Вестник Нижегородского университета им. Н.И. Лобачевского, 2008, № 4, с. 122–126

УДК 512.64

О ПОДОБИИ МАТРИЦ ВТОРОГО ПОРЯДКА НАД КОЛЬЦОМ ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ, ИМЕЮЩИХ ПРИВОДИМЫЙ ХАРАКТЕРИСТИЧЕСКИЙ МНОГОЧЛЕН

С.В. Сидоров

Нижегородский госуниверситет им. Н.И. Лобачевского

sesidorov@yandex.ru

Поступила в редакцию 05.05.2008

Рассматривается задача о подобии матриц второго порядка над кольцом целых гауссовых чисел с приводимым характеристическим многочленом. Описаны классы подобных матриц, приведены канонические матрицы для каждого класса и найдено число классов.

Ключевые слова: подобие матриц, целые гауссовы числа.

Введение

Задача о подобии матриц с коэффициентами из некоторого поля F хорошо известна в линейной алгебре. Две квадратные матрицы $A, B \in F^{n\times n}$ называют подобными над полем F, если существует такая невырожденная матрица $S \in F^{n\times n}$, что $AS = SB$. Подобные матрицы являются матрицами одного и того же линейного преобразования в разных базисах. Существует известный алгоритм определения подобия матриц над полем, который основывается на приведении характеристической матрицы $A-\lambda E$ к нормальной диагональной форме Смита (см. например, [1]). Этот алгоритм использует тот факт, что кольцо многочленов $F[\lambda]$ является евклидовым.

Понятие подобия матриц над полем F легко обобщается на произвольное коммутативное кольцо K с единицей. При этом требуется, чтобы матрица S была обратима над кольцом K, что эквивалентно условию $\det S \in K^*$, где K^* – множество обратимых элементов кольца K. Поскольку кольцо $K[\lambda]$ не является евклидовым, если K не поле, в этом случае алгоритм приведения к нормальной диагональной форме Смита не работает. Это усложняет задачу. В данной работе рассматривается подобие матриц над кольцом целых гауссовых чисел $Z[i]$. Очевидно, что $Z[i]^* = \{1,-1,i,-i\}$.

Определение 1. *Будем говорить, что матрица* $B \in Z[i]^{n\times n}$ *подобна матрице* $A \in Z[i]^{n\times n}$, *если существует такая матрица* $S \in Z[i]^{n\times n}$, *что* $AS = SB$ *и* $\det S \in Z[i]^*$, *и обозначать это A~B. При этом матрица* S *называется трансформирующей A в B матрицей.*

Ясно, что отношение подобия есть отношение эквивалентности. Следовательно, множество матриц порядка n разбивается на классы подобных матриц. Очевидно, если матрицы подобны над кольцом $Z[i]$, то они подобны и над полем рациональных гауссовых чисел $Q[i]$. Следовательно, класс $K_{Q[i]}(A)$ матриц, подобных A над полем $Q[i]$, разбивается на подклассы матриц, подобных над $Z[i]$. Пусть $K_{Z[i]}(A) = \{B \in Z[i]^{n\times n} \mid A \sim B\}$ – множество матриц, подобных матрице A над кольцом $Z[i]$.

Возникают две задачи: 1) для данных матриц A и B выяснить, являются ли они подобными над $Z[i]$, и если являются, найти трансформирующую матрицу; 2) описать классы подобных матриц, т.е. выделить в каждом классе матрицу простейшего вида (каноническую матрицу), которая бы однозначно характеризовала класс.

Здесь мы ограничимся рассмотрением матриц второго порядка, имеющих приводимый характеристический многочлен. Одним из необходимых условий подобия матриц является равенство их характеристических многочленов. Поэтому сразу предположим, что матрицы A и B имеют один и тот же характеристический многочлен $d(\lambda) = \lambda^2 - a\lambda + b$, где a – след матриц, b – определитель. Поскольку $d(\lambda)$ приводим над $Z[i]$, то оба его корня принадлежат $Z[i]$. Пусть $d(\lambda)=(\lambda-\alpha)(\lambda-\beta)$ и $x=(x_1,x_2)^T$ – собственный вектор матрицы A, соответствующий собственному числу α, причем $x\in Z[i]^2$ и НОД$(x_1,x_2)=1$. Тогда найдется такой вектор $y\in Z[i]^2$, что $\det T=1$, где T – матрица, столбцами которой являются векторы x и y. Система векторов x,y образует базис пространства $Q[i]^2$. Определим в пространстве $Q[i]^2$ линейное преобразование φ, матрицей которого в стандартном базисе является матрица A. Тогда в базисе x,y матрица преобразования φ будет иметь вид $C=$ $=T^{-1}AT=\begin{pmatrix}\alpha & r\\ 0 & \beta\end{pmatrix}\in Z[i]^{2\times 2}$, т.е. матрицы A и C подобны над $Z[i]$. Рассмотрим два возможных случая: 1) $\alpha=\beta$; 2) $\alpha\neq\beta$.

Случай кратного собственного числа

В первом случае $d(\lambda)=(\lambda-\alpha)^2$. Над полем рациональных гауссовых чисел $Q[i]$ матрица с таким характеристическим многочленом подобна одной из жордановых матриц: $J_1=\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}$ или $J_2=\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}$, т.е. $K_{Q[i]}(J_1)=$ $=\{A\in Z[i]^{2\times 2}\mid A\approx J_1\}=\{J_1\}$, $K_{Q[i]}(J_2)=$ $=\{A\in Z[i]^{2\times 2}\mid A\approx J_2\}$, где символом $\approx$ обозначено подобие матриц над полем $Q[i]$. Выясним, что изменится над $Z[i]$. Ясно, что класс $K_{Q[i]}(J_1)=\{J_1\}$, состоящий из одной матрицы, совпадает с классом $K_{Z[i]}(J_1)$. Любая матрица из класса $K_{Q[i]}(J_2)$ подобна над $Z[i]$ некоторой матрице вида $\begin{pmatrix}\alpha & r\\ 0 & \alpha\end{pmatrix}$, где $r\neq 0$. Но в силу того, что $\begin{pmatrix}\alpha & r\\ 0 & \alpha\end{pmatrix}\sim\begin{pmatrix}\alpha & -r\\ 0 & \alpha\end{pmatrix}\sim\begin{pmatrix}\alpha & ir\\ 0 & \alpha\end{pmatrix}\sim\begin{pmatrix}\alpha & -ir\\ 0 & \alpha\end{pmatrix}$, можно считать, что коэффициент $r=r_1+ir_2$ удовлетворяет условию $r_1>0, r_2\geq 0$. Теперь покажем, что матрицы $A_1=\begin{pmatrix}\alpha & r'\\ 0 & \alpha\end{pmatrix}$, $A_2=\begin{pmatrix}\alpha & r''\\ 0 & \alpha\end{pmatrix}$ не подобны, если числа r' и r'' не равны и удовлетворяют написанным выше условиям. Действительно, если $A_1\sim A_2$, то существует матрица $T=\begin{pmatrix}t_{11} & t_{12}\\ t_{21} & t_{22}\end{pmatrix}$ такая, что $A_1T=TA_2$ и $\det T\in Z[i]^*$. Тогда

$$A_1T=\begin{pmatrix}\alpha t_{11}+r't_{21} & \alpha t_{12}+r't_{22}\\ \alpha t_{21} & \alpha t_{22}\end{pmatrix}=$$

$$=\begin{pmatrix}\alpha t_{11} & r''t_{11}+\alpha t_{12}\\ \alpha t_{21} & r''t_{21}+\alpha t_{22}\end{pmatrix}=TA_2.$$

Отсюда следует, что $t_{21}=0$, $r't_{22}-r''t_{11}=0$, значит $t_{11},t_{22}\in \mathrm{Z[i]}^*$ и $\frac{r'}{r''}\in \mathrm{Z[i]}^*$. Но из-за ограничений на r',r'' выполнение условия $\frac{r'}{r''}\in \mathrm{Z[i]}^*$ невозможно. Тем самым доказана следующая теорема.

Теорема 1. Пусть $d(\lambda)=(\lambda-\alpha)^2$. Тогда

1) $K_{Q[i]}(J_1)=K_{Z[i]}(J_1)=\{J_1\}$;

2) $K_{Q[i]}(J_2)=\bigcup\limits_{r\in M}K_{Z[i]}(R_r(\alpha))$, где $R_r(\alpha)=$ $=\begin{pmatrix}\alpha & r\\ 0 & \alpha\end{pmatrix}$ – каноническая матрица и $M=\{r=$ $=u+iv\in Z[i]\mid u>0, v\geq 0\}$.

Случай различных собственных чисел

Теперь рассмотрим случай, когда характеристический многочлен $d(\lambda)$ имеет различные корни, т.е. $d(\lambda)=(\lambda-\alpha)(\lambda-\beta)$, $\alpha\neq\beta$. Над полем $Q[i]$ матрица, имеющая такой характеристический многочлен, подобна диагональной матрице $J_3=\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$, т.е. $K_{Q[i]}(J_3)=$ $=\{A\in Z[i]^{2\times 2}\mid A\approx J_3\}$. Каждая матрица из $K_{Q[i]}(J_3)$ подобна над $Z[i]$ некоторой матрице $\begin{pmatrix}\alpha & r\\ 0 & \beta\end{pmatrix}$. Выясним, при каком условии подобны две матрицы вида $A_1=\begin{pmatrix}\alpha & r'\\ 0 & \beta\end{pmatrix}$ и $A_2=\begin{pmatrix}\alpha & r''\\ 0 & \beta\end{pmatrix}$. Если они подобны, то найдется матрица $T=\begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$ такая, что $A_1T=TA_2$ и $\det T\in Z[i]^*$. Тогда

$$A_1T=\begin{pmatrix} \alpha t_{11}+r't_{21} & \alpha t_{12}+r't_{22} \\ \beta t_{21} & \beta t_{22} \end{pmatrix}=$$

$$=\begin{pmatrix} \alpha t_{11} & r''t_{11}+\beta t_{12} \\ \alpha t_{21} & r''t_{21}+\beta t_{22} \end{pmatrix}=TA_2.$$

Из этого равенства следует, что $(\beta-\alpha)t_{21}=0$, т.е. $t_{21}=0$ и $(\beta-\alpha)t_{12}=r't_{22}-r''t_{11}$. Поскольку $\det T\in Z[i]^*$, то $t_{11},t_{22}\in Z[i]^*$ и $r''=\varepsilon r'+$ $+(\beta-\alpha)q$, где $\varepsilon=\frac{t_{22}}{t_{11}}\in Z[i]^*$ и $q=\frac{-t_{12}}{t_{11}}\in Z[i]$.

Определение 2. *Пусть I – произвольный идеал кольца $Z[i]$. Будем говорить, что два элемента $a,b\in Z[i]$ являются I-эквивалентными (или эквивалентными относительно идеала I), если существует такое $\varepsilon\in Z[i]^*$, что $a+b\varepsilon\in I$.*

Легко проверить, что введенное отношение I-эквивалентности является отношением эквивалентности на множестве элементов кольца $Z[i]$. Таким образом, имеет место следующее утверждение.

Утверждение 1. Две матрицы $A_1=\begin{pmatrix} \alpha & r' \\ 0 & \beta \end{pmatrix}$ и $A_2=\begin{pmatrix} \alpha & r'' \\ 0 & \beta \end{pmatrix}$ подобны над кольцом $Z[i]$ тогда и только тогда, когда r' и r'' эквивалентны относительно идеала $I=(\beta-\alpha)$, порожденного элементом $\beta-\alpha$.

Пусть $\beta-\alpha=m+ni$. Не уменьшая общности можно считать $n\ge 0$, а если $n=0$, то $m>0$. Из определения I-эквивалентности следует, что класс эквивалентности K_a, содержащий элемент $a\in Z[i]$, является объединением четырех смежных классов: $a+I, -a+I, ia+I, -ia+I$. Следовательно, в качестве представителя класса эквивалентности можно взять элемент из некоторого смежного класса. Известно, что представителем любого смежного класса фактор-кольца кольца $Z[i]$ по идеалу $I=$ $=(m+ni)$ является некоторая точка квадрата с вершинами 0, $m+ni$, $-n+mi$, $(m-n)+$ $+(m+n)i$ (см. рис. 1). Этот квадрат обозначим

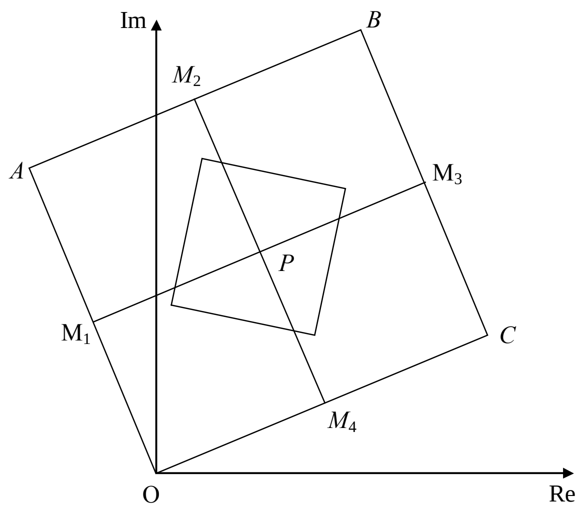

Рис. 1. Квадрат $K(m, n)$

через $K(m,n)$. Но не все точки квадрата $K(m,n)$ принадлежат разным классам I-эквивалентности. Действительно, легко показать, что для любого $a\in Z[i]$ точки a, $2P-a$, $P+i(P-a)$ и $P-i(P-a)$, где $P=\frac{m-n}{2}+$ $+\frac{m+n}{2}i$ – центр рассматриваемого квадрата, эквивалентны относительно идеала I. Заметим, что эти точки также образуют квадрат с центром в точке P. Кроме того, если точка a принадлежит исходному квадрату $K(m,n)$, то полученный новый квадрат находится внутри исходного. Верно и обратное: если точки образуют вершины квадрата с центром P, то они I-эквивалентны. Следовательно, представитель любого класса эквивалентности находится в квадрате $K\left(\frac{m}{2},\frac{n}{2}\right)$ (на рисунке это квадрат OM_1PM_4). Заметим, что точки на сторонах OM_1 и M_1P эквивалентны точкам на сторонах OM_4 и M_4P соответственно.

Обозначим через $K(m+ni)$ множество целочисленных точек, лежащих внутри квадрата $K(m,n)$ и на двух его смежных сторонах, содержащих вершины 0, $m+ni$, $(m-n)+$ $+(m+n)i$. Из приведенных выше рассуждений следует лемма.

Лемма 1. Элементы из $K\left(\frac{m}{2}+\frac{n}{2}i\right)$ образуют множество представителей всех классов эквивалентности относительно идеала $I=$

$=(m+ni)$. Различные элементы в $K\left(\frac{m}{2}+\frac{n}{2}i\right)$ не являются *I*-эквивалентными.

Осталось вычислить количество классов эквивалентности относительно идеала $I=(m+ni)$. Обозначим число таких классов через $N(I)$. Для вычисления $N(I)$ нам понадобится следующая лемма (см. например, [2]).

Лемма 2 (формула Пика, 1899). Если внутри многоугольника с вершинами в точках с целыми координатами лежат s, а на границе – p целочисленных точек, то площадь многоугольника равна $s+\frac{p}{2}-1$.

Лемма 3. Пусть $I=(m+ni)$ – идеал, порожденный элементом $m+ni$. Тогда верны следующие утверждения.

1) Если $m\equiv 0(\operatorname{mod} 2)$, $n\equiv 0(\operatorname{mod} 2)$, то $N(I)=\frac{m^2+n^2}{4}+2$.

2) Если $m+n\equiv 1(\operatorname{mod} 2)$, то $N(I)=\frac{m^2+n^2+3}{4}$.

3) Если $m\equiv 1(\operatorname{mod} 2)$, $n\equiv 1(\operatorname{mod} 2)$, то $N(I)=\frac{m^2+n^2+6}{4}$.

Доказательство. Согласно лемме 1 $N(I)$ равно мощности множества $K\left(\frac{m}{2}+\frac{n}{2}i\right)$. В силу симметрии внутри квадратов OM_1PM_4, M_1AM_2P, M_2BM_3P, M_3CM_4P находится одинаковое количество целочисленных точек (обозначим его через s). Через p_1 обозначим количество целочисленных точек, лежащих на каждой из сторон M_1P, M_2P, M_3P, M_4P, не считая вершин. Через p_2 обозначим количество целочисленных точек, лежащих на каждой из сторон OM_1, M_1A, AM_2, M_2B, BM_3, M_3C, CM_4, M_4O, не считая вершин. Рассмотрим три возможных варианта.

1) $m\equiv 0(\operatorname{mod} 2)$, $n\equiv 0(\operatorname{mod} 2)$.

В этом случае вершины квадрата $K\left(\frac{m}{2},\frac{n}{2}\right)$ являются целочисленными, поэтому можно непосредственно применить формулу Пика. Внутри квадрата $K\left(\frac{m}{2},\frac{n}{2}\right)$ находится s, а на границе $2p_1+2p_2+4$ целочисленных точек. Следовательно, по Лемме 2 $s+p_1+p_2+2-$ $-1=\frac{m^2+n^2}{4}$. Так как $N(I)=s+p_1+p_2+3$, то $N(I)=\frac{m^2+n^2}{4}+2$.

2) $m+n\equiv 1(\operatorname{mod} 2)$.

Здесь воспользуемся леммой 2 для квадрата $K(m,n)$. Согласно этой лемме $4s+4p_1+$ $+\frac{8p_2+4}{2}-1=m^2+n^2=m^2+n^2$. Поскольку $N(I)=s+p_1+p_2+1$, то $N(I)=\frac{m^2+n^2+3}{4}$.

3) $m\equiv 1(\operatorname{mod} 2)$, $n\equiv 1(\operatorname{mod} 2)$.

Аналогично предыдущему случаю по формуле Пика, примененной к квадрату $K(m,n)$, имеем $4s+4p_1+1+\frac{8p_2+4}{2}-1=m^2+n^2$. Так как $N(I)=s+p_1+p_2+2$, то $N(I)=$ $=\frac{m^2+n^2+6}{4}$. Лемма доказана.

Из утверждения 1 и леммы 3 непосредственно следует теорема.

Теорема 2. Пусть $d(\lambda)=(\lambda-\alpha)(\lambda-\beta)$, $\alpha\neq\beta$, причем можно считать, что $\beta-\alpha=$ $=m+ni$, где $n\geq 0$, а если $n=0$, то $m>0$. Тогда $K_{Q[i]}(J_3)=\bigcup_{k\in M}K_{Z[i]}(R_k(\alpha,\beta))$, где $R_k(\alpha,\beta)=$ $=\begin{pmatrix}\alpha & k\\ 0 & \beta\end{pmatrix}$ – каноническая матрица и $M=$ $=K\left(\frac{m}{2}+\frac{n}{2}i\right)$. Число классов подобия $N(\alpha,\beta)=$ $=|M|$ определяется следующим образом:

1) если $m\equiv 0(\operatorname{mod} 2)$, $n\equiv 0(\operatorname{mod} 2)$, то $N(\alpha,\beta)=\frac{|\beta-\alpha|^2}{4}+2$;

2) если $m+n\equiv 1(\bmod 2)$, то $N(\alpha,\beta)=$ $=\dfrac{|\beta-\alpha|^2+3}{4}$;

3) если $m\equiv 1(\bmod 2)$, $n\equiv 1(\bmod 2)$, то $N(\alpha,\beta)=\dfrac{|\beta-\alpha|^2+6}{4}$.

Суммируя приведенные результаты, отметим, что в случае кратного собственного числа количество классов подобия счетно, а в случае различных собственных чисел конечно.

Список литературы

1. Мальцев А.И. Основы линейной алгебры. ОГИЗ, 1948. 424 с.

2. Прасолов В.В. Задачи по планиметрии. М: МЦНМО, 2006. 635 с.

ON SIMILARITY OF 2×2 MATRICES OVER THE RING OF GAUSSIAN INTEGERS WITH REDUCIBLE CHARACTERISTIC POLYNOMIAL

S.V. Sidorov

The similarity problem for 2×2 matrices over the ring of Gaussian integers with reducible characteristic polynomial is considered. The classes of similar matrices are described, canonical matrices for each class are given, and the number of similarity classes has been found.