

Глава 18

Кольца и поля

18.1. Линейная алгебра

Пусть K — кольцо, F — поле. Введена операция умножения элементов кольца K на элементы поля F , причем K является линейным пространством над F . Причем для любых $a, b \in K$ и любого $\alpha \in F$

$$\alpha(ab) = (\alpha a)b = a(\alpha b).$$

Тогда K называется *линейной алгеброй* (или просто *алгеброй*) над полем F . Ее размерностью называется размерность K как линейного пространства над F .

Пример 18.1.

1. Трехмерное векторное пространство $\mathbf{V}_3$ над полем $\mathbb{R}$, если в качестве операции умножения рассматривается векторное произведение.
2. Арифметическое пространство F^n над полем F с покомпонентной операцией умножения элементов из F^n .
3. Кольцо $F^{n \times n}$ является n^2 -мерной линейной алгеброй над полем F .
4. Поле $\mathbb{C}$ является двумерной линейной алгеброй над полем $\mathbb{R}$.
5. Поле $\{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Q}\}$ является двумерной линейной алгеброй над полем $\mathbb{Q}$.

Если V — конечномерное линейное пространство над полем F , то для того, чтобы задать в V операцию умножения, достаточно определить ее на элементах какого либо базиса $e_1, e_2, \dots, e_n$.

Действительно, если

$$a = \sum_{j=1}^n \alpha_j e_j, \quad b = \sum_{j=1}^n \beta_j e_j,$$

где $\alpha_j \in F, \beta_j \in F$, то

$$ab = \sum_{i=1}^n \alpha_i e_i \sum_{j=1}^n \beta_j e_j = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \beta_j e_i e_j.$$

Пример 18.2. Рассмотрим поле $\mathbb{C}$ как линейную алгебру над полем $\mathbb{R}$. Эта алгебра двумерная. В качестве базиса рассмотрим $1, i$. Операция умножения комплексных чисел полностью определяется всеми попарными произведениями:

$\cdot$	1	i
1	1	i
i	i	-1

Упражнение 18.3. Доказать, что алгебра комплексных чисел изоморфна линейной алгебре матриц вида

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix},$$

где $\alpha \in \mathbb{R}, \beta \in \mathbb{R}$.

Упражнение 18.4. Доказать, что алгебра $\{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Q}\}$ изоморфна линейной алгебре матриц вида

$$\begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix},$$

где $\alpha \in \mathbb{Q}, \beta \in \mathbb{Q}$.

18.2. Тело кватернионов

Рассмотрим множество $\mathbb{H}$ квадратных комплексных матриц вида

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix},$$

где $\alpha, \beta \in \mathbb{C}, a, b, c, d \in \mathbb{R}$. Легко проверить, что $\mathbb{H}$ образует двумерную линейную алгебру над $\mathbb{C}$ (подалгебру алгебры $\mathbb{C}^{2 \times 2}$). Эта алгебра образует тело. Действительно, любая ненулевая матрица A из $\mathbb{H}$ невырождена, так как

$$\begin{vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{vmatrix} = \alpha\bar{\alpha} + \beta\bar{\beta} = |\alpha|^2 + |\beta|^2 \neq 0,$$

если α и β одновременно не равны нулю, и, следовательно, для ненулевой матрицы A всегда существует обратная. Это тело некоммутативно, например,

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

Итак, $\mathbb{H}$ — тело, но не поле.

Тело $\mathbb{H}$ можно рассматривать как 4-мерную линейную алгебру над полем $\mathbb{R}$. Например, базис образуют матрицы

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Действительно, эти матрицы линейно независимы над $\mathbb{R}$, а разложение произвольной матрицы из $\mathbb{H}$ по этим матрицам имеет вид:

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}.$$

Таблица умножения для базисных элементов имеет вид:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Например, $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$ и т. д.

Тело (алгебра) $\mathbb{H}$ называется телом (алгеброй) *кватернионов*. Легко видеть, что множества кватернионов вида

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a\mathbf{1} \quad \text{и} \quad \begin{pmatrix} a+bi & 0 \\ 0 & a-bi \end{pmatrix} = a\mathbf{1} + bi,$$

где $a \in \mathbb{R}$, $b \in \mathbb{R}$, изоморфно полям (алгебрам) $\mathbb{R}$ и $\mathbb{C}$ соответственно. Это позволяет отождествить вещественные числа a с кватернионами вида $a\mathbf{1} + 0i + 0j + 0k$, а комплексные числа $a + bi$ с кватернионами вида $a\mathbf{1} + bi + 0j + 0k$. Таким образом, $\mathbf{1}$ можно рассматривать как обычную вещественную единицу, а i как «обычную» мнимую единицу i (но кроме нее в теле кватернионов есть еще две «мнимых единицы»: j и k).

Итак,

$$\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$$

и мы расширили понятие числа, построив надтело $\mathbb{H}$ поля $\mathbb{C}$.

Теорема 18.5 (Фробениус). Пусть T — тело, содержащее в себе поле $\mathbb{R}$, причем $ax = xa$ для любых $a \in \mathbb{R}$, $x \in T$ и T — конечномерная линейная алгебра над $\mathbb{R}$. Тогда T изоморфно либо $\mathbb{R}$, либо $\mathbb{C}$, либо $\mathbb{H}$.

Упражнение 18.6. Доказать, что алгебра $\mathbb{H}$ изоморфна алгебре вещественных матриц вида

$$\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix},$$

где $a, b, c, d \in \mathbb{R}$.

18.3. Идеал

Пусть K — ассоциативное кольцо. Подкольцо I кольца K называется его *левым идеалом*, если $IK \subseteq I$. Подкольцо I кольца K называется его *правым идеалом*, если $KI \subseteq I$. Если I является как левым, так и правым идеалом, то I называется просто *идеалом* (или *двусторонним идеалом*).

В любом кольцо K есть два *тривиальных* идеала: $\{0\}$ и K . Оказывается в теле других идеалов нет.

Утверждение 18.7. В любом теле T только два идеала: $\{0\}$ и T .

Доказательство. Пусть $I \neq \{0\}$, тогда найдется $a \in I$, $a \neq 0$. Тогда $1 = a^{-1}a \in I$, так как $a^{-1} \in T$, $a \in I$. Итак, $1 \in I$, но отсюда следует что $b = 1 \cdot b \in I$ для любого $b \in T$, откуда $T = I$. ■

Легко доказать

Утверждение 18.8. *Пересечение идеалов является идеалом.*

Минимальный по включению идеал, содержащий элемент a , называется *главным идеалом*, порожденным элементом a и обозначается (a) .

Утверждение 18.9. *Пусть a — элемент кольца K , тогда $(a) = \{ak + an : k \in K, n \in \mathbb{Z}\}$. Если кольцо K содержит единицу, тогда $(a) = \{ak : k \in K\}$.*

В кольце $\mathbb{Z}$ все идеалы главные. Действительно, все аддитивные группы (и подкольца) исчерпываются $n\mathbb{Z}$, где $n \in \mathbb{Z}$. Все они являются главными идеалами и других идеалов нет.

Аналогичная ситуация — в кольце многочленов $F[x]$ над полем F .

Утверждение 18.10. *В кольце многочленов $F[x]$ над полем F любой идеал главный.*

Доказательство. Пусть I — идеал кольца $F[x]$. Если $I = \{0\}$, то $I = (0)$. Пусть теперь $I \neq \{0\}$. Найдем в I ненулевой многочлен f минимальной степени. Докажем, что $I = (f)$. Действительно, пусть $g \in I$. Разделим g с остатком на f :

$$g = qf + r,$$

где $r = g - qf \in I$ — либо нулевой многочлен, либо $\deg r < \deg f$. Однако последнее противоречит условию минимальности степени многочлена f , значит, $r = 0$ и $g \in (f)$. ■

18.4. Фактор-кольцо

Пусть K — кольцо, а I — идеал в нем. Рассматривая I как подгруппу аддитивной группы K , построим фактор-группу K/I , состоящую из смежных классов $a + I$, где $a \in K$. Напомним, что операция сложения смежных классов определена равенством:

$$(a + I) + (b + I) = (a + b) + I, \quad (18.1)$$

т.е. *суммой* смежных классов, которым принадлежат элементы a и b , является смежный класс, которому принадлежит элемент $a + b$. Аналогично на множестве смежных классов определим операцию умножения:

$$(a + I) \cdot (b + I) = ab + I, \quad (18.2)$$

т.е. *произведением* смежных классов, которым принадлежат элементы a и b , называется смежный класс, которому принадлежит элемент ab .

Докажем, что это определение является корректным, т.е. результат произведения не зависит от представителей a и b , которых мы берем из смежных классов.

Утверждение 18.11. *Если $a' \in a + I$, $b' \in b + I$, тогда $a'b' \in ab + I$.*

Доказательство. Так как $a' \in a + I$, $b' \in b + I$, то найдутся $i \in I$ и $j \in I$, такие, что $a' = a + i$, $b' = b + j$, откуда

$$a'b' = (a + i)(b + j) = ab + \underbrace{ib + aj + ij}_{\in I} \in ab + I$$

($ib \in I$ и $aj \in I$, так как I — идеал). ■

Теперь легко видеть, что множество смежных классов $K/I = \{a + I : a \in K\}$ относительно введенных операций (18.1) и (18.2) образует кольцо. Оно называется *фактор-кольцом*.

18.5. Гомоморфизмы колец

Утверждение 18.12. Пусть I — идеал кольца K , тогда отображение $\eta : K \rightarrow K/I$, заданное формулой $\eta a = a + I$, где $a \in K$, является сюръективным гомоморфизмом из K в K/I .

Доказательство. Сюръективность отображения η очевидна. Для любых a, b из K имеем

$$\eta(a + b) = (a + b) + I = (a + I) + (b + I) = \eta a + \eta b,$$

$$\eta(a \cdot b) = ab + I = (a + I) \cdot (b + I) = \eta a \cdot \eta b,$$

это доказывает, что η — гомоморфизм. ■

Пусть $\varphi : K \rightarrow K'$ — гомоморфизм из кольца K в кольцо K' . Ядром гомоморфизма φ называется множество всех элементов из K , отображающихся в ноль $0'$ кольца K' :

$$\text{Кер } \varphi = \{x \in K : \varphi x = 0'\}.$$

Утверждение 18.13. Ядро $\text{Кер } \varphi$ гомоморфизма $\varphi : K \rightarrow K'$ является идеалом кольца K .

Доказательство. Легко проверить, что $\text{Кер } \varphi$ — подкольцо в K . Для любого $a \in K$ и любого $i \in I$ имеем

$$\varphi(ai) = \varphi a \cdot \varphi i = \varphi a \cdot 0' = 0', \quad \varphi(ia) = \varphi i \cdot \varphi a = 0' \cdot \varphi a = 0',$$

т. е. $ai \in \text{Кер } \varphi$, $ia \in \text{Кер } \varphi$, откуда $\text{Кер } \varphi$ — идеал. ■

Утверждение 18.14. Пусть $\varphi : K \rightarrow K'$ — гомоморфизм из кольца K в кольцо K' . Тогда образ φK гомоморфизма изоморфен фактор-кольцу $K/\text{Кер } \varphi$:

$$\varphi K \cong K/\text{Кер } \varphi,$$

а именно, отображение $\psi : K/\text{Кер } \varphi \rightarrow \varphi K$, определяемое формулой $\psi(a + \text{Кер } \varphi) = \varphi a$, является изоморфизмом.

Доказательство. Покажем, что ψ — изоморфизм. Сначала проверим, что отображение ψ является биекцией. Действительно, для любых a, b из K

$$\varphi a = \varphi b \Leftrightarrow 0' = \varphi b - \varphi a = \varphi(b - a) \Leftrightarrow b - a \in \text{Кер } \varphi \Leftrightarrow a + \text{Кер } \varphi = b + \text{Кер } \varphi.$$

$$\begin{array}{ccc}
 K & \xrightarrow{\varphi} & \varphi K \\
 & \searrow \eta \quad \swarrow \psi & \\
 & K / \text{Ker } \varphi &
 \end{array}$$

Теперь докажем, что φ — гомоморфизм. Для любых a, b из K имеем

$$\psi\left((a + \text{Ker } \varphi) + (b + \text{Ker } \varphi)\right) = \psi\left((a + b) + \text{Ker } \varphi\right) = \varphi(a + b) = \varphi a + \varphi b = \psi(a + \text{Ker } \varphi) + \psi(b + \text{Ker } \varphi),$$

$$\psi\left((a + \text{Ker } \varphi) \cdot (b + \text{Ker } \varphi)\right) = \psi(ab + \text{Ker } \varphi) = \varphi(ab) = \varphi a \cdot \varphi b = \psi(a + \text{Ker } \varphi) \cdot \psi(b + \text{Ker } \varphi),$$

что завершает доказательство. ■

18.6. Китайская теорема об остатках

Рассмотрим задачу восстановления целого числа по остаткам.

Пример 18.15. Пусть известно, что некоторое целое число x удовлетворяет условиям

$$0 \leq x < 60, \quad x \bmod 5 = 4, \quad x \bmod 4 = 3, \quad x \bmod 3 = 1.$$

Восстанавливается ли x по этим условиям и если да, то единственным ли образом? Ответ: $x = 19$ (единственное решение).

Пусть $K_1, K_2, \dots, K_s$ — кольца. Рассмотрим декартово произведение этих колец:

$$K_1 \times K_2 \times \dots \times K_s = \{(a_1, a_2, \dots, a_s) : a_i \in K_i \ (i = 1, 2, \dots, s)\}$$

и введем покомпонентные операции сложения и умножения:

$$(a_1, a_2, \dots, a_s) + (b_1, b_2, \dots, b_s) = (a_1 + b_1, a_2 + b_2, \dots, a_s + b_s),$$

$$(a_1, a_2, \dots, a_s) \cdot (b_1, b_2, \dots, b_s) = (a_1 b_1, a_2 b_2, \dots, a_s b_s).$$

Очевидно, что с такими операциями $K_1 \times K_2 \times \dots \times K_s$ является кольцом.

Теорема 18.16 (Китайская теорема об остатках). Пусть $m_1, m_2, \dots, m_s$ — попарно взаимно простые натуральные числа, т. е. $\text{НОД}(m_i, m_j) = 1$ при $i \neq j$. Тогда для любых целых $r_1, r_2, \dots, r_s$, где $0 \leq r_i \leq m_i - 1$ ($i = 1, 2, \dots, s$), существует, причем единственный, целый x , такой, что

$$x \equiv r_i \pmod{m_i} \quad (i = 1, 2, \dots, s), \quad 0 \leq x \leq M - 1,$$

где $m = m_1 m_2 \dots m_s$.

Доказательство. Мы докажем, что кольца $\mathbb{Z}_m$ и $\mathbb{Z}_1 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_s$ изоморфны. Для этого рассмотрим отображение $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_1 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_s$, определяемое формулой

$$\varphi x = (x \bmod m_1, x \bmod m_2, \dots, x \bmod m_s).$$

Легко видеть, что это отображение — гомоморфизм.

Найдем его ядро:

$$\varphi x = (0, 0, \dots, 0) \Leftrightarrow x \bmod m_i = 0 \quad (i = 1, 2, \dots, s).$$

Так как $m_1, m_2, \dots, m_s$ — попарно взаимно простые, то последнее условие эквивалентно тому, что $x \bmod m = 0$. Таким образом, $\text{Ker } \varphi = m\mathbb{Z}$.

Теперь докажем, что гомоморфизм φ является сюръективным. Для этого для произвольных целых $r_1, r_2, \dots, r_s$, где $0 \leq r_i \leq m_i - 1$, построим x , такой, что $\varphi x = (r_1, r_2, \dots, r_s)$. Вначале найдем $\alpha_1, \alpha_2, \dots, \alpha_s$, такие, что

$$\alpha_j \equiv 1 \pmod{m_j}, \quad \alpha_j \equiv 0 \pmod{m_i} \quad (i \neq j).$$

Такие $\alpha_1, \alpha_2, \dots, \alpha_s$ всегда существуют. Например, можно положить

$$\alpha_j = (m_1 \dots m_{j-1} m_{j+1} \dots m_s)^{\phi(m_j)} \quad (j = 1, 2, \dots, s),$$

где $\phi(m_j)$ — функция Эйлера. Теперь легко проверить, что $x = \alpha_1 r_1 + \alpha_2 r_2 + \dots + \alpha_s r_s$ удовлетворяет нужным свойствам.

Изоморфизм $\mathbb{Z}_1 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_s \cong \mathbb{Z}_m$ следует теперь из утверждения 18.14. ■

Пример 18.17. Для $m_1 = 5$, $m_2 = 4$, $m_3 = 3$ можно взять $\alpha_1 = 36$, $\alpha_2 = 45$, $\alpha_3 = 40$. Если $r_1 = 4$, $r_2 = 3$, $r_3 = 1$ получаем

$$x \equiv \alpha_1 r_1 + \alpha_2 r_2 + \alpha_3 r_3 = 36 \times 4 + 45 \times 3 + 40 \times 1 = 319 \equiv 19 \pmod{60}.$$

Итак, $x = 19$.

18.7. Расширения полей

Пусть F и $\overline{F}$ — два поля с одними и теми же операциями, причем $F \subseteq \overline{F}$, тогда F называется *подполем* поля $\overline{F}$, а $\overline{F}$ называется *надполем* поля F или *расширением* поля F . Легко видеть, что $\overline{F}$ является линейной алгеброй над F . Если эта линейная алгебра конечномерная, то расширение называется *конечным*, при этом размерность $\dim_F \overline{F}$ называется *степенью* расширения.

Например, рассмотрим фактор-кольцо $\overline{F} = F \subseteq F[x]/(f)$, где f — неприводимый над F многочлен. Так как f — неприводимый, то $\overline{F}$ — поле. Отождествляя элементы из F и соответствующие им смежные классы можно считать, что $F \subseteq \overline{F}$.

Теорема 18.18. Пусть $f(x) \in F[x]$ и $\deg f > 0$. Тогда существует такое расширение $\overline{F} \supseteq F$, в котором $f(x)$ содержит корень.

Доказательство. Пусть $p(x)$ — неприводимый множитель многочлена $f(x)$. Рассмотрим поле $\overline{F} = F \subseteq F[x]/(p)$. Легко видеть, что $\overline{x} = x + (p) \in \overline{F}$ является корнем многочлена f . ■

Пусть $\overline{F}$ — расширение поля F . Тогда $\overline{F}$ называется *полем разложения* многочлена $f \in F[x]$, если f в этом поле раскладывается на линейные множители.

Утверждение 18.19. Для любого многочлена $f \in F[x]$ существует его поле разложения.

Доказательство. Индукция по степени многочлена f . ■

Пусть, как и выше, $\overline{F}$ — расширение поля F . Элемент $\alpha \in \overline{F}$ называется *алгебраическим* над F , если существует ненулевой многочлен $f \in F[x]$, такой, что $f(\alpha) = 0$, при этом f называется многочленом, *аннулирующим* элемент α . Если аннулирующего многочлена нет, то α называется *трансцендентным* над F .

Теорема 18.20. *Если расширение $\overline{F}$ поля F конечное, то любой элемент в расширении — алгебраический.*

Доказательство. Пусть $\alpha \in \overline{F}$, $\dim_F \overline{F} = n$. Рассмотрим элементы $1, \alpha, \alpha^2, \dots, \alpha^n$. Они (как и любые $n+1$ элементов в $\overline{F}$) будут линейно зависимыми над F , т. е. найдутся такие $\lambda_0, \lambda_1, \dots, \lambda_n$ из F , что

$$\lambda_0 + \lambda_1 \alpha + \dots + \lambda_n \alpha^n = 0,$$

откуда следует, что многочлен $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ — аннулирующий для α . ■

Легко проверить, что множество всех многочленов, аннулирующих заданный элемент α , является идеалом в $F[x]$. Но в $F[x]$ любой идеал является главным. Многочлен, порождающий этот идеал, называется *минимальным* аннулирующим многочленом для α .

Утверждение 18.21. *Если α — алгебраический элемент над F , то его минимальный аннулирующий многочлен неприводим над F .*

Доказательство. Пусть f — минимальный аннулирующий многочлен для α . Предположим, что f приводим, т. е. $f = gh$, причем $\deg g < \deg f$ и $\deg h < \deg f$. Тогда $f(\alpha) = g(\alpha)h(\alpha) = 0$, откуда (так как в поле нет делителей нуля) $g(\alpha) = 0$ или $h(\alpha) = 0$. В любом случае нашли аннулирующий многочлен степени, меньшей $\deg f$, что невозможно. ■

Пусть p — минимальный аннулирующий многочлен для $\alpha \in \overline{F}$. Рассмотрим отображение $\varphi : F[x] \rightarrow \overline{F}$, определяемое формулой $\varphi(g(x)) = g(\alpha)$. В частности, $\varphi(x) = \alpha$. Тогда из утверждения 18.14 следует, что

$$F[x]/\text{Ker } \varphi \cong \text{Im } \varphi,$$

где $\text{Ker } \varphi = (p)$. Но $F[x]/(p) = \{g(x + (p)) : \deg g < \deg p\}$, откуда $\text{Im } \varphi$ есть множество многочленов от α степени меньше $\deg p$.

Обозначим $F[\alpha] = \text{Im } \varphi$ — минимальное поле, полученное присоединением к F элемента α . Итак,

$$F[\alpha] \cong F[x]/(p).$$

Утверждение 18.22. *Пусть F_1, F_2 — два расширения поля F , причем $\alpha_1 \in F_1, \alpha_2 \in F_2$ и минимальные многочлены для α_1 и α_2 совпадают. Тогда $F[\alpha_1] \cong F[\alpha_2]$.*

Доказательство. Имеем $F[\alpha_1] \cong F[x]/(p) \cong F[\alpha_2]$. ■

18.8. Конечные поля

В данном разделе мы дадим полную классификацию конечных полей, которые называются *полями Галуа*.

Пусть F — конечное поле характеристики $\chi(F) = p$. Напомним, что p — простое число и $(1) \cong \mathbb{Z}_p$. Отождествляя соответствующие элементы в (1) и $\mathbb{Z}_p$ можно считать, что $\mathbb{Z}_p \subseteq F$. Значит F является конечным расширением поля $\mathbb{Z}_p$. Обозначим $n = \dim_{\mathbb{Z}_p} F$. Таким образом, F как линейное пространство изоморфно арифметическому пространству $\mathbb{Z}_p^n$. В частности, отсюда получаем, что $|F| = p^n$.

Мы доказали важный результат о строении полей.

Теорема 18.23. Любое конечное поле F имеет порядок p^n , где $p = \chi(F)$ — простое число, а n — натуральное.

Мультипликативная группа поля F^* имеет порядок $p^n - 1$. По теореме Лагранжа для любого $a \in F^*$ имеем $a^{p^n-1} = 1$. Умножая обе части этого равенства на a , получаем $a^{p^n} = a$, что, очевидно, верно и для $a=0$. Таким образом, корнем многочлена $f = x^{p^n} - x$ является каждый элемент $a \in F$. Обратим внимание, что $f \in \mathbb{Z}_p[x]$. Получаем интересное следствие.

Следствие 18.24. Конечное поле F является полем разложения многочлена $f = x^{p^n} - x$, где $p = \chi(F)$ — простое число, а n — натуральное.

Теорема 18.23 уже содержит много информации о строении конечных полей. Следующие две теоремы дают их полную классификацию.

Теорема 18.25. Для любого простого p и любого натурального n существует поле из p^n элементов.

Доказательство. Рассмотрим поле $\overline{F}$ разложения многочлена $f = x^{p^n} - x \in \mathbb{Z}_p[x]$. Так как $f' = -1$, $\text{НОД}(f, f') = 1$, то f не имеет кратных корней. Рассмотрим множество $F = \{\alpha_1, \alpha_2, \dots, \alpha_{p^n}\} \subseteq \overline{F}$ всех его корней. Оно образует подполе в $\overline{F}$. Действительно, для любых x, y из F

$$(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n} = x + y, \quad (xy)^{p^n} = x^{p^n} y^{p^n} = xy, \quad (x^{-1})^{p^n} = (x^{p^n})^{-1} = x^{-1}.$$

$\overline{F}$ содержит p^n элементов. ■

Теорема 18.26. Конечные поля одного порядка изоморфны между собой.

Доказательство. Пусть F_1, F_2 — два конечных поля и $|F_1| = |F_2| = p^n$. Каждое из этих полей по следствию 18.24 является полем разложения многочлена $f = x^{p^n} - x \in \mathbb{Z}_p[x]$. Пусть α — корень этого многочлена в поле F_1 , такой, что $F_1 = \mathbb{Z}_{p^n}[\alpha]$, а β — корень этого многочлена в поле F_2 , такой, что $F_2 = \mathbb{Z}_{p^n}[\beta]$. Так как α и β являются корнями некоторого неприводимого множителя многочлена f , то, согласно утверждению 18.22, $F_1 \cong F_2$. ■

Конечное поле из p^n элементов обозначается $GF(p^n)$.

Глава 19

Матрицы над евклидовым кольцом

19.1. Нормальная диагональная форма

В данной главе везде предполагается, что K — некоторое евклидово кольцо. Рассмотрим кольцо $K^{m \times n}$ матриц размера $m \times n$ с элементами из K . Везде далее мы будем обращаться к двум важным примерам таких колец:

1. Кольцо $F[\lambda]^{m \times n}$, где F — некоторое поле. Элементы этого кольца называются *многочленными матрицами*, или *λ -матрицами* над полем F .
2. Кольцо $\mathbb{Z}^{m \times n}$ целочисленных матриц.

Элементарными преобразованиями таких матриц назовем преобразования следующих типов:

1. перестановка i -й и j -й строк;
2. умножение i -й строки на обратимый элемент из K (т. е. для кольца λ -матриц возможно умножение на ненулевой скаляр, для кольца целочисленных матриц — умножение на ± 1);
3. прибавление к i -й строке j -й строки, умноженной на произвольный элемент из K ,

и аналогичные преобразования столбцов.

Будем говорить, что матрица $A \in K^{m \times n}$ эквивалентна матрице $B \in K^{m \times n}$ и писать $A \sim B$, если от A к B можно перейти при помощи цепочки элементарных преобразований. Легко видеть, что отношение эквивалентности обладает тремя основными свойствами: рефлексивностью, симметричностью и транзитивностью. Отсюда следует, что множество всех матриц из $K^{m \times n}$ разбивается на непересекающиеся классы эквивалентных матриц. Возникает вопрос о канонической матрице, характеризующей данный класс.

Канонической или *нормальной диагональной* матрицей называется матрица $\text{diag}(d_1, \dots, d_r, d_{r+1}, \dots, d_p)$ из $K^{m \times n}$, где $p = \min\{m, n\}$, в которой $d_j \mid d_{j-1}$ ($j = 2, 3, \dots, r$), $d_j = 0$ ($j = r + 1, \dots, p$).

Теорема 19.1. *Для любой матрицы $A \in K^{m \times n}$ существует эквивалентная ей нормальная диагональная матрица D , называемая канонической или нормальной диагональной формой матрицы A . Диагональные элементы нормальной диагональной формы, называемые инвариантами множителями, определяются единственным образом с точностью до умножения на обратимые элементы из K .*

Пример 19.2. Найдем нормальную диагональную форму λ -матрицы

$$\begin{pmatrix} -\lambda + 1 & 2\lambda^3 - \lambda^2 - 2\lambda - 1 & \lambda^3 + 2\lambda + 3 & -\lambda - 1 \\ -2\lambda + 5 & -2\lambda^2 + 8\lambda + 3 & -2\lambda - 2 & \lambda + 1 \\ -2\lambda^2 + 5\lambda + 1 & -2\lambda^3 + 8\lambda^2 + 4\lambda & -2\lambda^2 - 2\lambda & \lambda^2 + \lambda \\ \lambda - 1 & -2\lambda^3 + \lambda^2 + 5\lambda + 4 & -\lambda^3 - 4\lambda - 5 & 2\lambda + 2 \end{pmatrix}$$

над полем комплексных чисел (или любым другим числовым полем). Из третьей строки вычтем вторую, умноженную на λ , и полученную строку переставим с первой:

$$\begin{pmatrix} 1 & \lambda & 0 & 0 \\ -2\lambda + 5 & -2\lambda^2 + 8\lambda + 3 & -2\lambda - 2 & \lambda + 1 \\ -\lambda + 1 & 2\lambda^3 - \lambda^2 - 2\lambda - 1 & \lambda^3 + 2\lambda + 3 & -\lambda - 1 \\ \lambda - 1 & -2\lambda^3 + \lambda^2 + 5\lambda + 4 & -\lambda^3 - 4\lambda - 5 & 2\lambda + 2 \end{pmatrix}.$$

Из второй, третьей и четвертой строки вычитаем первую, умноженную на $-2\lambda+5$, $-\lambda+1$ и $\lambda-1$ соответственно. Далее полученный первый столбец, умноженный на λ , вычитаем из четвертого столбца:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3\lambda + 3 & -2\lambda - 2 & \lambda + 1 \\ 0 & 2\lambda^3 - 3\lambda - 1 & \lambda^3 + 2\lambda + 3 & -\lambda - 1 \\ 0 & -2\lambda^3 + 6\lambda + 4 & -\lambda^3 - 4\lambda - 5 & 2\lambda + 2 \end{pmatrix}.$$

Переставляем второй и четвертый столбцы. К третьей строке прибавляем вторую. Из четвертой вычитаем вторую, умноженную на 2. После этого к третьему столбцу прибавим второй, умноженный на 2, и из четвертого вычтем второй, умноженный на 3:

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

К четвертой строке прибавляем третью. Далее из четвертого столбца вычитаем третий, умноженный на 2:

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

Это нормальная диагональная матрица.

Пример 19.3. Найдем нормальную диагональную форму целочисленной матрицы

$$\begin{pmatrix} 84 & 24 & -72 & -72 & 72 \\ -28 & 8 & 60 & 60 & -76 \\ 488 & 224 & -240 & -240 & 164 \end{pmatrix}.$$

Из первого столбца вычтем второй, умноженный на 2. Из четвертого столбца вычтем третий. К пятому столбцу прибавим третий. Получим:

$$\begin{pmatrix} 36 & 24 & -72 & 0 & 0 \\ -44 & 8 & 60 & 0 & -16 \\ 40 & 224 & -240 & 0 & -76 \end{pmatrix}.$$

Из первой и третьей строк вычтем вторую, умноженную на 3 и 28 соответственно. Из первого, третьего и пятого столбцов вычтем второй, умноженный на -5 , 7 и -2 соответственно. Получим:

$$\begin{pmatrix} 168 & 0 & -252 & 0 & 48 \\ -4 & 8 & 4 & 0 & 0 \\ 1272 & 0 & -1920 & 0 & 372 \end{pmatrix}.$$

К первой и третьей строкам прибавим вторую, умноженную на 63 и 480 соответственно. Прибавим к первому столбцу третий. Из второго отнимем третий, умноженный на 2. После этого надлежащим образом переставим строки и столбцы:

$$\begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 504 & -84 & 48 & 0 \\ 0 & 3840 & -648 & 372 & 0 \end{pmatrix}.$$

Из третьей строки вычтем вторую, умноженную на 7. Из второго столбца вычтем четвертый, умноженный на 10. К третьему столбцу прибавим четвертый, умноженный на 2. Получим:

$$\begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 24 & 12 & 48 & 0 \\ 0 & -48 & 12 & 36 & 0 \end{pmatrix}.$$

Из третьей строки вычтем вторую. Из второго и четвертого столбцов вычтем третий, умноженный на 2 и 4 соответственно. Получим:

$$\begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 12 & 0 & 0 \\ 0 & -72 & 0 & -12 & 0 \end{pmatrix}.$$

Вычтем из второго столбца четвертый, умноженный на 6. Далее умножим третью строку (или четвертый столбец) на -1 и после надлежащей перестановки столбцов получим нормальную диагональную матрицу:

$$\begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 & 0 \\ 0 & 0 & 12 & 0 & 0 \end{pmatrix}.$$

На матрицы из $K^{m \times n}$ можно распространить понятие минора и ранга. При элементарных преобразованиях ранг матрицы не изменяется.

Наибольший общий делитель всех миноров k -го порядка матрицы $A \in K^{m \times n}$ обозначим Δ_k ($k = 1, 2, \dots, \min\{m, n\}$).

Утверждение 19.4. При элементарных преобразованиях матрицы величины Δ_k не изменяются.

Утверждение 19.5. Для инвариантных множителей d_j матрицы A справедливы формулы:

$$d_j = \begin{cases} \Delta_1 & \text{при } j = 1, \\ \frac{\Delta_j}{\Delta_{j-1}} & \text{при } j = 2, \dots, r, \\ 0 & \text{при } j = r + 1, \dots, \min\{m, n\}, \end{cases}$$

где r — ранг матрицы A .

Пример 19.6.

$$\begin{pmatrix} \lambda + 4 & -3 & -3 \\ 0 & \lambda - 2 & 0 \\ 6 & -3 & \lambda - 5 \end{pmatrix}.$$

Так как матрица содержит ненулевые константы, то $\Delta_1 = 1$. Все миноры второго порядка, содержащие вторую строку делятся на $\lambda - 2$. Вычислим остальные миноры второго порядка:

$$\begin{vmatrix} \lambda + 4 & -3 \\ 6 & -3 \end{vmatrix} = -3\lambda + 6, \quad \begin{vmatrix} \lambda + 4 & -3 \\ 6 & \lambda - 5 \end{vmatrix} = \lambda^2 - \lambda - 2 = (\lambda + 1)(\lambda - 2),$$

$$\begin{vmatrix} -3 & -3 \\ -3 & \lambda - 5 \end{vmatrix} = -3\lambda + 6.$$

Получаем $\Delta_2 = \lambda - 2$. Разлагая определитель исходной матрицы по второй строке, находим $\Delta_3 = (\lambda + 1)(\lambda - 2)^2$. Таким образом, инвариантные множители равны

$$d_1 = \Delta_1 = 1, \quad d_2 = \frac{\Delta_2}{\Delta_1} = \lambda - 2, \quad d_3 = \frac{\Delta_3}{\Delta_2} = (\lambda + 1)(\lambda - 2).$$

Нормальная диагональная форма имеет вид

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda - 2 & 0 \\ 0 & 0 & (\lambda + 1)(\lambda - 2) \end{pmatrix}.$$

Пример 19.7. Найдём нормальную диагональную форму целочисленной матрицы

$$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 2 \\ -1 & 5 & 8 \end{pmatrix}$$

Имеем $\Delta_1 = 1$. Легко видеть, что каждый минор второго порядка, содержащий вторую строку или третий столбец, делится на 2. Отстаётся единственный минор второго порядка:

$$\begin{vmatrix} 1 & 1 \\ -1 & 5 \end{vmatrix} = 6,$$

поэтому $\Delta_2 = 2$. Вычисляем определитель всей матрицы:

$$\begin{vmatrix} 1 & 1 & 2 \\ 0 & 2 & 2 \\ -1 & 5 & 8 \end{vmatrix} = 8,$$

откуда $\Delta_3 = 8$. Получаем

$$d_1 = \Delta_1 = 1, \quad d_2 = \frac{\Delta_2}{\Delta_1} = 2, \quad d_3 = \frac{\Delta_3}{\Delta_2} = 4.$$

Нормальная диагональная форма имеет вид

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Следствие 19.8. Матрицы A и B из $K^{m \times n}$ эквивалентны тогда и только тогда, когда их нормальные диагональные формы совпадают (с точностью до умножения диагональных элементов на обратимые элементы из K).

Матрица $P \in K^{n \times n}$ называется *унимодулярной*, если в $K^{n \times n}$ существует обратная к ней матрица.

Утверждение 19.9. Пусть $P \in K^{n \times n}$. Для того, чтобы P была унимодулярной необходимо и достаточно, чтобы $\det P \in K$ и $\det P \neq 0$.

Теорема 19.10. Для того, чтобы матрицы A и B из $K^{m \times n}$ были эквивалентны необходимо и достаточно, чтобы существовали унимодулярные матрицы P из $K^{m \times m}$ и Q из $K^{n \times n}$, такие, что $B = PAQ$.

Для нахождения унимодулярных матриц P и Q , таких, что $B = PAQ$ достаточно приписать снизу и справа от матрицы A по единичной матрице (соответствующего порядка) и элементарными преобразованиями привести A к B , при этом все преобразования со строками производить также с единичной матрицей, приписанной справа, а преобразования со столбцами — с единичной матрицей, приписанной снизу. Чаще удобнее приводить матрицу A не к виду B , а каждую из матриц A, B привести к нормальной диагональной форме D . Если $D = P_1 A Q_1 = P_2 A Q_2$, где P_1, P_2, Q_1, Q_2 — унимодулярные матрицы, то $B = (P_2^{-1} P_1) A (Q_1 Q_2^{-1})$, причем матрицы $P_2^{-1} P_1, Q_1 Q_2^{-1}$ — унимодулярные.

Пример 19.11. Приведем λ -матрицу

$$A = \begin{pmatrix} \lambda & \lambda + 1 \\ 0 & \lambda \end{pmatrix}$$

к нормальной диагональной форме и найдем P, Q , такие, что $D = PAQ$.

Выпишем матрицу

$$\left(\begin{array}{cc|cc} \lambda & \lambda + 1 & 1 & 0 \\ 0 & \lambda & 0 & 1 \\ \hline 1 & 0 & & \\ 0 & 1 & & \end{array} \right).$$

Из ее второго столбца вычтем первый:

$$\left(\begin{array}{cc|cc} \lambda & 1 & 1 & 0 \\ 0 & \lambda & 0 & 1 \\ \hline 1 & -1 & & \\ 0 & 1 & & \end{array} \right).$$

Теперь вычтем из первого столбца второй, умноженный на λ , и вычтем из второй строки первую, умноженную на λ . Получим:

$$\left(\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ -\lambda^2 & 0 & -\lambda & 1 \\ \hline \lambda + 1 & -1 & & \\ -\lambda & 1 & & \end{array} \right).$$

Умножаем первый столбец на -1 и переставляем его со вторым:

$$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & \lambda^2 & -\lambda & 1 \\ \hline -1 & -\lambda - 1 & & \\ 1 & \lambda & & \end{array} \right).$$

Мы нашли

$$A = \begin{pmatrix} 1 & 0 \\ 0 & \lambda^2 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} -1 & -\lambda - 1 \\ 1 & \lambda \end{pmatrix}.$$

Матрицы P и Q определяются не однозначно.

19.2. Связь подобия числовых матриц с эквивалентностью λ -матриц

В данном разделе рассматриваются только λ -матрицы, т. е. элементы кольца $F[\lambda]^{m \times n}$, где F — поле.

Заметим, что кольцо $F[\lambda]^{m \times n}$ *многочленных матриц* (λ -матриц), изоморфно кольцу $F^{m \times n}[\lambda]$ *матричных многочленов*, т. е. многочленов, коэффициентами которых являются матрицы из $F^{m \times n}$. *Естественный изоморфизм* задается простым правилом, которое мы покажем на примере.

Пример 19.12. Многочленной матрице

$$\begin{pmatrix} \lambda^2 + 2\lambda - 2 & -\lambda^2 + 5\lambda - 1 & \lambda^2 + 3\lambda + 2 \\ -\lambda^2 + 3\lambda + 1 & 2\lambda^2 - 2\lambda + 5 & 3\lambda^2 + 5\lambda + 2 \\ \lambda^2 - 2\lambda - 1 & \lambda^2 - 4\lambda - 3 & 2\lambda^2 - 2\lambda - 1 \end{pmatrix}$$

соответствует матричный многочлен

$$\begin{pmatrix} 1 & -1 & 1 \\ -1 & 2 & 3 \\ 1 & 1 & 2 \end{pmatrix} \cdot \lambda^2 + \begin{pmatrix} 2 & 5 & 3 \\ 3 & -2 & 5 \\ -2 & -4 & -2 \end{pmatrix} \cdot \lambda + \begin{pmatrix} -2 & -1 & 2 \\ 1 & 5 & 2 \\ -1 & -3 & -1 \end{pmatrix}.$$

Естественный изоморфизм из $F[\lambda]^{m \times n}$ в $F^{m \times n}[\lambda]$ позволяет нам отождествлять λ -матрицы и соответствующие ей матричные многочлены.

Пусть A — матрица из $F^{n \times n}$, тогда $A - \lambda E$ называется ее *характеристической матрицей*.

Теорема 19.13. Пусть A, B — матрицы из $F^{n \times n}$. Для того, чтобы A и B были подобны необходимо и достаточно, чтобы их характеристические матрицы $A - \lambda E$ и $B - \lambda E$ были эквивалентны.

Более того, если $B - \lambda E = P(A - \lambda E)Q$, где P, Q — унимодулярные λ -матрицы, то $B = LAR$ и $L = R^{-1}$, где L — остаток от деления P на $B - \lambda E$ слева, а R — остаток от деления Q на $B - \lambda E$ справа. Таким образом, R — трансформирующая матрица.

Утверждение 19.14. Имеет место эквивалентность

$$J_n(\lambda_0) - \lambda E = \begin{pmatrix} \lambda_0 - \lambda & 1 & \dots & 0 & 0 \\ 0 & \lambda_0 - \lambda & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_0 - \lambda & 1 \\ 0 & 0 & \dots & 0 & \lambda_0 - \lambda \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & (\lambda - \lambda_0)^n \end{pmatrix}$$

Таким образом, все инвариантные множители характеристической матрицы жордановой клетки равны 1, кроме последнего, равного $(\lambda - \lambda_0)^n$.

Утверждение 19.15. Если многочлены $f_1(\lambda), f_2(\lambda), \dots, f_n(\lambda)$ из $F[\lambda]$ попарно взаимно просты, то

$$\begin{pmatrix} f_1(\lambda) & 0 & \dots & 0 \\ 0 & f_2(\lambda) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & f_n(\lambda) \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & f_1(\lambda) \dots f_n(\lambda) \end{pmatrix}.$$

Утверждение 19.16. Пусть $J = \text{diag}(J_{k_1}(\lambda_1), J_{k_2}(\lambda_2), \dots, J_{k_s}(\lambda_s))$, тогда

$$J - \lambda E \sim \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & 1 & & \\ & & & & (\lambda - \lambda_1)^{k_1} & \\ & & & & & (\lambda - \lambda_2)^{k_2} \\ & & & & & & \ddots \\ & & & & & & & (\lambda - \lambda_s)^{k_s} \end{pmatrix}$$

Матрица из предыдущего утверждения хотя и диагональна, но в общем случае не является нормальной диагональной.

Рассмотрим теперь матрицу $J - \lambda E = \text{diag}(J_1 - \lambda E, J_2 - \lambda E, \dots, J_s - \lambda E)$, где $J_1, \dots, J_s$ — жордановы клетки. Пусть $\lambda_1, \dots, \lambda_s$ — все собственные значения матрицы J , причем $\lambda_i \neq \lambda_j$ при $i \neq j$. Пусть к собственному числу λ_i относится q_i жордановых клеток и пусть порядки этих клеток, расположенные в неубывающем порядке, суть $k_{i1} \leq k_{i2} \leq \dots \leq k_{iq_i}$. Обозначим

$$e_{n-j+1}(\lambda) = \prod_{i=1}^k (\lambda - \lambda_i)^{k_{ij}} \quad (j = 1, 2, \dots, n),$$

полагая, что если для некоторого $q_i < j$, то соответствующий множитель $(\lambda - \lambda_i)^{k_{ij}}$ равен 1.

Утверждение 19.17. $J - \lambda E \sim \text{diag}(e_1(\lambda_1), \dots, e_n(\lambda_n))$, причем матрица, стоящая справа, имеет нормальный диагональный вид.

Пример 19.18. Пусть

$$J = \begin{pmatrix} 2 & & & & & \\ & 2 & & & & \\ & & 2 & 1 & 0 & \\ & & 0 & 2 & 1 & \\ & & 0 & 0 & 2 & \\ & & & & & 3 & 1 \\ & & & & & 0 & 3 \\ & & & & & & & 3 & 1 \\ & & & & & & & 0 & 3 \end{pmatrix}.$$

Тогда

$$\begin{aligned} J - \lambda E &\sim \text{diag}(1, 1, 1, 1, \lambda - 2, \lambda - 2, (\lambda - 2)^3, (\lambda - 3)^2, (\lambda - 3)^2) \sim \\ &\sim \text{diag}(1, 1, 1, 1, 1, 1, \lambda - 2, (\lambda - 2)(\lambda - 3)^2, (\lambda - 2)^3(\lambda - 3)^2). \end{aligned}$$

Последняя матрица является нормальной диагональной формой матрицы J .

Пусть

$$d_i = e_{i1}(\lambda)e_{i2}(\lambda) \dots e_{ip_i}(\lambda) \quad (i = 1, 2, \dots, n)$$

— разложение i -го инвариантного множителя на неприводимые над полем F множители, причем $e_{ij} \neq e_{ik}$ при $j \neq k$. Система

$$e_{ij}(\lambda) \quad (i = 1, 2, \dots, n; j = 1, 2, \dots, p_i)$$

называется системой элементарных делителей матрицы.

Теорема 19.19. Матрица A из $F^{n \times n}$ тогда и только тогда подобна жордановой матрице, когда система элементарных делителей матрицы $A - \lambda E$ состоит только из линейных многочленов

$$(\lambda - \lambda_i)^{t_j} \quad (i = 1, 2, \dots, n; j = 1, 2, \dots, p_i).$$

В этом случае жорданова матрица составлена из жордановых клеток, которые по элементарным делителям можно найти следующим образом. Каждому элементарному делителю $(\lambda - \lambda_i)^{t_j}$ соответствует клетка t_j -го порядка с λ_j на диагонали. Жорданова форма определяется единственным с точностью до перестановки жордановых клеток образом.

Следствие 19.20. Любая матрица над алгебраически замкнутым полем (в частности, над полем комплексных чисел) подобна жордановой.

Пример 19.21. Найдём жорданову форму и соответствующую трансформирующую матрицу для матрицы

$$A = \begin{pmatrix} 2 & 17 & -68 \\ 0 & -2 & 16 \\ 0 & -1 & 6 \end{pmatrix}.$$

Составляем матрицу $A - \lambda E$ и приписываем к ней снизу единичную:

$$A - \lambda E = \left(\begin{array}{ccc|ccc} 2 - \lambda & 17 & -68 & & & \\ 0 & -2 - \lambda & 16 & & & \\ 0 & -1 & 6 - \lambda & & & \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array} \right)$$

С помощью преобразований строк и столбцов матрицу $A - \lambda E$ приведём к нормальной диагональной форме. Все преобразования со столбцами будем проделывать так же с матрицей, стоящей снизу. Умножим второй столбец на -1 . Далее вычтем этот столбец, умноженный на $6 - \lambda$, из третьего столбца:

$$\left(\begin{array}{ccc|ccc} 2 - \lambda & -17 & 34 - 17\lambda & & & \\ 0 & 2 + \lambda & (\lambda - 2)^2 & & & \\ 0 & 1 & 0 & & & \\ \hline 1 & 0 & 0 & & & \\ 0 & -1 & 6 - \lambda & & & \\ 0 & 0 & 1 & & & \end{array} \right)$$

Прибавляем третью строку, умноженную на 17, к первой. Вычитаем третью строку, умноженную на $\lambda + 2$, из второй. В результате получим:

$$\left(\begin{array}{ccc|ccc} 2-\lambda & 0 & 34-17\lambda & & & \\ 0 & 0 & (\lambda-2)^2 & & & \\ 0 & 1 & 0 & & & \\ \hline 1 & 0 & 0 & & & \\ 0 & -1 & 6-\lambda & & & \\ 0 & 0 & 1 & & & \end{array} \right)$$

Переставляя строки и столбцы надлежащим образом, получим:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 0 & 2-\lambda & 34-17\lambda & & & \\ 0 & 0 & (\lambda-2)^2 & & & \\ \hline 0 & 1 & 0 & & & \\ -1 & 0 & 6-\lambda & & & \\ 0 & 0 & 1 & & & \end{array} \right)$$

Вычитаем из третьего столбца второй, умноженный на 17:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 0 & 2-\lambda & 0 & & & \\ 0 & 0 & (\lambda-2)^2 & & & \\ \hline 0 & 1 & -17 & & & \\ -1 & 0 & 6-\lambda & & & \\ 0 & 0 & 1 & & & \end{array} \right)$$

Меняем знак у второго столбца:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 0 & \lambda-2 & 0 & & & \\ 0 & 0 & (\lambda-2)^2 & & & \\ \hline 0 & -1 & -17 & & & \\ -1 & 0 & 6-\lambda & & & \\ 0 & 0 & 1 & & & \end{array} \right)$$

Матрица $A - \lambda E$ приведена к нормальной диагональной форме. Элементарными делителями являются $\lambda - 2$ и $(\lambda - 2)^2$, поэтому A подобна жордановой матрице

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Чтобы найти трансформирующую матрицу Q (т.е. матрицу, для которой $J = Q^{-1}AQ$) элементарными преобразованиями приведем $J - \lambda E$ к нормальной диагональной форме. Составляем матрицу

$$\left(\begin{array}{ccc|ccc} 2-\lambda & 0 & 0 & & & \\ 0 & 2-\lambda & 1 & & & \\ 0 & 0 & 2-\lambda & & & \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array} \right)$$

Вычитаем из второго столбца третий, умноженный на $2 - \lambda$:

$$\left(\begin{array}{ccc} 2 - \lambda & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -(2 - \lambda)^2 & 2 - \lambda \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda - 2 & 1 \end{array} \right)$$

Вычитаем из третьей строки вторую, умноженную на $2 - \lambda$:

$$\left(\begin{array}{ccc} 2 - \lambda & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -(2 - \lambda)^2 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda - 2 & 1 \end{array} \right)$$

Преставляя строки и столбцы надлежащим образом, получаем:

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & \lambda - 2 & 0 \\ 0 & 0 & (2 - \lambda)^2 \\ \hline 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 2 - \lambda \end{array} \right)$$

Итак,

$$Q_1(\lambda) = \begin{pmatrix} 0 & -1 & -17 \\ -1 & 0 & 6 - \lambda \\ 0 & 0 & 1 \end{pmatrix}, \quad Q_2(\lambda) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 2 - \lambda \end{pmatrix}.$$

Вычислим

$$Q_0(\lambda) = Q_1(\lambda)Q_2(\lambda)^{-1} = \begin{pmatrix} 1 & 17 & 0 \\ 0 & 2\lambda - 8 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Найдем остаток Q при делении $Q_0(\lambda)$ на $J - \lambda E$ справа:

$$Q = Q_0(J) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot J + \begin{pmatrix} 1 & 17 & 0 \\ 0 & -8 & -1 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 17 & 0 \\ 0 & -4 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Матрица Q и есть искомая трансформирующая матрица и $J = Q^{-1}AQ$.

Матрицей *естественной формы*, или матрицей, имеющей *нормальную естественную форму*, называется клеточно-диагональная матрица $B = \text{diag}(B_1, B_2, \dots, B_s) \in F^{n \times n}$, где $B_1, \dots, B_s$ являются матрицами, сопровождающими многочлены $f_1(\lambda), \dots, f_s(\lambda)$ соответственно, причем $f_i(\lambda) \nmid f_{i-1}(\lambda)$ ($i = 2, 3, \dots, s$).

Утверждение 19.22. Первые $n - s$ инвариантных множителя матрицы естественной формы являются 1. Остальные инвариантные множители равны $f_1(\lambda), \dots, f_s(\lambda)$.

Теорема 19.23. Любая матрица A из $F^{n \times n}$ подобна над F единственной матрице B естественной формы, называемой нормальной естественной формой матрицы A , причем $B = \text{diag}(B_1, B_2, \dots, B_s) \in F^{n \times n}$, где $B_1, \dots, B_s$ — матрицы, сопровождающие инвариантные множители $f_1(\lambda), \dots, f_s(\lambda)$ матрицы. Две матрицы из $F^{n \times n}$ подобны над F тогда и только тогда, когда их естественные формы совпадают.

Квазиестественной матрицей называется клеточно-диагональная матрица $B = \text{diag}(B_1, B_2, \dots, B_s) \in F^{n \times n}$, где $B_1, \dots, B_s$ являются матрицами, сопровождающими многочлены вида

$$(f_1(\lambda))^{k_1}, (f_2(\lambda))^{k_2}, \dots, (f_s(\lambda))^{k_s},$$

где $f_1(\lambda), \dots, f_s(\lambda)$ неприводимы над полем F и имеют старшие коэффициенты, равные единице.

Утверждение 19.24. Элементарные делители квазиестественной матрицы являются $(f_1(\lambda))^{k_1}, (f_2(\lambda))^{k_2}, \dots, (f_s(\lambda))^{k_s}$.

Теорема 19.25. Любая матрица A из $F^{n \times n}$ подобна над F квазиестественной матрице B , определяемой однозначно с точностью до порядка следования диагональных клеток, называемой нормальной квазиестественной формой матрицы A , причем $B = \text{diag}(B_1, B_2, \dots, B_s) \in F^{n \times n}$, где $B_1, \dots, B_s$ — матрицы, сопровождающие элементарные делители $(f_1(\lambda))^{k_1}, (f_2(\lambda))^{k_2}, \dots, (f_s(\lambda))^{k_s}$ матрицы. Две матрицы из $F^{n \times n}$ подобны над F тогда и только тогда, когда их нормальные квазиестественные формы совпадают.

Пример 19.26. Инвариантные множители матрицы J из примера 19.18 равны

$$1, 1, 1, 1, 1, 1, \lambda - 2, (\lambda - 2)(\lambda - 3)^2 = \lambda^3 - 8\lambda^2 + 21\lambda - 18,$$

$$(\lambda - 2)^3(\lambda - 3)^2 = \lambda^5 - 12\lambda^4 + 57\lambda^3 - 134\lambda^2 + 156\lambda - 72,$$

поэтому ее естественная форма равна

$$\begin{pmatrix} 2 & & & & & & & & \\ & 8 & -21 & 18 & & & & & \\ & 1 & 0 & 0 & & & & & \\ & 0 & 1 & 0 & & & & & \\ & & & & 12 & -57 & 134 & -156 & 72 \\ & & & & 1 & 0 & 0 & 0 & 0 \\ & & & & 0 & 1 & 0 & 0 & 0 \\ & & & & 0 & 0 & 1 & 0 & 0 \\ & & & & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Элементарные делители матрицы J равны

$$\lambda - 2, \lambda - 2, (\lambda - 2)^3 = \lambda^3 - 6\lambda^2 + 12\lambda - 8, (\lambda - 3)^2 = \lambda^2 - 6\lambda + 9, (\lambda - 3)^2 = \lambda^2 - 6\lambda + 9,$$

поэтому квазиестественная форма равна

$$\begin{pmatrix} 2 & & & & & & & & \\ & 2 & & & & & & & \\ & & 6 & -12 & 8 & & & & \\ & & 1 & 0 & 0 & & & & \\ & & 0 & 1 & 0 & & & & \\ & & & & & 6 & -9 & & \\ & & & & & 1 & 0 & & \\ & & & & & & & 6 & -9 \\ & & & & & & & 1 & 0 \end{pmatrix}.$$

Пример 19.27. Инвариантные множители матрицы A из примера 19.21 равны

$$1, \quad \lambda - 2, \quad (\lambda - 2)^2 = \lambda^2 - 4\lambda + 4,$$

поэтому ее естественная форма равна

$$B = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & -4 \\ 0 & 1 & 0 \end{pmatrix}.$$

В данном примере квазиестественная форма совпадает с естественной, так как элементарные делители ненулевой степени совпадают с инвариантными множителями.

Найдем матрицу Q , такую, что $B = Q^{-1}AQ$. Для этого приведем $B - \lambda E$ к нормальной диагональной форме. Запишем матрицу

$$\begin{pmatrix} 2-\lambda & 0 & 0 \\ 0 & 4-\lambda & -4 \\ 0 & 1 & -\lambda \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Прибавим к третьему столбцу второй, умноженный на λ . Вычтем из второй строки третью, умноженную на $4 - \lambda$. Получим:

$$\begin{pmatrix} 2-\lambda & 0 & 0 \\ 0 & 0 & -\lambda^2 + 4\lambda - 4 \\ 0 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix}.$$

Переставляя строки и столбцы и меняя знак у двух строк, получаем:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda - 2 & 0 \\ 0 & 0 & (\lambda - 2)^4 \\ \hline 0 & 1 & 0 \\ 1 & 0 & \lambda \\ 0 & 0 & 1 \end{pmatrix}.$$

Итак,

$$Q_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & \lambda \\ 0 & 0 & 1 \end{pmatrix}, \quad Q_0 = Q_1 Q_3^{-1} = \begin{pmatrix} -1 & 0 & -17 \\ 0 & -1 & 6 \\ 0 & 0 & 1 \end{pmatrix}$$

(матрица Q_1 вычислена в примере 19.21). Далее необходимо найти остаток Q при делении Q_0 на $J - \lambda E$, но так как матрица Q_0 — скалярная, то $Q = Q_0$. Итак, Q_0 — искомая трансформирующая матрица.

Теорема 19.28. Последний инвариантный множитель матрицы $A \in F^{n \times n}$ является ее минимальным многочленом.