решётки $R(M, \rho)$, $R(K^n, W)$ изоморфны; отображения $f|_{R(M, \rho)}: R(M, \rho) \rightarrow R(K^n, W)$, $g|_{R(K^n, W)}: R(K^n, W) \rightarrow R(M, \rho)$ являются изоморфизмами решёток.

9. Итак, изучать надо подмодули K -модуля K^n . Точнее: как устроена решётка $R(K^n, W)$?

Эта решётка изоморфна решётке подмодулей K -модуля K^n/W ; $W = AK^n$ для некоторой невырожденной матрицы A . Обозначим через $\bar{A}$ матрицу, дополнительную к A .

Имеем: $\bar{A}\bar{A} = \Delta \cdot E$, где $\Delta = \det(A)$ – определитель матрицы A ; E – единичная матрица. Поэтому $\Delta E \subseteq \bar{A}\bar{A}$, $\Delta EK^n \subseteq \bar{A}\bar{A}K^n$, $\Delta \cdot K^n \subseteq \bar{A}K^n = W$. При этом $\Delta \neq 0$.

Значит, K -модуль K^n/W сингулярный, т. е. любой его элемент имеет ненулевой аннулятор. Так как при этом K -модуль K^n/W конечнопорождён, то K^n/W является конечномерным k -пространством. На этом конечномерном k -пространстве K^n/W символ s действует как линейное отображение. И нас интересует решётка подмодулей K -модуля K^n/W . То есть нас интересует решётка подмодулей одного линейного преобразования s на конечномерном пространстве. Понятно, что нужно вспомнить жорданову форму линейного преобразования.

10. Проще всего линейное преобразование выглядит для алгебраически замкнутого поля. Поэтому интересен случай, когда поле k алгебраически замкнуто. В частности, когда k – поле комплексных чисел $\mathbb{C}$.

11. Вопрос. Пусть k – произвольное алгебраически замкнутое поле; V – произвольное конечномерное k – пространство; S – произвольное линейное преобразование пространства V . Как устроена решётка инвариантных подпространств пространства V ?

5. АЛГОРИТМ ОТЩЕПЛЕНИЯ: ОБОСНОВАНИЕ

Далее A – невырожденная матрица из M . Приведём теперь алгоритм отщепления справа от A . Он позволяет находить все разложения вида $BC = A$, где C – простая матрица из M .

1.1. В алгебре M рассмотрим правый идеал AM . Рассмотрим также подмодуль $AMK^n = AK^n$ K -модуля K^n . K -модуль AK^n порождается столбцами матрицы A . Рассмотрим все n столбцов $A_1, \dots, A_n$ матрицы A .

1.2. Рассмотрим фактор-модуль $K^n / (AK^n)$. Введём обозначения: $\Delta = \det(A)$ – определитель матрицы A ; E – единичная матрица (размера $n \times n$).

1.3. Существует матрица $\bar{A}$ такая, что $\bar{A}A = \bar{A}A = \Delta \cdot E$. Так как матрица A невырожденная, то матрица $\bar{A}$ единственная. Она называется *дополнительной* к A .

2.1. K -модуль $K^n / (AK^n)$ аннулируется полиномом $\Delta = \det(A)$. Действительно, $\bar{A}A = \Delta \cdot E$, где $\bar{A}$ – матрица, дополнительная к A . Значит, $\bar{A}AK^n = \Delta \cdot K^n$. Поэтому $AK^n \supseteq \bar{A}AK^n \supseteq \Delta \cdot K^n$.

2.2. K -модуль $K^n / (AK^n)$ является конечномерным k -пространством (ведь $AK^n \supseteq \Delta \cdot K^n$).

2.3. На конечномерном пространстве $K^n / (AK^n)$ линейно действует элемент s .

2.4. $\Delta \neq 0$ (ведь матрица A невырожденная).

3.1. Если полином Δ степени 0 (константа), то матрица A обратима, и раскладывать на множители нечего. Алгоритм заканчивается.

3.2. Далее: полином Δ не ноль, но не обратим в K .

3.3. Разложим полином Δ на простые множители.

3.4. Выберем простой сомножитель d полинома Δ .

4.1. Рассмотрим фактор-алгебру $\bar{K} = K / (d = 0)$ алгебры K по идеалу, порождённому элементом d . Так как элемент d простой, то алгебра $\bar{K}$ является полем.

4.2. Рассмотрим фактор-алгебру матриц $\bar{M} = M / (d \cdot E = 0)$ алгебры M по идеалу, порождённому элементом $d \cdot E$.

4.3. Обозначим через $\bar{A}$ образ матрицы A при каноническом гомоморфизме $M \rightarrow \bar{M}$.

5.1. Так как в алгебре K элемент d является делителем элемента Δ , то $\bar{\Delta} = 0$, т. е. определитель матрицы $\bar{A}$ нулевой, т. е. матрица $\bar{A}$ вырожденная. Значит, её аннулятор $= (\bar{A}, \bar{K}^n)$ в $\bar{K}$ -модуле $\bar{K}^n$ ненулевой.

5.2. Возьмём произвольный ненулевой элемент $\bar{X}$ из этого аннулятора.

5.3. Рассмотрим произвольный прообраз X (при каноническом гомоморфизме $K^n \rightarrow \bar{K}^n$) элемента $\bar{X}$ из K^n .

5.4. В $k(s)$ -модуле $k(s)^n$ рассмотрим элемент $Y = AX \cdot d^{-1}$. Здесь $k(s)$ – поле дробей полиномов из $k[s]$; $k(s)^n$ – множество столбцов из $k(s)$ высоты n . По построению, $w \in K^n$.

6.1. Рассмотрим подмодуль V K -модуля K^n , порождённый столбцами $A_1, \dots, A_n, Y$. Этот модуль порождён не более чем n элементами (лемма 1).

6.2. С помощью элементарных преобразований столбцов приведём множество $A_1, \dots, A_n, Y$ столбцов к ступенчатому виду (нули будут над ступеньками).

6.3. Исключим нулевые столбцы.

6.4. Получим множество N из не более чем n столбцов, порождающее K -модуль V .

7.1. Так как $AK^n \subseteq V$ и k -пространство K^n / AK^n конечномерно, то k -пространство K^n / V также конечномерно. Значит, множество N не может содержать менее чем n элементов.

7.2. Поэтому множество N содержит ровно n элементов.

7.3. Составим из n элементов множества N матрицу. Обозначим её через B .

7.4. В силу выбора матрицы B , $AM \subseteq BM$, $AM \neq BM$, и фактор-модуль над M BM / AM простой.

8.1. Из $AM \subseteq BM$ следует $A \in BM$, т. е. $A = BC$ для некоторой матрицы C из M .

8.2. Вспомним, что матрица A невырожденная. Значит, матрицы B, C также являются невырожденными.

8.3. По построению, $\det(B) = \det(A) / d$. Значит, $\det(C) = d$. Поэтому определитель матрицы C простой. Следовательно, по лемме 10 матрица C простая.

9. Найдём матрицу C по формуле: $C = B^{-1}A$.

10. Этим заканчивается алгоритм отщепления. От невырожденной матрицы A отщепляем справа любую возможную простую матрицу C . Произвольность матрицы C следует невырожденности матрицы A , из равенства $A = BC$, из произвольности матрицы B .

6. АЛГОРИТМ ОТЩЕПЛЕНИЯ: ВЫЧИСЛЕНИЕ

Далее A – невырожденная матрица из M .

1.1. Выпишем все n столбцов $A_1, \dots, A_n$ матрицы A .

1.2. Вычислим определитель $\Delta = \det(A)$ матрицы A .

2.1. Если полином Δ степени 0 (константа), то алгоритм заканчиваем (матрица A обратима и раскладывать на множители нечего).

2.2. Далее: полином Δ не ноль, но не обратим в K .

2.3. Разложим полином Δ на простые множители.

2.4. Выберем простой сомножитель d полинома Δ .

3.1. Для всех $i, j \in \bar{n}$ с помощью алгоритма деления полиномов из K с остатком вычислим остаток $\overline{a_{i,j}}$ при делении полинома $a_{i,j}$ (элемент матрицы A в ячейке (i, j)) на полином d . Из этих остатков составим матрицу $\overline{A}$ (в ячейку (i, j) этой матрицы помещаем полином $\overline{a_{i,j}}$).

3.2. Методом Гаусса вычислим подпространство всех столбцов $\overline{X}$ высотой n из $\overline{K}^n$ таких, что $\overline{AX} = 0$ ($\overline{K}$ – это поле $K / (d = 0)$).

3.3. Выберем любой ненулевой элемент $\overline{X}$ из Ann .

3.4. Рассмотрим произвольный столбец X из $X \in \overline{X} + d \cdot K^n$.

3.5. Вычислим столбец $Y = AX \cdot d^{-1}$.

По построению $Y \in K^n$.

4.1. Выпишем столбы $A_1, \dots, A_n, Y$.

4.2. Элементарными преобразованиями столбцов приведём множество $A_1, \dots, A_n, Y$ столбцов к ступенчатому виду (нули будут над ступеньками).

- 4.3. Исключим нулевые столбцы.
- 4.4. Получим множество N из n столбцов.
5. Составим из этих n столбцов матрицу. Обозначим её B .
6. Вычислим матрицу C по формуле: $C = B^{-1}A$.
7. Этим заканчивается алгоритм отщепления (от невырожденной матрицы A отщепляем справа любую возможную простую матрицу).

7. ИНВАРИАНТЫ МНОГОКРАТНОГО ОТЩЕПЛЕНИЯ

Применяя теперь алгоритм отщепления к матрице B и т. д., получим возрастающую цепочку $AM \subset BM \subset \dots$.

В алгебре M возрастающие цепочки идеалов обрываются (лемма 5). Поэтому процесс многократного отщепления рано или поздно закончится. И даже известно число шагов этого процесса: это число делителей полинома $\det(A)$ (не обязательно различных).

1. В результате процесса получим плотную цепочку $\rho_1 \subset \dots \subset \rho_m \subset M$ правых идеалов алгебры M . Здесь m – число делителей полинома $\det(M)$ при его разложении в произведение простых сомножителей (не обязательно различных). Каждому звену цепочки можно приписать простой делитель полинома $\det(A)$. Вместо самой цепочки правых идеалов проще рассматривать цепочку $\rho_1 K^n \subset \dots \subset \rho_m K^n \subset K^n$ подмодулей K -модуля K^n . Эта цепочка также плотная.

2. Для невырожденной матрицы A K -модуль $K^n / (AK^n)$ является конечномерным k -пространством. На конечномерном k -пространстве действует элемент s – как линейное преобразование. Всё сразу сводится к линейной алгебре.

3. Для произвольного элемента f из K обозначим через V^f множество всех элементов K -модуля $K^n / (AK^n)$, каждый из которых аннулируется некоторой степенью элемента f . Множество V^f является K -модулем.

Если полином $\det(A)$ является делителем некоторой степени полинома ab , то K -модуль $K^n / (AK^n)$ есть прямая сумма своих подмодулей V^a, V^b . Поэтому K -модуль $K^n / (AK^n)$ разлагается в прямую сумму своих подмодулей V^d , по всем простым делителям d полинома $\det(A)$ (здесь делитель d можно брать только один раз).

4. Для разложения на простые множители невырожденной матрицы A нужны следующие данные:

1) плотная цепочка $\rho_0 \subset \rho_1 \subset \dots \subset \rho_m \subset M$ правых идеалов алгебры M такая, что $\rho_0 = AM$;

2) для каждого правого идеала из этой цепочки (не считая ρ_0 и M) нужно выбрать порождающую матрицу.

Этими данными разложение задано однозначно.

Более простые инварианты разложения. Для разложения на простые множители невырожденной матрицы A можно использовать следующие данные:

1) плотная цепочка $\rho_0 K^n \subset \rho_1 K^n \subset \dots \subset \rho_m K^n \subset K^n$ правых подмодулей K -модуля K^n такая, что $\rho_0 K^n = AK^n$;

2) для каждого K -модуля из этой цепочки (не считая $\rho_0 K^n, K^n$) нужно выбрать элемент из K^n , т. е. выбрать порождающее множество не более чем из n элементов (существование этого множества гарантирует лемма 1). Если в этом множестве меньше чем n элементов –

дополнить его до n -элементного любыми элементами из K^n . Пронумеровать эти n элементов (чтобы из множества получилась n -ка).

Этими данными разложение задано однозначно.

8. ЧАСТНЫЕ СЛУЧАИ

1. Если при разложении полинома $\det(A)$ на простые сомножители нет одинаковых, то существует совсем простой набор данных разложения матрицы A : разложение на простые множители матрицы A соответствует разложению на простые множители полинома $\det(A)$.

2. Своей простотой выделяется более общий случай: когда элемент s действует на конечномерное k -пространство $V = K^n / (AK^n)$ полупросто, т. е. его жорданова форма диагональна. Эквивалентные инвариантные формулировки этого свойства:

1) любой подмодуль K -модуля V дополняется;

2) для любого простого делителя d полинома $\det(A)$, пространство V^d аннулируется полиномом d .

3) конечномерное k -пространство V есть прямая сумма своих подпространств V_d , где $d \in D$; D – множество всех простых делителей полинома $\det(A)$; V_d – множество элементов из V , аннулируемых элементом d .

3. Если поле k алгебраически замкнуто (например, это поле комплексных чисел), то всё сводится к жордановой форме линейного преобразования, полученного при действии элемента s на конечномерное k -пространство K^n / AK^n .

9. АЛГОРИТМ РЕШЕНИЯ УРАВНЕНИЯ $ax + by = d$ В ПОЛИНОМАХ

Для произвольных полиномов a, b из $K = k[s]$ обозначим через d их наибольший общий делитель. Здесь для произвольных $a, b \in K$ изложен алгоритм нахождения их наибольшего общего делителя d и полиномов x, y из K таких, что $ax + by = d$, вместе с обоснованием, на базе алгоритма деления полиномов с остатком.

1. Рассмотрим матрицу $\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$ при конкретных a, b . Например, $a = s^3, b = s^2 + 1$:

$$\begin{pmatrix} s^3 & 1 & 0 \\ s^2 + 1 & 0 & 1 \end{pmatrix}.$$

2. Будем рассматривать следующее элементарное преобразование строк: из одной строки можно вычитать другую, предварительно помноженную на полином из K .

С помощью этого элементарного преобразования строк будем уменьшать степени по s элементов первой строки до тех пор, пока один из элементов первой строки не станет делителем другого (т. е. если на следующем шаге в первой строке получим 0, то этот шаг делать не надо).

$\begin{pmatrix} s^3 & 1 & 0 \\ s^2 + 1 & 0 & 1 \end{pmatrix} : \begin{pmatrix} -s & 1 & -s \\ s^2 + 1 & 0 & 1 \end{pmatrix}$ (к первой строке прибавили вторую, предварительно помноженную на $-s$)

$$: \begin{pmatrix} -s & 1 & -s \\ 1 & s & 1-s^2 \end{pmatrix} \text{ (ко второй строке прибавили первую, предварительно помноженную на } s).$$

3. В первом столбце получена единица. На следующем шаге в первом столбце должны получить 0. Поэтому элементарные преобразования строк матрицы закончены.

Рассмотрим вектор – строку полученной матрицы, в которой в первом месте стоит делитель первой ячейки другой строки: $(1, s, 1-s^2)$.

Первый элемент вектора – это наибольший общий делитель d элементов a, b ; второй и третий элементы – это полиномы x, y .

Итак, $x = s, y = 1-s^2$.

4. Несложно проверить, что $ax + by = d : s^3 \cdot s + (1+s^2) \cdot (1-s^2) = 1$.

5. При желании полином d можно нормировать – вектор можно поделить на старший коэффициент полинома d .

Обоснование алгоритма. Введём обозначения: K_3 – множество строчек-троек полиномов из K ; V – множество троек (z, x, y) из K_3 таких, что $z = ax + by$; V^2 – множество столбцов высоты 2, элементы которых лежат в V , или множество матриц 2×3 , у которых строки – элементы из V .

Равенство $z = ax + by$ равносильно тому, что $-z + ax + by = 0$. Поэтому V есть аннулятор

столбца $\begin{pmatrix} -1 \\ a \\ b \end{pmatrix}$.

Элементарные преобразования строк произвольной матрицы 2×3 равносильны умножению этой матрицы справа на матрицу 2×2 с единичным определителем (точнее, даже треугольную матрицу с единицами на главной диагонали).

Теперь понятно, что V^2 есть левый $M_2(K)$ -модуль. Значит, при элементарных преобразованиях матриц из V^2 получаем матрицу из V_2 со строками из V .

Поэтому в конце, когда получим тройку (d, x, y) , автоматически будет выполнено равенство $d = xa + yb$.

10. ПРИМЕР

Рассмотрим $n = 2$, $A = s \cdot E = \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix}$. Можно сразу привести два разложения матрицы A : $\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$, $\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}$. Кажется, будто бы все разложения матрицы A этими двумя и ограничиваются, но это не так. Покажем это с помощью алгоритма отщепления.

Рассмотрим произвольное $m \in \bar{n}$. Тогда $AK^m = sK^m$, $K^m / (AK^m) = K^m / (sK^m) \cong k^m$ ($\cong$ – значок изоморфизма). Здесь имеется в виду изоморфизм K -модулей; элемент s зануляет (аннулирует) весь K -модуль k^m .

Специализируем это для $n = 2$: $AK^2 = sK^2$, $K^2 / (AK^2) \cong k^2$.

1. $\text{Ann} = k^2$.

2. Можно (и нужно) выбрать любой ненулевой элемент $\bar{X}$ из $\text{Ann} = k^2$. Если выберем $\bar{X} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ или $\bar{X} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, то получим оба приведённых выше диагональных разложения матрицы A . Выберем $\bar{X} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $X = \bar{X}$.

3. Составим из X и из столбцов матрицы A матрицу: $\begin{pmatrix} 1 & s & 0 \\ 1 & 0 & s \end{pmatrix}$.
4. Элементарными преобразованиями столбцов приведём эту матрицу к ступенчатому виду: $\begin{pmatrix} 1 & s & 0 \\ 1 & 0 & s \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & -s & s \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & s & 0 \end{pmatrix}$.
5. Исключим нулевой столбец. Полученную матрицу $\begin{pmatrix} 1 & 0 \\ 1 & s \end{pmatrix}$ обозначим через B .
6. Вычислим определитель матрицы B : $\det(B) = s \neq 0$.
7. Выпишем для B дополнительную матрицу $\bar{B}$: $\bar{B} = \begin{pmatrix} s & 0 \\ -1 & 1 \end{pmatrix}$ (для этого в матрице 2×2 элементы по диагонали меняют местами, а у элементов вне диагонали меняют знак).
8. Выпишем матрицу B^{-1} , обратную к B : $B^{-1} = (\det B)^{-1} \cdot \bar{B} = s^{-1} \cdot \begin{pmatrix} s & 0 \\ -1 & 1 \end{pmatrix}$.
9. Вычислим матрицу $C = B^{-1}A$: $C = B^{-1}A = s^{-1}\bar{B} \cdot s \cdot E = \bar{B} = \begin{pmatrix} s & 0 \\ -1 & 1 \end{pmatrix}$.

Таким образом, получено разложение матрицы A (в произведение простых матриц): $A = BC = B\bar{B}$, или $\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & s \end{pmatrix} \begin{pmatrix} s & 0 \\ -1 & 1 \end{pmatrix}$.

Замечание. Полученный пример является частным случаем разложений

$$B\bar{B} = \det(B) \cdot E, \quad \bar{B}B = \det(B) \cdot E.$$

Здесь B – любая квадратная матрица; $\bar{B}$ – дополнительная к ней. Если матрица B размера 2×2 и определитель $\det(B)$ простой, то матрицы B , $\bar{B}$ простые, и приведённые выше разложения есть разложения в произведение простых матриц.

ЗАКЛЮЧЕНИЕ

В работе исследован вопрос об единственности разложения невырожденных полиномиальных матриц на простые множители (матрицы n на n над алгеброй полиномов от одной буквы).

СПИСОК ЛИТЕРАТУРЫ

1. Дэвенпорт Г. Высшая арифметика. Введение в теорию чисел. – М.: Наука, Гл. ред. физ.-мат. лит., 1965. – 176 с.
2. Евклид. Начала: пер. с греч. В 3 т. – М.-Л.: ГИТТЛ, 1948-1950. – 507 с. – Т. 1: кн. I-VI; т. 2: кн. VII-IX; т. 3: кн. X-XII.
3. Хрестоматия по истории математики. Алгебра. Теория чисел. Геометрия: учеб. пособие для физ.-мат. фак. пед. ин-в / И.Г. Башмакова, Ю.А. Белый, С.С. Демидов, Б.А. Розенфельд, А.П. Юшкевич. – М.: Просвещение, 1976. – 316 с.
4. Бурбаки Н. Очерки по истории математики: пер. с фр. – М.: ИЛ, 1963. – 292 с.
5. Гаусс К.Ф. Труды по теории чисел. – М.: Изд-во АН СССР, 1959. – 979 с.
6. Начала гидростатики. Архимед, Стевин, Галилей, Паскаль / под общ. ред И.И. Агола и др. – М.-Л.: Гос. техн.-теорет. изд-во, 1932. – 413 с.
7. Бурбаки Н. Алгебра. Т. 3. Модули, кольца, формы. – М.: Наука, гл. ред. физ.-мат. лит., 1966. – 554 с.
8. Бурбаки Н. Коммутативная алгебра. – М.: Мир, 1971. – 706 с.
9. Кострикин А.И. Введение в алгебру. Основы алгебры. – М.: Наука, 1994. – 319 с.
10. Алгебра и теория чисел: учеб. пособие для студентов-заочников II курса физ.-мат. факультетов пед. ин-тов / Н.А. Казачек, Г.Н. Перлатов, Н.Я. Виленкин, А.И. Бородин. – М.: Просвещение, 1984. – 193 с.

11. Винберг Е.Б. Алгебра многочленов: учеб. пособие для студентов-заочников III-IV курсов физ.-мат. факультетов пед. ин-тов. – М.: Просвещение, 1980. – 175 с.
12. Куликов Л.Я. Алгебра и теория чисел: учеб. пособие для пед. ин-тов по спец. «Математика», «Математика и физика», «Физика и математика». – М.: Высш. шк., 1979. – 562 с.
13. Anthaklis P.J., Michel A.N. Linear Systems. – Boston: Birkhauser, 2006. – 670 p.
14. Wang Qing-Guo. Decoupling Control. – Berlin Heidelberg: Springer-Verlag, 2003. – 356 p.
15. Vidyasagar M. Control system sythesis: a factorization approach. Pt. 1. – San Rafael, CA: Morgan & Claypool, 2011. – 184 p.
16. Vidyasagar M. Control system sythesis: a factorization approach. Pt. 2. – San Rafael, CA: Morgan & Claypool, 2011. – 227 p.
17. Kailath T. Linear Systems. – Englewood Cliffs, New York: Prentice-Hall, 1980. – 704 p.
18. Wolovich W. Linear Multivariable Control. – Berlin; Heidelberg: Springer-Verlag, 1974. – 368 p.
19. Воевода А.А. Матричные передаточные функции (основные понятия): учеб. пособие. – Новосибирск: изд-во НГТУ, 1994. – 95 с.
20. Воевода А.А. Матричные передаточные функции (синтез): конспект лекций. – Новосибирск: изд-во НГТУ, 1995. – 95 с.
21. MacDuffee C.C. The Theory of Matrices. – Berlin: Springer, 1933. – 119 p.
22. Cahen E. Théory des nombres. Vol. 1. – Paris: Librairie scintifique A. Hermann & Fils, 1914. – 425 p.

Корюкин Анатолий Николаевич, кандидат физико-математических наук, старший научный сотрудник Института математики им. Соболева. Основные направления научных исследований – теория ассоциативных некоммутативных колец, математические основы теории автоматического управления. Имеет более 40 публикаций. E-mail: koryukin@sibmail.ru

*The decomposition on simple multipliers of nondegenerate polinomialny matrixes**

A.N. KORYUKIN[†]

[†] Sobolev's Institute of mathematics, 4 prospect Koptyuga, Novosibirsk, 630090, Russian Federation, candidate of physical and mathematical sciences, senior researcher, e-mail: koryukin@sibmail.ru

Object of research. In algebra of polinomialny matrixes (over algebra of K of polynoms from one letter) the size n on n the question of uniqueness of decomposition on simple multipliers is studied. **Urgency.** The theory of divisibility is a classical part of the mathematics which has entered into process of training in higher educational institutions. But still the question of uniqueness of decomposition on simple multipliers was studied only for commutative algebras, and only in the absence of zero dividers. Meanwhile in the linear theory of automatic control (multichannel systems) long ago concepts of the greatest left and right dividers of polinomialny matrixes that can form a basis of the theory of divisibility for polinomialny matrixes also are successfully used. The most important question of the theory of divisibility - existence and uniqueness of decomposition on simple multipliers. The question of uniqueness of decomposition on simple multipliers is complicated by that in a ring of matrixes there is no commutativity. **Results.** It is shown that in a ring of polinomialny matrixes the left and right ideals main (matrixes over algebra of polynoms from one letter). From this it follows that for any number of nondegenerate matrixes there is the greatest left divider, the greatest right divider, the smallest left multiple, smallest right multiple. It is shown that for any nondegenerate matrix there is a decomposition on simple multipliers. Indecomposable matrixes are characterized: it in accuracy of a matrix with simple (indecomposable) determinant. The problem of uniqueness of decomposition is solved on simple multipliers so: for any nondegenerate matrix of A all simple right dividers (simple matrixes of B for which there is a matrix the C such that $A = BC$) are described. This description is made in terms of a lattice of K -submodules n -ok polynoms of K . The decomposition of $A = BC$ allows to find all decomposition of a nondegenerate matrix of A on simple multipliers. These searches are written down in the form of two algorithms (for mathematicians and for engineers). Some invariants of decomposition of a matrix on simple multipliers are described. Some special cases of decomposition are described. One example of decomposition is given. **Technique and tools.** Theory of rings. Divisibility theory.

Keywords: Polinomialny matrixes, simple multipliers, indecomposable elements, decomposition on simple multipliers, uniqueness of decomposition on simple multipliers, the theorem of uniqueness of decomposition on the simple multipliers, the greatest general left divider, the greatest general right divider

* Received 01 July 2013.

REFERENCES

1. Davenport H. *The higher arithmetic. An Introduction to the theory of numbers*. New Jork, Harper & Brothers, 1960. (Russ. ed.: Devenport G. *Vysshaya arifmetika. Vvedenie v teoriyu chisel*. Moskow, Nauka Publ., Glavnaya redaktsiya fiziko-matematicheskoi literatury, 1965. 176 p.).
2. Evklid. *Nachala*. V 3 t. Perevod s grecheskogo [Beginnings. Translation from Greek. In 3 vol.]. Moscow, Leningrad, GITTL Publ., 1948-1950. 507 p. Vol. I: books of I-VI. Vol. II: books of VII-IX. Vol. III: books X-XII.
3. Bashmakova I.G., Belyi Yu.A., Demidov S.S., Rozenfeld B.A., Yushkevich A.P. *Khrestomatiya po istorii matematiki. Algebra. Teoriya chisel. Geometriya*. [Anthology of mathematics history. Algebra. Theory of numbers. Geometry]. Moscow, Prosveshchenie Publ., 1976. 316 p.
4. Bourbaki N. *Elements of the History of Mathematics*. Translation from French. 1960 (Russ. ed.: Burbaki N. *Ocherki po istorii matematiki*. Moscow, IL Publ., 1963. 292 p.).
5. Gauss K.F. *Untersuchungen über höhere Arithmetik*. Translated from Latin. Springer, 1889. (Russ. ed.: Gauss K.F. *Trudy po teorii chisel*. Moscow, Academy of Sciences of the USSR Publ., 1959. 979 p.).
6. Agola I.I., ed., et al. *Nachala gidrostatiki. Arkhimed, Stevin, Galilei, Paskal'* [Began hydrostatics. Archimedes, Galilei, Pascal, Stevin]. Moscow, Leningrad, Gosudarstvennoe tekhniko-teoreticheskoe izdatel'stvo, 1932. 413 p.
7. Bourbaki N. *Algebre*. Vol. 3. Translation from French], Paris, Heimann, 1962. (Russ. ed.: Burbaki N. *Algebra. T. 3. Moduli, kol'tsa, formy*. Moscow, Nauka Publ., Glavnaya redaktsiya fiziko-matematicheskoi literatury, 1966. 554 p.).
8. Bourbaki N. *Algebre commutative* (Russ. ed.: Burbaki N. *Kommutativnaya algebra*. Moscow, Mir Publ., 1971. 706 p.).
9. Kostrikin A.I. *Vvedenie v algebru. Osnovy algebrы* [Introduction in algebra. Algebra bases]. Moscow, Nauka Publ., 1994. 319 p.
10. Kazachek N.A., Perlatov G.N., Vilenkin N.Ya., Borodin A.I. *Algebra i teoriya chisel* [Algebra and theory of numbers]. Moscow, Prosveshchenie Publ., 1984. 193 p.
11. Vinberg E.B. *Algebra mnogochlenov* [Algebra of multinomials]. Moscow, Prosveshchenie Publ., 1980. 175 p.
12. Kulikov L.Ya. *Algebra i teoriya chisel* [Algebra and theory of numbers]. Moscow, Vysshaya shkola Publ., 1979. 562 p.
13. Anthaklis Panos J., Michel Antjony N. *Linear Systems*. Boston, Birkhauser, 2006. 670 p.
14. Wang Qing-Guo. *Decoupling Control*. Berlin, Heidelberg, Springer-Vedrlag, 2003. 356 p.
15. Vidyasagar M. *Control system sythesis: a factorization approach*. Pt. I. San Rafael, CA, Morgan & Claypool, 2011. 184 p.
16. Vidyasagar M. *Control system sythesis: a factorization approach*. Pt. II. San Rafael, CA, Morgan & Claypool, 2011. 227 p.
17. Kailath T. *Linear Systems*. Englewood Cliffs, New Jork, Prentice-Hall, 1980. 704 p.
18. Wolovich W. *Linear Multivariable Control*. Berlin, Heidelberg, Springer-Verlag, 1974. 368 p.
19. Voevoda A.A. *Matrichnye peredatochnye funktsii (osnovnye ponyatiya)* [Matrix transfer functions (the main concepts)]. Novosibirsk, NSTU Publ., 1994. 95 p.
20. Voevoda A.A. *Matrichnye peredatochnye funktsii (sintez)* [Matrix transfer functions (synthesis)]. Novosibirsk, NSTU Publ., 1995. 95 p.
21. MacDuffee C.C. *The Theory of Matrices*. Berlin, Springer, 1933. 119 p.
22. Cahen E. *Théory des nombres*. Vol. 1. Paris, Librairie scientifique A. Hermann & Fils, 1914. 425 p.