I. Кривые и поверхности второго порядка.

Парабола.

Определение. Линия называется параболой, если существует декартова система координат Oxy, в которой уравнение этой линии имеет вид

$$y^2 = 2px \ (p > 0). \tag{1}$$

Уравнение и система координат называются каноническими. Число p называется фокальным параметром, точка $F = (\frac{p}{2}, 0)$ - фокусом, прямая $x = -\frac{p}{2}$ - директрисой, Ox - ось параболы, точка O - вершина параболы. Для произвольной точки M параболы отрезок FM называется фокальным радиусом. Касательная к параболе в точке (x_0, y_0) имеет уравнение $y_0 y = p(x + x_0)$.

Утверждение 1. Парабола является множеством точек, равноудаленных от фокуса и директрисы.

Доказательство. Условие равноудаленности $x + \frac{p}{2} = \sqrt{(x - \frac{p}{2})^2 + y^2}$ эквивалентно равенству (1).

Оптическое свойство параболы. Касательная к параболе в точке $M = (x_0, y_0)$ пересекает ось Ox в точке $N = (-x_0, 0)$, находящейся на том же расстоянии от фокуса F, что и точка M. Треугольник FNM равнобедренный, то есть $\angle FNM = \angle FMN$. Следовательно, ***если в фокус параболы поместить источник излучения, то отраженные от параболы лучи будут параллельны ее оси.***

Эллипс.

Определение. Линия называется эллипсом, если существует декартова система координат Oxy, в которой уравнение этой линии имеет вид

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \ (a \geq b > 0). \tag{2}$$

Уравнение и система координат называются каноническими. a, b - соответственно большая и малая полуоси эллипса. Фокусами называются точки $F_1 = (-c, 0)$ и $F_2 = (c, 0)$, где $c = \sqrt{a^2 - b^2}$. Точка O - центр эллипса; $(\pm a, 0), (\pm b, 0)$ - вершины; $e = \frac{c}{a}$ - эксцентриситет; прямые $x = \pm\frac{a}{e}$ - директрисы; $p = \frac{b^2}{a}$ - фокальный параметр, равен длине полухорды, проходящей через фокус перпендикулярно оси Ox; для произвольной точки M отрезки $r_1 = MF_1$ и $r_2 = MF_2$ называются фокальными радиусами.

$r_1^2 = (x + c)^2 + y^2 = x^2 + 2cx + c^2 + b^2 - \frac{b^2}{a^2}x^2 = \frac{c^2}{a^2}x^2 + 2cx + a^2 = (\frac{c}{a}x + a)^2 = (ex + a)^2$. Так как $e < 1$ и $|x| \leq a$, то $r_1 = ex + a$. Аналогично доказывается, что $r_2 = a - ex$. Из этих равенств следует, что ***эллипс это множество точек,***

для которых отношение расстояния до фокуса к расстоянию до одноименной директрисы равно эксцентриситету.

Так как $r_1 + r_2 = 2a$, то эллипс можно определить также как ***множество точек, сумма расстояний от которых до фокусов постоянна.***

Касательная к эллипсу в точке $M = (x_0, y_0)$ имеет уравнение $\dfrac{x_0x}{a^2} + \dfrac{y_0y}{b^2} = 1$.

Оптическое свойство эллипса. Пусть точка $M = (x_0, y_0)$ принадлежит эллипсу. Найдем расстояния d_1, d_2 от фокусов F_1, F_2 до касательной к эллипсу, проведенной в точке M.

$$d_1 = \frac{|-\dfrac{x_0c}{a^2} - 1|}{\sqrt{\dfrac{x_0^2}{a^4} + \dfrac{y_0^2}{b^4}}} = \frac{r_1}{\sqrt{a\dfrac{x_0^2}{a^4} + \dfrac{y_0^2}{b^4}}}\ ,\ d_2 = \frac{r_2}{\sqrt{a\dfrac{x_0^2}{a^4} + \dfrac{y_0^2}{b^4}}}.$$

Отсюда $\dfrac{d_1}{r_1} = \dfrac{d_2}{r_2}$, следовательно, отрезки F_1M, F_2M образуют одинаковые углы с касательной. Это означает, что лучи от источника света, помещенного в один из фокусов, после отражения от эллипса собираются в другом фокусе.

Гипербола

Определение. Линия называется гиперболой, если существует декартова система координат Oxy, в которой уравнение этой линии имеет вид

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1. \tag{3}$$

Уравнение и система координат называются каноническими. a, b - соответственно действительная и мнимая полуоси эллипса. Фокусами называются точки $F_1 = (-c, 0)$ и $F_2 = (c, 0)$, где $c = \sqrt{a^2 + b^2}$. Точка O - центр эллипса; $(\pm a, 0)$ - вершины; $e = \dfrac{c}{a}$ - эксцентриситет; прямые $x = \pm\dfrac{a}{e}$ - директрисы; $p = \dfrac{b^2}{a}$ - фокальный параметр, равен длине полухорды, проходящей через фокус перпендикулярно оси Ox; $y = \pm\dfrac{b}{a}x$ - асимптоты; для произвольной точки M отрезки $r_1 = MF_1$ и $r_2 = MF_2$ называются фокальными радиусами.

Так же как для эллипса выводятся равенства $r_1 = |ex + a|$, $r_2 = |a - ex|$, из которых следует, в частности, что ***гипербола это множество точек, для которых отношение расстояния до фокуса к расстоянию до одноименной директрисы равно эксцентриситету.***

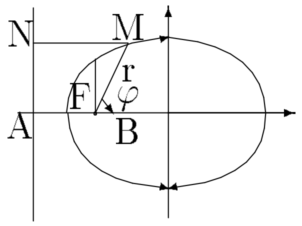
Так как для гиперболы $|x| > a$, $e > 1$, то $|ex| > a$, следовательно,

$$r_1 = \begin{cases} a + ex, & \text{при } x > 0 \\ -a - ex, & \text{при } x \le 0 \end{cases},\ r_2 = \begin{cases} -a + ex, & \text{при } x > 0 \\ a - ex, & \text{при } x \le 0 \end{cases}.$$

Отсюда $|r_1 - r_2| = 2a$, следовательно, ***гипербола это множество точек, для которых абсолютная величина разности расстояний до фокусов есть величина постоянная.***

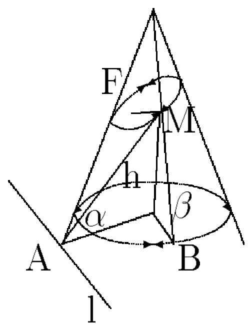
Касательная к гиперболе в точке $M = (x_0, y_0)$ имеет уравнение $\frac{x_0 x}{a^2} - \frac{y_0 y}{b^2} = 1$.

Уравнения эллипса, гиперболы и параболы в полярных координатах.



Центр полярной системы координат для эллипса в левом фокусе, для гиперболы - в правом фокусе. Вывод уравнения для эллипса: $r = e|MN| = e|AF + FB| = e(\frac{p}{e} + r\cos\varphi) \rightarrow r = \frac{p}{1 - e\cos\varphi}$ Аналогично выводится уравнение для правой ветви гиперболы и для параболы.

Кривые второго порядка и конические сечения.



Верхний овал на рисунке есть сечение конуса некоторой плоскостью π_1; F - точка касания π_1 и некоторой сферы, вписанной в конус; нижний овал это окружность, по которой сфера касается конуса; π_2 - плоскость, проходящая через окружность; M - произвольная точка конического сечения; B - точка пенесечения окружности и образующей конуса, проходящей через M; α - угол между плоскостями π_1, π_2; β - угол между MB и π_2; l - линия пересечения π_1, π_2; h - длина перпендикуляра, опущенного из M на π_2.

$FM = MB$ как отрезки касательных к сфере. $h = MB\sin\beta = FM\sin\beta = AM\sin\alpha$. Отсюда вытекает, что $\frac{FM}{AM} = \frac{\sin\alpha}{\sin\beta}$ - не зависит от выбора точки M. Следовательно, сечение конуса плоскостью π_1 является эллипсом, один из фокусов которого находится в точке F , прямая l является директрисой эллипса.

Пример 1. Найти уравнение гиперболы, для которой точка $F(-2, 2)$ служит фокусом , а прямые $2x - y + 1 = 0$, $x + 2y - 7 = 0$ - асимптотами.

Пример 2. Найти каноническое уравнение и каноническую систему координат кривой, заданной уравнением $5x^2 + 4xy + 8y^2 - 32x - 56y + 80 = 0$.

Исследование квадрик.

Определение. Квадрикой называется множество точек $x = (x_1, .., x_n)$ n - мерного аффинного пространства, удовлетворяющих уравнению вида

$$\sum_{i,j} a_{ij}x_i x_j + 2\sum_i b_i x_i + c = 0.$$

Уравнение квадрики можно представить в матричной форме:

$$x^T Ax + 2(b, x) + c = 0.$$

Преобразуем уравнение методом, который был разобран на примере.

1. Находим собственные числа $\lambda_1, \lambda_2, ...\lambda_n$ и ортонормированный базис из собственных векторов $h_1, h_2, ...h_n$ матрицы A. Предположим, для определенности, что $\lambda_1, ..., \lambda_r \neq 0$, где $r = \operatorname{rg} A$.

2. Полагая $P = (h_1...h_n)$ делаем замену $x = Py$. Уравнение квадрики принимает вид $\lambda_1 y_1^2 + ... + \lambda_r y_r^2 + 2b_1' y_1 + ... + 2b_n' y_n + c = 0$.

3. Делаем замену $y_i = z_i - \dfrac{a_i'}{\lambda_i} (i = 1, .., r), y_i = z_i (i = r+1, .., n)$. $\lambda_1 z_1^2 + ... + \lambda_r z_r^2 + 2b_{r+1}' z_{r+1} + ... + 2b_n' z_n + c' = 0$.

4. Положим $\mu = \sqrt{b_{r+1}'^2 + .. + b_n'^2}$. Если $\mu = 0$, то преобразования закончены и в итоге получили уравнение

$$\lambda_1 z_1^2 + ... + \lambda_r z_r^2 + c' = 0.$$

Если $\mu \neq 0$, то рассмотрим n - мерный вектор $g_1 = \dfrac{1}{\mu}(0, ..., 0, b_{r+1}', ..., b_n')^T$. Так как $|g_1| = 1$, то систему $e_1, .., e_r, g_1$ можно дополнить до ортонормированного базиса $e_1, .., e_r, g_1, ..., g_{n-r}$. После замены $z = (e_1, .., e_r, g_1, ..., g_{n-r})v$ получаем уравнение $\lambda_1 v_1^2 + ... + \lambda_r v_r^2 + 2\mu v_{r+1} + c' = 0$.

5. Выполняем последнюю замену $v_{r+1} = w_{r+1} - \dfrac{c'}{2\mu}$, $v_i = w_i$, при $i \neq r+1$. В итоге получили уравнение

$$\lambda_1 w_1^2 + ... + \lambda_r w_r^2 + 2\mu w_{r+1} = 0.$$

Определение. Преобразование $x = Py + q$, где P - ортогональная матрица, а q - вектор, называется изометрией. Если $P = E$ изометрию называют сдвигом.

Очевидно, что преобразование обратное к изометрии является изометрией, и что произведение изометрий - изометрия.

Определение. Уравнения квадрик называются ортогонально эквивалентными, если одно можно получить из другого в результате изометрии.

Описанный ранее алгоритм позволяет утверждать, что уравнение любой квадрики ортогонально по крайней мере одному из уравнений вида

$$F(x) = \lambda_1 x_1^2 + ... + \lambda_r x_r^2 + c = 0. \tag{1}$$

$$F(x) = \lambda_1 x_1^2 + ... + \lambda_r x_r^2 + 2\mu x_{r+1} = 0 \ (\mu > 0). \tag{2}$$

Оказывается, что ***с точностью до порядка следования слагаемых в квадратичной форме, такое уравнение в точности одно.***

Докажем это предложение. Сделаем подстановку $x = Py + q$ в уравнение квадрики $F(x) = x^T Ax + 2a^T x + c$. Получим

$$y^T P^T APy + 2y^T P^T (Aq + a) + F(q) = 0. \qquad (3)$$

Если P ортогональная, то матрицы A и $P^T AP$ подобны, следовательно, имеют одинаковые собственные числа. Поэтому пара ортогонально эквивалентных уравнений вида (1), (2) с точностью до обозначений неизвестных имеет одинаковые квадратичные части. Поэтому, для доказательства надо исследовать выражение $2y^T P^T (Aq + a) + F(q)$. Рассмотрим 3 случая.

1. Предположим, что уравнение (1) изометрией $x = Py + q$ сводится к уравнению

$$\lambda_1 x_1^2 + ... + \lambda_r x_r^2 + c' = 0. \qquad (4)$$

В нашем случае $A = \mathrm{diag}(\lambda_1, .., \lambda_r, 0, ..., 0)$, $a = 0$. Из сопоставления выражений (1) и (3) следует, что $F_1(q) = c'$, $P^T (Aq + a) = 0$. Так как P невырождена и $a = 0$, то $Aq = 0 \to q^T Aq = 0 \to F_1(q) = c$ и, значит , (1) и (4) совпадают.

2. Предположим, что уравнение (1) сводится к уравнению

$$\lambda_1 y_1^2 + ... + \lambda_r y_r^2 + 2\alpha y_{r+1} = 0 \ (\alpha > 0). \qquad (5)$$

Из (3) следует, что $P^T Aq = \mu e_{r+1}$. Из равенства $P^T AP = A$ следует, что $P^T A = AP^{-1}$ и, далее, $AP^{-1} = \alpha e_{r+1}$. Вектор слева имеет нулевую $(r + 1)$ - ю компоненту, следовательно, $\alpha = 0$ - противоречие.

3. Уравнение (2) сводится к (5). В этом случае $P^T (Aq + \mu e_{r+1}) = \alpha e_{r+1}$. Вычислим скалярные квадраты левой и правой частей этого равенства.

$(P^T (Aq + \mu e_{r+1}), P^T (Aq + \mu e_{r+1})) = (Aq + \mu e_{r+1}, Aq + \mu e_{r+1}) = (AC, AC) + \mu^2$ - левая часть, $(\alpha e_{r+1}, \alpha e_{r+1}) = \alpha^2$ - правая часть. Так как $(AC, AC) + \mu^2 = \alpha^2$, то $\mu \le \alpha$. Однако, уравнение (5) также сводится к уравнению (2), поэтому должно выполняться и неравенство $\alpha \le \mu$, следовательно, уравнения (2) и (5) совпадают.

Ортогональная классификация кривых и поверхностей второго порядка.

$\lambda_1 x^2 + \lambda_2 y^2 + c = 0$

1. $\lambda_1, \lambda_2 > 0, c < 0-$ эллипс;
2. $\lambda_1, \lambda_2 > 0, c > 0-$ мнимый эллипс;
3. $\lambda_1, \lambda_2 > 0, c = 0-$ мнимые пересекащиеся прямые;
4. $\lambda_1 > 0, \lambda_2 < 0, c < 0-$ гипербола;
5. $\lambda_1 > 0, \lambda_2 < 0, c = 0-$ пересекающиеся прямые;

$\lambda x^2 + c = 0$	6. $\lambda > 0, c < 0$ - параллельные прямые;
	7. $\lambda > 0, c > 0$ - мнимые параллельные прямые;
	8. $c = 0$ - совпадающие прямые;
$\lambda x^2 + 2\mu y = 0$	9. парабола;
$\lambda_1 x^2 + \lambda_2 y^2 + \lambda_3 z^2 + c = 0$	10. $\lambda_1, \lambda_2, \lambda_3 > 0, c < 0-$ эллипсоид;
	11. $\lambda_1, \lambda_2, \lambda_3 > 0, c > 0-$ мнимый эллипсоид;
	12. $\lambda_1, \lambda_2 > 0, \lambda_3 > 0, c = 0-$ мнимый конус;
	13. $\lambda_1, \lambda_2 > 0, \lambda_3 < 0, c = 0-$ конус;
	14. $\lambda_1, \lambda_2 > 0, \lambda_3 < 0, c > 0-$ двуполостный гиперболоид;
	15. $\lambda_1, \lambda_2 > 0, \lambda_3 < 0, c < 0-$ однополостный гиперболоид;
$\lambda_1 x^2 + \lambda_2 y^2 + 2\mu z = 0$	16. $\lambda_1, \lambda_2 > 0-$ эллиптический параболоид;
	17. $\lambda_1 > 0, \lambda_2 < 0-$ гиперболический параболоид;

Пересечение прямой и квадрики.

$$F(x) = x^T A x + 2(b, x) + c = 0 \tag{1}$$

$$x = x_0 + lt \tag{2}$$

$$l^T A l t^2 + 2 l^T (A x_0 + b) t + F(x_0) = 0 \tag{3}$$

Определение. Вектор $l \neq 0$ называется асимтотическим для (1), если $l^T A l = 0$.

Асимтотический вектор называют также асимптотическим направлением.

Пример 3. У эллипса $x^2 + y^2 = 1$ нет асимптотических направлений; у гиперболы $x^2 - y^2 = 1$ два асипмтотических направления: (1,1) и (1.-1); у параболы $y^2 = 2x$ - одно: (1,0).

Определение. Точка x_0, удовлетворяющая равенству $Ax_0 + b = 0$ называется центром квадрики.

Замечание. Перенос начала системы координат в центр квадрики(если он существует) позволяет избавиться от линейной части в уравнении квадрики.

Покажем, что центр квадрики является ее центром симметрии.

Утверждение 2. Если точка x принадлежит квадрике с центром x_0, то точка $x' = 2x - x_0$ также принадлежит квадрике.

Доказательство. В нашем случае уравнение (3) принимает вид

$$l^T A l t^2 + F(x_0) = 0. \tag{4}$$

Положим $l = x - x_0$. Так как $x = x_0 + 1 \cdot l$, то уравнение (4) имеет корень $t = 1$, следовательно, имеет и корень $t = -1$, поэтому точка $x_0 - l = x'$ принадлежит квадрике.

Пусть l неасимптотический вектор и уравнение (3) имеет вещественные корни t_1, t_2. Тогда прямая (2) пересекает квадрику в двух , возможно совпадающих, точках x_1 и x_2. Вычислим координату x середины хорды, соединяющей эти точки.

$x = \dfrac{x_1 + x_2}{2} = x_0 + \dfrac{t_1 + t_2}{2} l = x_0 - \dfrac{l^T(Ax_0 + b)}{l^T A l}$, $l^T x = l^T x_0 - l^T(Ax_0 + b) = -l^T b$. Отсюда получаем уравнение

$$l^T(Ax + b) = 0. \tag{5}$$

Таким образом середина любой хорды, параллельной l, принадлежит гиперплоскости (5), которая называется ***диаметральной гиперплоскостью, сопряженной вектору*** l.

Замечание. Любой центр квадрики принадлежит любому ее диаметру.

Пример 1. Найти уравнеие диаметра линии $5x^2 - 3xy + y^2 - 3x + 2y - 5 = 0$, проходящего через середину хорды, отсекаемой этой линией на прямой $x - 2y - 1 = 0$. Ответ:$17x - 4y - 4 = 0$.

Вновь рассмотрим уравнение (3). Если $F(x_0) = 0$ и $l^T(Ax_0 + b) = 0$, то уравнение имеет корень $t = 0$ кратности 2 и прямая (2) является касательной к квадрике. Если $Ax_0 + b \neq 0$, то все касательные прямые принадлежат гиперплоскости $(Ax_0 + b)(x - x_0) = 0$, называемой ***касательной гиперплоскостью.*** (Если $Ax_0 + b = 0$, то уравнение квадрики после переноса системы координат принимает вид $x^T A x = 0$, т.е. это либо конус, либо пара плоскостей.)

Пример 2. Найти уравнения касательных к линии $x^2 + xy + y^2 + 2x + 3y - 3 = 0$, параллельных прямой $x + y = 0$. Ответ: $x + y = 1$, $x + y = -13/3$.

Если в уравнении (3) все коэффициенты равны нулю, то прямая (2) расположена на поверхности (1) и называется ее ***прямолинейной образующей.*** Очевидными примерами поверхностей, обладающих прямолинейными образующими, являются цилиндрические поверхности и конус.

Покажем, что прямолинейные образующие есть также у однополостного гиперболоида и гиперболического параболоида.

Рассмотрим гиперболоид, заданный уравнением $x^2 + y^2 - z^2 = 1$. Возьмем на нем произвольную точку (x_0, y_0, z_0). Тогда, для нахождения направляющего вектора $l = (l_1, l_2, l_3)$ надо решить систему уравнений

$$\begin{cases} l_1^2 + l_2^2 - l_3^2 = 0 \\ x_0 l_1 + y_0 l_2 - z_0 l_3 = 0 \end{cases}. \qquad (6)$$

Первое уравнение задает конус, второе - плоскость, проходящую через вершину конуса. Так как плоскость проходит через точку $M = (z_0 x_0, z_0 y_0, z_0^2 + 1)$, расположенную внутри конуса($m_1^2 + m_2^2 - m_3^2 < 0$), то система (6) определяет два различных направления. Итак, ***через каждую точку однополостного гиперболоида проходит ровно две прямолинейные образующие.***

Рассмотрим гиперболический параболоид $x^2 - y^2 = 2z$. Система для определения прямолинейной образующей, проходящей через точку (x_0, y_0, z_0) имеет вид $\begin{cases} l_1^2 - l_2^2 = 0 \\ x_0 l_1 + y_0 l_2 - l_3 = 0 \end{cases}$. Решением системы являются векторы $(1, -1, x_0 - y_0)$, $(1, 1, x_0 + y_0)$. Следовательно, ***через каждую точку гиперболического параболоида проходит ровно две прямолинейные образующие.***

Прямолинейные образующие гиперболоида можно получить другим способом. Преобразуем уравнение

$x^2 + y^2 - z^2 = 1 \to x^2 - z^2 = 1 - y^2 \to (x - z)(x + z) = (1 - y)(1 + y)$.

Из последнего равенства видно, что гиперболоиду принадлежат прямые двух семейств:

$\begin{cases} \lambda(x - z) = \mu(1 - y) \\ \mu(x + z) = \lambda(1 + y) \end{cases}$ и $\begin{cases} \lambda(x + z) = \mu(1 - y) \\ \mu(x - z) = \lambda(1 + y) \end{cases}$, где $\lambda^2 + \mu^2 \neq 0$.

Аналогично можно получить два семейства прямолинейных образующих гиперболического параболоида: $\begin{cases} z = \lambda(x + y) \\ \lambda = x - y \end{cases}$ и $\begin{cases} z = \lambda(x - y) \\ \lambda = x + y \end{cases}$.

II. Группы .

Пусть G - непустое множество. Говорят, что на G определена бинарная операция $'*'$, если каждой паре $g_1, g_2 \in G$ соответствует третий элемент $g_3 = g_1 * g_2$ того же множества.

Определение. Непустое множество G с бинарной операцией $'*'$ называется группой, если выполняются следующие аксиомы:

1. операция ассоциативна;
2. $\exists e \in G \;/\; \forall g \in G \; g * e = e * g = g$;
3. $\forall g \in G \quad \exists g' \;/\; g * g' = e$.

Пример 3. Циклическая группа $\{e, a, a^2, ..., a^{n-1}\}$.

Определение. Подстановкой n-й степени называется взаимно- однозначное отображение n - элементного множества на себя.

Для множества $M = \{m_1, m_2, ..., m_n\}$ любую подстановку можно записать в виде

$$\begin{pmatrix} m_1 & \dots & m_n \\ m_{i_1} & \dots & m_{i_n} \end{pmatrix}.$$

В строках подстановки иногда удобнее записывать не элементы множества, а их номера. Так для множества $M = \{a, b, c\}$ подстановки

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

идентичны.

Результат действия двух подстановок π_1, π_2 есть третья подстановка π, которая называется их произведением.

Тождественная и обратная подстановки.

Ассоциативность умножения легко показать с помощью диаграммы

$$i_1 \xrightarrow{\pi_1} i_2 \xrightarrow{\pi_2} i_3 \xrightarrow{\pi_3} i_4$$

$[(\pi_1\pi_2)\pi_3](i_1) = \pi_3(i_3) = i_4$, $[\pi_1(\pi_2\pi_3)](i_1) = (\pi_2\pi_3)(i_2) = i_4$.

Таким образом, множество всех подстановок n - й степени является группой относительно умножения.

Графическое изображение подстановок. Разложение в произведение независимых циклов, произведение транспозиций:$(i_1..i_k) = (i_1\ i_2)..(i_1\ i_k)$.

Определение. Непустое подмножество элементов группы G являющееся группой относительно той же операции, называется подгруппой.

Свойства таблицы умножения группы.

1. Каждая строка и столбец содержат каждый символ точно один раз.

2. Существуют строка и столбец, помеченные символом e и тождественные первой строке и первому столбцу соответственно.

3. Символы e, расположенные выше и ниже главной диагонали, симметричны.

4. ассоциативность проявляется в том, что любые два элемента r, s группы, их произведение $u = rs$ и e образуют в таблице умножения следующую конфигурацию

$$\begin{array}{c|ccc} & y & & x \\ \hline z & u & \text{---} & r \\ & | & & | \\ x & s & \text{---} & e \end{array}$$

Другими словами, если e одна из вершин прямоугольника, er - вертикальное, а es - горизонтальное ребро того же прямоугольника, то rs - его последняя вершина.

Действительно, из ассоциативности и равенств $r = zx^{-1}$, $s = xy$ получаем $rs = (zx^{-1})(xy) = zy = u$.

Если таблица обладает указанным выше свойством, то для любых элементов a, b, c группы таблица содержит следующий фрагмент

$$\begin{array}{c|ccc} & e & bc & b \\ \hline e & e & bc & b \\ a & a & v & ab \\ b^{-1} & b^{-1} & c & e \end{array}$$

Элемент v, стоящий на пересечении столбца bc и строки a, согласно правилу составления таблицы равен a(bc), а по свойству таблицы - равен (ab)c.

Гомоморфизмы групп.

Определение. Пусть $G = \{M, *\}$ и $G' = \{M', \circ\}$ - группы. Отображение φ множества M в множество M' называется гомоморфизмом, если для любых $g, h \in M$ выполняется равенство $\varphi(g*h) = \varphi(g) \circ \varphi(h)$(сохраняется операция).

Определение. Изоморфизмом называется взаимно однозначное соответствие, сохраняющее операцию.

Пример 4. Конечная циклическая группа порядка n изоморфна группе корней степени n из 1.

Пример 5. Бесконечная циклическая группа изоморфна группе целых чисел относительно сложения.

Пример 6. $\{R_+, *\} \xrightarrow{\ln} \{R, +\}$.

Пример 7. Группы $\{Q_+, *\}$и$\{Q, +\}$ не изоморфны.

Утверждение 1. Гомоморфный образ группы есть группа.

Доказательство. Пусть G группа, e единичный элемент, $H = \varphi(G)$ гомоморфный образ G ,$\circ$ операция в H. Проверим выполнение аксиом группы для H.

1. Существование единичного элемента. Так как для $\forall h \in H \quad \exists g \in G$ такой, что $h = \varphi(g)$,то $h \circ \varphi(e) = \varphi(g) \circ \varphi(e) = \varphi(g*e) = \varphi(g) = h$.

2. Существование обратного элемента. $h \circ \varphi(g^{-1}) = \varphi(g) \circ \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e)$.

3. Ассоциативность.$h_1 * (h_2 * h_3) = \varphi(g_1) * (\varphi(g_2) * \varphi(g_3)) = \varphi(g_1) \circ \varphi(g_2 * g_3) = \varphi(g_1 * (g_2 * g_3)) = \varphi((g_1 * g_2) * g_3)) = \ldots$

Теорема Кэли. Любая группа конечного порядка n изоморфна некоторой подгруппе группы S_n.

Доказательство. Пусть $G = \{g_1, \ldots, g_n\}$ некоторая группа. Рассмотрим отображение

$$\varphi(g_i) = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1 g_i & \ldots & g_n g_i \end{pmatrix}.$$

Ясно, что φ взаимно однозначное отображение. Кроме того,

$$\varphi(g_i g_j) = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1(g_i g_j) & \ldots & g_n(g_i g_j) \end{pmatrix} = \begin{pmatrix} g_1 & \cdots & g_n \\ (g_1 g_i) g_j & \ldots & (g_n g_i) g_j \end{pmatrix} =$$

$$= \begin{pmatrix} g_1 & \cdots & g_n \\ g_1 g_i & \ldots & g_n g_i \end{pmatrix} \begin{pmatrix} g_1 g_i & \cdots & g_n g_i \\ (g_1 g_i) g_j & \ldots & (g_n g_i) g_j \end{pmatrix} = \varphi(g_i)\varphi(g_j).$$

Из предыдущего утверждения следует, что образ отображения есть группа.

Смежные классы. Если M, N два подмножества некоторой группы G, то $M * N \stackrel{\text{def}}{=} \{m * n | m \in M, n \in N\}$. Если, например, M состоит из одного элемента, тогда используется запись $m * N$.

Определение. Левыми(правыми) смежными классами группы G по подгруппе H называются множества вида $g * H (H * g)$, где $g \in G$.

Каждый элемент класса считается представителем этого класса.

Утверждение 2. $a * H = b * H \leftrightarrow a^{-1} * b \in H, H * a = H * b \leftrightarrow a * b^{-1} \in H$.

Утверждение 3. Любые два левых класса либо совпадают, либо не имеют общих элементов.

Доказательство. $x \in a * H \cap b * H \to a * h_1 = b * h_2 \to a^{-1} * b \in H \to a * H = b * H$.

Пример 1. $G = \{e, a, a^2, a^3, a^4, a^5\}, H = \{e, a^3\}$.

Определение. Мощность множества смежных классов называется индексом подгруппы H в группе G и обозначается $|G : H|$.

Теорема Лагранжа. Если H подгруппа конечной группы G, то $|G| = |H||G : H|$.

Определение. Порядком элемента группы называется порядок порожденной этим элементом циклической подгруппы.

Иными словами, порядок элемента a это наименьшее натуральное число n такое, что $a^n = e$.

Следствие 3.1. Порядок элемента конечной группы является делителем порядка группы.

Необходимо отметить, что из теоремы Лагранжа не следует, что в произвольной группе порядка n существует подгруппа порядка l, если l делит n. В качестве примера можно привести группу четных подстановок 4-й степени A_4, в которой нет подгруппы 6-го порядка.(Подстановка называется четной, если она раскладывается в произведение четного числа транспозиций.)

В циклической группе $\{e, a, a^2, ..., a^{n-1}\}$ порядка n для каждого делителя d числа n существует подгруппа порядка d: $\{e, a^{\frac{n}{d}}, ..., a^{\frac{(d-1)n}{d}}\}$.

Упражнение. Доказать, что, кроме перечисленных выше, других подгрупп циклическая группа не имеет.

Утверждение 4. Подмножество H группы G является подгруппой, если выполняется любое из условий:

1. $\forall a, b \in H \quad ab^{-1} \in H$;
2. H- конечно и $\forall a, b \in H \quad ab \in H$.

Теорема Силова. Пусть $G = \{g_1, ..., g_n\}$ - группа порядка n, p - простое число. Для любого p^s, делящего n в G существует подгруппа порядка p^s.

Доказательство. Пусть $|G| = p^r l, HOD(p, l) = 1$. Пусть $A = \{M_1, ..., M_q\}$

- множество всех подмножеств мощности p^s. Так как $q = C_{p^s}^{p^r l} = p^{r-s} l \prod_{j=1}^{p^s-1} \frac{p^r l - j}{j}$, то q не делится на p^{r-s+1}.

Назовем орбитой элемента M из A множество $MG = \{Mg | g \in G\}$. Орбита любого элемента Mg' из MG совпадает с MG, поэтому орбиты двух элементов из A либо совпадают либо не пересекаются, так, что A разбивается на непересекающиеся орбиты. Так как q не делится на p^s, то существует орбита $\{M_1, ..., M_m\}$, мощность m которой не делится на p^{r-s+1}.

Обозначим $G_i = \{g \in G | M_1 g = M_i g\}, \quad i = 1, 2, ..., m.$

Покажем, что G_1 -подгруппа, а G_i правые смежные классы G/G_1.

$\forall g_1, g_2 \in G_1$ имеем $M_1(g_1 g_2) = (M_1 g_1) g_2 = M_1 g_2 = M_1$, следовательно, G_1 - подгруппа.

$\forall g_1, g_2 \in G_i, \quad M_1 g_1 = M_1 g_2 \to M_1 g_1 g_2^{-1} = M_1 \to g_1 g_2^{-1} \in G_1.$

Так как $m|G_1| = p^r l$, то $|G_1|$ делится на p^s, поэтому $|G_1| \geq p^s$. С другой стороны, если $x \in M_1$, то по определению G_1 имеем $xG_1 \subseteq M_1$, следовательно, $|G_1| \leq |M_1| = p^s$.

Гомоморфизмы и нормальные подгруппы.

Определение. Подгруппа H группы G называется нормальной, если

$$\forall g \in G, \quad gH = Hg. \tag{1}$$

Пример 1. Подгруппа $\{(1), (1, 2)\}$ не является нормальной в S_3.

Покажем, что условие (1) можно заменить на условие

$$\forall g \in G, \quad gHg^{-1} \subseteq H. \tag{2}$$

Действительно, из (2) следует, что $\forall g \in G \quad H \subseteq g^{-1}Hg \subseteq H$. Следовательно, $g^{-1}Hg = H$ или, что то же самое, $Hg = gH$.

Утверждение 5. Множество смежных классов группы G по нормальной подгруппе H образует группу относительно операции, действующей в G. Она называется фактор-группой и обозначается G/H.

Доказательство. 1. Замкнутость: $aH \cdot bH = a(Hb)H = a(bH)H = abH$.

2. Единичный элемент - H.

3. Обратный элемент: $(aH)^{-1} = a^{-1}H$.

Определение. Ядром гомоморфизма $G \xrightarrow{\varphi} \bar{G}$ называется $\ker \varphi = \{g \in G | \varphi(g) = \bar{e}\}$.

Утверждение 6. Если H - нормальная подгруппа в G, то отображение $\varphi(g) = gH$ есть гомоморфизм G на G/H, причем $H = \ker \varphi$.

Доказательство. Так как $\varphi(g_1 g_2) = g_1 g_2 H = g_1 H \cdot g_2 H = \varphi(g_1)\varphi(g_2)$, то φ - гомоморфизм. Далее, для всякого $g \in H$ имеем $\varphi(g) = gH = H$.

Утверждение 7. Если φ гомоморфизм $G \to \bar{G}$, то:

1. $\ker \varphi$ - нормальная подгруппа;

2. $G/\ker\varphi$ изоморфна $\bar{G}$.

Доказательство. 1. $\forall g \in G \quad \varphi(g^{-1}\ker\varphi\ g) = \varphi(g^{-1})\varphi(\ker\varphi)\varphi(g) = \varphi(g^{-1})\varphi(g) = e$.

2. Рассмотрим отображение $F(g\ker\varphi) = \varphi(g)$.

a)$F(g\ker\varphi \cdot r\ker\varphi) = F(gr\ker\varphi) = \varphi(gr)$ и $F(g\ker\varphi)F(r\ker\varphi) = \varphi(g)\varphi(r) = \varphi(gr)$,то есть операция сохраняется.

b) $\varphi(g) = \varphi(r) \leftrightarrow \bar{e} = [\varphi(g)]^{-1}\varphi(r) = \varphi(g^{-1})\varphi(r) = \varphi(g^{-1}r) \leftrightarrow g^{-1}r \in \ker\varphi \leftrightarrow$ g и r принадлежат одному классу, то есть $g\ker\varphi = r\ker\varphi$.

Задача. Найти все гомоморфизмы группы $G = \{e, a, a^2, ..., a^{n-1}\}$ в группу $\bar{G} = \{\bar{e}, \bar{a}, \bar{a}^2, ..., \bar{a}^{m-1}\}$.

Решение. Пусть φ один из гомоморфизмов.

1. Так как $\varphi(G)$ - группа, то $|\varphi(G)|$ делит $|\bar{G}| = m$.

2. Так как $G/\ker\varphi$ изоморфна $\varphi(G)$, то $|\varphi(G)|$ делит n.

3. $\varphi(G)$ порождена $\varphi(a)$, поэтому гомоморфизм φ полностью определяется значением $\varphi(a)$.

Пусть $d = HOD(m, n)$, тогда существует d гомоморфизмов: $\varphi_i(a) = \bar{a}^{\frac{mi}{d}}, \quad i = 0, .., d-1$.

III. Кольца и поля.

Определение. Множество называется кольцом, если для любых пары его элементов определены сумма и произведение,причем оно является абелевой группой относительно сложения и полугруппой относительно умножения. Кроме того, операции связаны законом дистрибутивности.

Пример 1. Кольцо целых чисел, кольцо вычетов по модулю n.

Определение. Ненулевые элементы a, b кольца называются соответственно левым и правым делителями нуля, если $a \cdot b = 0$.

Определение. Кольцо называется полем, если множество его ненулевых элементов образует абелеву группу относительно умножения.

Утверждение 1. Поле рациональных чисел содержится в любом числовом поле.

Замечание. Числовых полей бесконечно много:

1. $\{a + b\sqrt{n^2+1} |\ a, b \in Q\}$.

2. $P_n = \{a_0 + a_1\sqrt[n]{2} + ... + a_{n-1}\sqrt[n]{2^{n-1}} |\ a_0, .., a_{n-1} \in Q\}, P_2 \subset P_4 \subset P_8 ....$

Утверждение 2. Конечное кольцо без делителей нуля является полем.

Пример 1. Кольцо вычетов по простому модулю.

Утверждение 3. Для того, чтобы подмножество M кольца K было кольцом необходимо и достаточно чтобы

1. $\forall a, b \in M\ a - b \in M$;

2. $\forall a, b \in M\ ab \in M$.

Определение. Непустое множество I кольца K называется идеалом, если

1. $\forall a, b \in I \; a - b \in I$;

2. $\forall a \in I, \forall b \in K \; ab \in I$.

Примеры. 1. 2Z - идеал в кольце Z.

2. Идеал (a), порожденный элементом a некоторого кольца K, и состоящий из всевозможных выражений вида $ar + na$, $r \in K$, $n \in Z$.

Любой идеал I некоторого кольца K, являясь подгруппой аддитивной абелевой группы, определяет разбиение на смежные классы $M = \{I, a + I, b + I, c + I, ...\}$. Множество M является аддитивной абелевой группой по сложению. Однако, произведение двух классов может не быть смежным классом, например, Z разбивается на два класса 2Z и 2Z + 1, причем $2Z \cdot 2Z \neq 2Z$ и $2Z \cdot 2Z \neq 2Z + 1$. Если же определить правило умножения классов следующим образом: $(a + I)(b + I) \stackrel{\mathrm{def}}{=} ab + I$, то M станет кольцом, которое называется фактор-кольцом. Следует отметить, что введенное правило умножения корректно, так как не зависит от выбора представителей классов: $(a + i)(b + j) = ab + (aj + bi + ij) \in ab + I$.

Определение. Отображение $K \xrightarrow{\varphi} \bar{K}$ кольца в кольцо называется гомоморфизмом, если выполняются следующие условия:

1. $\forall a, b \in K \quad \varphi(a + b) = \varphi(a) \oplus \varphi(b)$,

2. $\forall a, b \in K \quad \varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$.

Гомоморфизм колец.

Определение. Ядром гомоморфизма называется множество $\ker \varphi = \{a \in K | \varphi(a) = \bar{0}\}$.

Утверждение 4. Ядро гомоморфизма - идеал.

Утверждение 5. Если φ гомоморфизм K в $\bar{K}$, то $K/\ker\varphi \simeq \bar{K}$.

Утверждение 6. Если I идеал кольца K, то фактор-кольцо K/I является гомоморфным образом кольца K.

IV. Полиномы от нескольких неизвестных.

Лексикографический порядок. Симметрический полином. Моногенный полином. Однородный симметрический полином.

Теорема о симметрических полиномах.

Однозначность представления.Формулы Виета.

Поле разложения многочлена.

Пусть f(x) некоторый многочлен с коэффициентами из некоторого поля P. Поле $\bar{P}$, в котором f(x) раскладывается в произведение многочленов первой степени, называется полем разложения для f(x). Очевидно, что $P \subseteq \bar{P}$.

Далее мы увидим, что поле разложения можно построить для любого многочлена.

Рассмотрим неприводимый над полем P многочлен f(x). Вначале построим поле P' , в котором f(x) будет обладать корнем. Элементами этого поля являются всевозможные выражения вида $a_0\Delta^{n-1}+...+a_{n-1}$, где $a_0,...,a_{n-1}\in P$. В частности, каждый элемент из P принадлежит P', поэтому P' называется расширением поля P. Складываются элементы $A,B\in P'$ так же как многочлены. Если $A=a_0\Delta^{n-1}+...+a_{n-1}$, $B=b_0\Delta^{n-1}+...+b_{n-1}$, то $A+B=(a_0+b_0)\Delta^{n-1}+...+(a_{n-1}+b_{n-1})$. Для нахождения AB находим остаток g(x) от деления многочлена $(a_0x^{n-1}+...+a_{n-1})(b_0x^{n-1}+...+b_{n-1})$ на f(x) и полагаем $AB\overset{\mathrm{def}}{=}g(\Delta)$. По той же схеме осуществляется упрощение выражений вида $\alpha_0\Delta^k+...+\alpha_k$, при $k\geq n$: если $\alpha_0x^k+...+\alpha_k\equiv v(x)(\mathrm{mod}\, f(x))$, то $\alpha_0\Delta^k+...+\alpha_k\overset{\mathrm{def}}{=}v(\Delta)$. Осталось заметить, что $f(\Delta)=0$. В поле $P', f(x)$ раскладывается в произведение, по крайней мере, двух многочленов ненулевой степени. Если все сомножители имеют степень 1, то задача решена. Иначе следует строить расширение поля P' и т.д..

Основная теорема алгебры. Всякий многочлен с комплексными коэффициентами имеет хотя бы один комплексный корень.

Доказательство. Вначале докажем теорему для многочленов с действительными коэффициентами.

Рассмотрим многочлен f(x) степени n. Представим n в виде $n=2^km$, где m нечетно. Доказательство проведем индукцией по k. При $k=0$ степень многочлена нечетна, поэтому можно выбрать достаточно большое действительное число α так, чтобы числа $f(\alpha), f(-\alpha)$ имели разные знаки. Из непрерывности функции f(x) следует, что на интервале $(-\alpha,\alpha)$ найдется корень уравнения $f(x)=0$. Предположим, что теорема справедлива для всех многочленов, степень которых имеет вид $2^{d-1}m$ (m - нечетно). Пусть P - поле разложения для f(x) степени 2^dm и $\alpha_1,\alpha_2,...$ - корни f(x). Выберем произвольное действительное число c и рассмотрим набор всевозможных элементов вида $\beta_{ij}^c=\alpha_i\alpha_j+c(\alpha_i+\alpha_j)$ $(i<j)$. Построим многочлен $g(x)=\prod\limits_{ij}(x-\beta_{ij}^c)$. Коэффициенты его действительны, степень равна $\binom{2^dm}{2}=2^{d-1}q$, где q -нечетное число. По предположению индукции g(x) имеет комплексный корень. Таким образом, для любого действительного числа c существует пара i, j такая, что β_{ij}^c - комплексное число. Так как число пар ограничено, то найдутся действительные числа c_1,c_2 такие, что $\beta_{ij}^{c_1},\beta_{ij}^{c_2}$ - комплексные числа.

Так как $\alpha_i\alpha_j, \alpha_i+\alpha_j$ удовлетворяют крамеровской системе линейных уравнений

$$\begin{cases} u+c_1v=\beta_{ij}^{c_1} \\ u+c_2v=\beta_{ij}^{c_2} \end{cases},$$

то являются комплексными числами. Следовательно, α_i,α_j есть корни квадратного уравнения $t^2 - (\alpha_i + \alpha_j)t + \alpha_i\alpha_j = 0$ с комплексными коэффициентами, значит, являются комплексными числами.

Пусть многочлен имеет комплексные коэффициенты. Представим его в виде $f(x) = u(x) + iv(x)$, где $u(x), v(x)$ - многочлены с действительными коэффициентами. Многочлен $r(x) = u^2(x) + v^2(x)$ имеет комплексный корень α. Так как $r(x) = (u(x) + iv(x))(u(x) - iv(x))$,то либо $u(\alpha) + iv(\alpha) = 0 \sim f(\alpha) = 0$, либо $u(\alpha) - iv(\alpha) = 0$. В последнем случае имеем $\overline{u(\alpha) - iv(\alpha)} = 0 \rightarrow u(\bar{\alpha}) + iv(\bar{\alpha}) = 0$, то есть $\bar{\alpha}$ является корнем $f(x)$.

V. Приведение λ матриц.

Определение. λ матрица называется нормальной диагональной, если ее элементы, расположенные вне главной диагонали равны 0, а каждый из диагональных элементов, кроме первого, либо равен нулю, либо делится на предыдущий.

Утверждение 1. Для всякой λ матрицы $A = (a_{ij})$ существует эквивалентная ей нормальная диагональная матрица.

Доказательство. Применим к матрице следующую процедуру.

0. Если все элементы матрицы равны нулю, то процедура завершается.

1. Найти ненулевой элемент наименьшей степени и перестановкой строк и столбцов поместить его в левый верхний угол.

2. for i:=2 to n do $(i) := (i) - \left[\frac{a_{i1}}{a_{11}}\right](1)$; for j:=2 to m do $[j] := [j] - \left[\frac{a_{1j}}{a_{11}}\right][1]$.

3. Если $a_{i1} = 0 \,\&\, a_{1j} = 0 \;\forall\, i, j > 1$, то перейти на 4 иначе перейти на 1.

4. Если $\exists\, a_{ij}$,который не делится на a_{11}, то $(1) := (1) + (i)$ и перейти на 1.

На выходе процедуры получится матрица вида

$$\begin{pmatrix} a'_{11} \;\; 0 \;\; 0 \; .... \;\; 0 \\ 0 \;\; a'_{22} \; a'_{23} \; ... \; a'_{2n} \\ .... \\ 0 \;\; a'_{m2} \; a'_{m3} ... \; a'_{mn} \end{pmatrix},$$

в которой все элементы делятся на a_{11}. Далее следует применить процедуру к подматрице, не содержащей первой строки и первого столбца.

Определение. Многочлены $e_i(\lambda)$, $i = 1, .., r$ называются инвариантными множителями.

Рассмотрим разложение инвариантных множителей в произведение неприводимых многочленов: $e_i(\lambda) = f_{i1}^{k_{i1}} ... f_{is_1}^{k_{is_1}}$, $i = 1, .., r$.

Многочлены $f_{i1}^{k_{i1}}$ называются элементарными делителями.

Зная порядок, ранг и систему элементарных делителей можно определить ее инвариантные множители.

Пример 1. $n = 4, r = 3, \{\lambda + 1, \lambda, \lambda^2, (\lambda - 1)^3, \lambda - 1\}$.

Утверждение 2. Система элементарных делителей диагональной матрицы
$A = \mathrm{diag}(f_1(\lambda), .., f_n(\lambda))$ равна объединению элементарных делителей диагональных элементов.

Доказательство. Пусть $r = rgA$, $d(\lambda)$ - неприводимый многочлен и $f_i(\lambda) = d^{s_i}(\lambda)g_i(\lambda)$, причем $g_i(\lambda)$ не делятся на $d(\lambda)$. Не уменьшая общности, считаем,что $s_1 \leq s_2 \leq ... \leq s_r$. Тогда $D_k(\lambda) = d^{s_1+..+s_k}G_k(\lambda)$, где $G_k(\lambda)$ не делятся на $d(\lambda)$. Отсюда $e_k(\lambda) = d^{s_k}\dfrac{G_k(\lambda)}{G_{k-1}(\lambda)}$, т.е. $d^{s_k}(\lambda)$ при $s_k \neq 0$ является элементарным делителем.

Утверждение 3. Система элементарных делителей блочно-диагональной матрицы равна объединению элементарных делителей блоков.

Деление λ матриц.

Каждая λ матрица представима в виде многочлена от λ, коэффициентами которого являются матрицы, например,
$\begin{pmatrix} \lambda^2-1 & 0 \\ \lambda & \lambda+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\lambda^2 + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\lambda + \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$

Утверждение 4. Пусть $A(\lambda) = A_0\lambda^s + A_1\lambda^{s-1} + ... + A_s$, B- матрицы одинакового размера, причем B - скалярная. Тогда существуют $P(\lambda), R, Q(\lambda), H$ такие,что

$$A(\lambda) = (\lambda E - B)P(\lambda) + R = Q(\lambda)(\lambda E - B) + H,$$

причем $R = B^sA_0 + ... + A_s$ и $H = A_0B^s + ... + A_s$.

Доказательство. Проведем доказательство индукцией по s. При $s = 0$ утверждение очевидно. Предположим, что утверждение справедливо для матричных многочленов степени меньшей, чем s. Рассмотрим

$$A'(\lambda) = A(\lambda) - (\lambda E - B)A_0\lambda^{s-1} = (A_1 + BA_0)\lambda^{s-1} + A_2\lambda^{s-2} + .. + A_s$$

степень которого меньше s , следовательно, найдутся $P'(\lambda), R'$ такие,что $A'(\lambda) = (\lambda E - B)P'(\lambda) + R'$. Отсюда

$$A(\lambda) = (\lambda E - B)(P'(\lambda) + A_0\lambda^{s-1}) + R'.$$

Таким образом, $P(\lambda), R$ действительно существуют, причем

$$R = R' = A'_{л}(B) = B^{s-1}(A_1 + BA_0) + B^{s-2}A_2 + .. + A_s.$$

Определение. λ матрица называется унимодулярной, если обратная к ней также λ матрица.

Утверждение 5. λ матрица унимодулярна тогда и только тогда, когда ее определитель является отличным от нуля действительным числом.

Утверждение 6. A, B эквивалентны тогда и только тогда, когда существуют унимодулярные P, Q такие, что $A = PBQ$.

Утверждение 7. Числовые матрицы A, B подобны тогда и только тогда, когда эквивалентны их характеристические матрицы.

Доказательство. Пусть $U(A - \lambda E)V = B - \lambda E$ Представим U, V в виде $U = (B - \lambda E)P + R,\ V = Q(B - \lambda E) + H$. Покажем, что $RAH = B$ & $R = H^{-1}$.

$$(U - (B - \lambda E)P)(A - \lambda E)(V - Q(B - \lambda E) =$$

$$U(A - \lambda E)V - (B - \lambda E)P(A - \lambda E)V - U(A - \lambda E)Q(B - \lambda E) +$$

$$(B - \lambda E)P(A - \lambda E)Q(B - \lambda E) = (B - \lambda E) -$$

$$(B - \lambda E)[PU^{-1} - V^{-1}Q + P(A - \lambda E)Q](B - \lambda E).$$

Пусть $S\lambda^k$ старший член матричного многочлена в квадратных скобках. Тогда старший член правой части равен $S\lambda^{k+2}$, а слева - многочлен первой степени. Равенство возможно только при $S = 0$. Следовательно, $R(A - \lambda E)H = B - \lambda E$, из чего легко получается требуемое.

Пример 1. Доказать, что $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ и $B = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ подобны и найти R такую, что $RAR^{-1} = B$.

Решение.

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

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

Отсюда $U = \begin{pmatrix} 0 & -1 \\ 1 & 2-\lambda \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 2-\lambda \end{pmatrix} = \begin{pmatrix} -1 & 4-2\lambda \\ 0 & -1 \end{pmatrix}$.

$R = U_л(B) = \begin{pmatrix} -1 & 4 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

Канонические формы матриц.

Определение. Жордановой клеткой размера n называется матрица вида

$$G_n(\alpha) = \begin{pmatrix} \alpha & 1 & \dots & 0 & 0 \\ 0 & \alpha & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha & 1 \\ 0 & 0 & \dots & 0 & \alpha \end{pmatrix}$$

Определение. Жордановой матрицей называется матрица вида

$$G = \mathrm{diag}(G_{n_1}(\alpha_1), G_{n_2}(\alpha_2), ..., G_{n_k}(\alpha_k)).$$

Лемма. Характеристическая матрица $G_n(\alpha) - \lambda E$ имеет единственный элементарный делитель $(\lambda - \alpha)^n$.

Утверждение 8. Каждая квадратная матрица над полем комплексных чисел подобна жордановой матрице.

Доказательство. Пусть $(\lambda-\lambda_1)^{n_1}, (\lambda-\lambda_2)^{n_2}, ..., (\lambda-\lambda_k)^{n_k}$ элементарные делители матрицы $A-\lambda E$. Рассмотрим матрицу $G = \mathrm{diag}(G_{n_1}(\lambda_1), G_{n_2}(\lambda_2), ..., G_{n_k}(\lambda_k))$

Так как $G - \lambda E$ и $A - \lambda E$ имеют одинаковые размеры, ранги ($n = rg = n_1 + ... + n_k$) и систему элементарных делителей, то они эквивалентны, следовательно, A подобна G.

Пример 1. Найти жорданову форму $\begin{pmatrix} 0 & -4 & -2 \\ 1 & 4 & 1 \\ 0 & 0 & 2 \end{pmatrix}$ Ответ: $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$.

Построение жорданова базиса.

Определение. Базис называется жордановым для линейного преобразования, если матрица преобразования в этом базисе жорданова.

Пусть φ некоторое преобразование пространства V. Как установлено выше матрица φ в некотором базисе $e_1, ..., e_n$ имеет блочно-диагональный вид

$$G = \mathrm{diag}(\Gamma_1(\lambda_1), \Gamma_2(\lambda_2), ..., \Gamma_s(\lambda_s)),$$

где $\Gamma_i(\lambda_i)$ подматрица размера k_i, содержащая все жордановы клетки с λ_i на диагонали. С блочно - диагональной матрицей связано разложение пространства в прямую сумму $V = V_1 \oplus V_2 \oplus ... \oplus V_s$ где V_i инвариантны относительно φ $\dim V_i = k_i$, а сужение φ/V_i в базисе $e_{k_1+..+k_{i-1}+1}, .., e_{k_1+..+k_i}$ имеет матрицу $\Gamma(\lambda_i)$.

Таким образом, достаточно найти жорданов базис преобразования φ/V_i в подпространстве V_i для $\forall$ $i \in \{1, ..., s\}$. Но прежде надо уметь находить V_i.

Утверждение 9. $\forall i \quad \exists \quad r \in Z \quad | \quad V_i = \ker(\varphi - \lambda_i E)^r$

Доказательство. Методом мат.индукции можно вывести следующую формулу:

$$G_k^m(\alpha) = \begin{pmatrix} \alpha^m & C_m^1 \alpha^{m-1} & ... & C_m^{k-1}\alpha^{m-k+1} \\ 0 & \alpha^m & ... & C_m^{k-2}\alpha^{m-k+2} \\ ... & ... & ... & ... \\ 0 & 0 & ... & \alpha^m \end{pmatrix} (m \geq k+1).$$

Из нее следует два замечания:

1.Если $\alpha \neq 0$, то при любом m $G_k^m(\alpha)$ невырождена;

2.Если $\alpha = 0$, то при $m \geq k$ $G_k^m(\alpha) = 0$.

Так как матрицей преобразования $\varphi - \lambda_i E$ в рассматриваемом базисе является $G - \lambda_i E = \mathrm{diag}(\Gamma(\lambda_1 - \lambda_i)...\Gamma(\lambda_s - \lambda_i)$, то матрицей преобразования $(\varphi - \lambda_i E)^r$ в рассматриваемом базисе является $(G - \lambda_i E)^r = \mathrm{diag}(\Gamma^r(\lambda_1 - \lambda_i)...\Gamma^r(\lambda_s - \lambda_i)$. Так как при $r \geq \mathrm{dim} V_i \quad \Gamma_i^r(0) = 0$, а $\Gamma_j^r(\lambda_1 - \lambda_j) \quad (j \neq i)$ невырождены, то $V_i = \ker(\varphi - \lambda_i E)^n$.

Теперь выясним как находить жорданов базис для преобразований с единственным собственным числом. Вначале рассмотрим следующий пример.

Пример 1. Известно, что матрица A подобна матрице

$$G = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}.$$

Найти жорданов базис.

Обозначим векторы жорданова базиса g_1, g_2, g_3. Согласно определению матрицы линейного преобразования справедливы равенства

$$Gg_1 = \alpha g_1, \quad Gg_2 = g_1 + \alpha g_2, \quad Gg_3 = g_2 + \alpha g_3$$

Поскольку A матрица того же преобразования, то

$$Ag_1 = \alpha g_1, \quad Ag_2 = g_1 + \alpha g_2, \quad Ag_3 = g_2 + \alpha g_3$$

Перепишем последние равенства в виде

$$(A - \alpha E)g_1 = 0 \quad (A - \alpha E)g_2 = g_1 \quad (A - \alpha E)g_3 = g_2 \qquad (1)$$

Рассмотрим подпространства

$$H_1 : (A - \alpha E)x = 0 \quad H_2 : (A - \alpha E)^2 x = 0 \quad H_3 : (A - \alpha E)^3 x = 0$$

Имеют место следующие соотношения:

$$H_1 \subset H_2 \subset H_3, \mathrm{dim} H_k = k, \; g_1 \in H_1, \; g_2 \in H_2, \; g_3 \in H_3$$

Так как g_1, g_2, g_3 - базис, то

$$g_2 \notin H_1, \; g_3 \notin H_2$$

Итак, для нахождения жорданова базиса в данном примере следует найти H_1, H_2, H_3, выбрать вектор g_3 из $H_3 \setminus H_2$ затем вычислить g_2 и g_1 по формулам (1)

Пример 2. Известно, что матрица A подобна матрице

$$\mathrm{G}=\begin{pmatrix}\alpha & 0 & 0\\ 0 & \alpha & 1\\ 0 & 0 & \alpha\end{pmatrix}.$$

Найти жорданов базис.

Также как в предыдущем примере рассмотрим подпространства

$$\mathrm{H}_1:(\mathrm{A}-\alpha\mathrm{E})\mathrm{x}=0 \quad \mathrm{H}_2:(\mathrm{A}-\alpha\mathrm{E})^2\mathrm{x}=0 \quad \mathrm{H}_3:(\mathrm{A}-\alpha\mathrm{E})^3\mathrm{x}=0.$$

Имеют место следующие соотношения:

$$\mathrm{H}_1\subset\mathrm{H}_2=\mathrm{H}_3, \mathrm{dim}\mathrm{H}_1=2\ , \mathrm{dim}\mathrm{H}_2=3\ , \mathrm{g}_1,\mathrm{g}_2\in\mathrm{H}_1\ , \mathrm{g}_3\in\mathrm{H}_2.$$

Так как $\mathrm{g}_1,\mathrm{g}_2,\mathrm{g}_3$ - базис, то $\mathrm{g}_3\notin\mathrm{H}_1$.

Итак, для нахождения жорданова базиса в данном примере следует найти $\mathrm{H}_1,\mathrm{H}_2$, выбрать вектор g_3 из $\mathrm{H}_2\setminus\mathrm{H}_1$, затем вычислить g_2 и в качестве g_1 выбрать любой вектор из H_1, не пропорциональный вектору g_2.

Общий метод. Определить собственные числа $\lambda_1,..,\lambda_\mathrm{s}$.

Выбирая в качестве α поочередно каждое из собственных чисел, выполнить следующие действия.

Найти $\mathrm{H}_\mathrm{i}=\ker(\mathrm{A}-\alpha\mathrm{E})^\mathrm{i}$, $\mathrm{i}=1,..,\mathrm{r}$, где $\mathrm{r}=\min\{\mathrm{k}|\mathrm{H}_\mathrm{k}=\mathrm{H}_{\mathrm{k}+1}\}$ Заметим, что при $\alpha=\lambda_\mathrm{i}$ H_r совпадает с V_i из теоремы.

Составить таблицу вида

$$\begin{array}{ccccccc}
a_1 & \dots & a_{s_1} & & & & \\
\underbrace{(A-\alpha E)a_1}_{b_1} & \dots & \underbrace{(A-\alpha E)a_{s_1}}_{b_{s_1}} & \underbrace{\mathrm{b}_{\mathrm{s}_1+1}\ \dots\ \mathrm{b}_{\mathrm{s}_2}}_{SP_1} & & & \\
\dots & \dots & \dots & \dots & \dots & \dots & \\
\underbrace{(A-\alpha E)^{r-1}a_1}_{c_1} & \dots & \underbrace{(A-\alpha E)^{r-1}a_{s_1}}_{c_{s_1}} & \underbrace{(A-\alpha E)^{r-2}b_{s_1+1}}_{c_{s_1+1}} & \dots & \underbrace{(A-\alpha E)^{r-2}b_{s_2}}_{c_{s_2}} & \underbrace{\dots\ \mathrm{c}_{\mathrm{s}_\mathrm{r}}}_{SP_{r-1}}
\end{array}$$

где первая сверху строка содержит линейно независимые векторы, для которых выполняется равенство

$$\mathrm{H}_\mathrm{r}=\mathrm{H}_{\mathrm{r}-1}\oplus\mathrm{L}(\mathrm{a}_1,...,\mathrm{a}_{\mathrm{s}_1}), \qquad (1)$$

вторая строка содержит линейно независимые векторы, для которых

$$\mathrm{H}_{\mathrm{r}-1}=\mathrm{H}_{\mathrm{r}-2}\oplus\mathrm{L}(\mathrm{b}_1,...,\mathrm{b}_{\mathrm{s}_2}) \qquad (2)$$

и т.д.. Последняя строка содержит базис H_1, так, что $\mathrm{s}_\mathrm{r}=\mathrm{dim}\mathrm{H}_1$. Списки $\mathrm{SP}_1,...,\mathrm{SP}_{\mathrm{r}-1}$ могут быть пустыми.

Покажем, что построение этой таблицы, главной особенностью которой являются свойства $(1),(2),..$, возможно.

1. Так как $H_{r-1} \subset H_r$, то в верхней строке можно выписать любой набор векторов, дополняющих базис H_{r-1} до базиса H_r.

2. Векторы $b_1, ..., b_{s_1}$ определяются ранее выбранными векторами, поэтому формирование второй строки возможно тогда и только тогда, когда $L(b_1, ..., b_{s_1}) \cap H_{r-2} = \{0\}$. Это равенство справедливо так как $\mu_1 b_1 + ... + \mu_{s_1} b_{s_1} \in H_{r-2} \to \mu_1 a_1 + ... + \mu_{s_1} a_{s_1} \in H_{r-1} \to \mu_1 = ... = \mu_{s_1} = 0$. Таким образом, можно построить набор $b_1, ...$, для которого выполняется условие (2).

Структура последующих строк таблицы такая же как и у второй, поэтому приведенное в пункте 2 рассуждение применимо и далее.(Можно доказать по индукции.)

Так как

$$H_r = L(a_1, ..., a_{s_1}) \oplus L(b_1, ..., b_{s_2}) ... \oplus L(c_1, ..., c_{s_m}),$$

то векторы таблицы образуют базис H_r.

Для того,чтобы получить именно жорданов базис, надо расположить их в следующем порядке: $c_1, ..b_1, a_1$,
$c_2, .., b_2, a_2, ...$, то есть, обходя столбцы таблицы слева направо , а каждый столбец - снизу вверх.

При этом выбор последовательности столбцов не имеет принципиального значения, но в каждом из них векторы следует нумеровать строго снизу вверх.

Жорданова форма содержит s_1 клеток размера r, $s_2 - s_1$ клеток размера $r - 1$ и т.д.

Фробениусова форма матрицы.

Фробениусовой клеткой называется матрица вида

$$F(a_1, .., a_n) = \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

$F - \lambda E$ имеет следующие инвариантные множители: $e_1 = .. = e_{n-1}, e_n = \lambda^n - a_1 \lambda^{n-1} - .. - a_n$.

Утверждение 10. Пусть A квадратная матрица, $e_i(\lambda) = \lambda^{k_i} + a_{1i}\lambda^{k_i - 1} + ... + a_{ik_i}, i = 1, ..., s$ - инвариантные множители ее характеристической матрицы, тогда A подобна фробениусовой матрице

$$\mathrm{diag}(F(-a_{11} ... - a_{1k_1}), ..., F(-a_{s1} ... - a_{sk_s})).$$

Нахождение характеристического уравнения.

Метод Данилевского. Находится блочно-треугольная матрица, в которой на диагонали расположены фробениусовы клетки.

1. Если $a_{n\,n-1} \neq 0$, то составляем матрицу

$$P = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn-1} & a_{nn} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

и обратную к ней

$$P^{-1} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ -\frac{a_{n1}}{a_{nn-1}} & -\frac{a_{n2}}{a_{nn-1}} & \dots & \frac{1}{a_{nn-1}} & -\frac{a_{n2}}{a_{nn-1}} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Вычисляем матрицу A^1, подобную исходной матрице.

$$A^1 = PAP^{-1} = \begin{pmatrix} a^1_{11} & a^1_{12} & \dots & a^1_{1n-1} & a^1_{1n} \\ a'_{21} & a^1_{22} & \dots & a^1_{2n-1} & a^1_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a^1_{n-11} & a^1_{n-12} & \dots & a^1_{n-1n-1} & a^1_{n-1n} \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Последняя строка такая же как у матрицы Фробениуса. Если $a^1_{n-1n-2} \neq 0$, то находим

$$P = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a'_{n-11} & a'_{n-12} & \dots & a'_{n-1n-2} & a'_{n-1n-1} & a'_{n-1n} \\ 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix},$$

обратную к ней, вычисляем матрицу $A^2 = P^{-1}A^1P$ с элементами a^2_{ij} и так далее.

2. Если на некотором шаге оказалось, что $a^k_{n-k\;n-k-1} = 0$, но $\exists\, j < n-k-1$ такой,что $a^k_{n-k\;j} \neq 0$, то надо переставить местами j и n-k-1 строки, затем j и n-k-1 столбцы (эта операция равносильна перестановке базисных векторов). Получится матрица подобная исходной, переходим к 1.

3. Если на некотором шаге $a^k_{n-k\,j} = 0$ $\forall j < n-k$, то матрица имеет вид $\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$, где B и D квадратные матрицы, причем D фробениусова матрица, поэтому задача сводится к вычислению характеристического многочлена для B.

Пример 1. Найти характеристический многочлен для матрицы

$$A = \begin{pmatrix} 4 & -3 & 1 & 2 \\ 5 & -8 & 5 & 4 \\ 6 & -12 & 8 & 5 \\ 1 & -3 & 2 & 2 \end{pmatrix}$$

Решение. Для того, чтобы обойтись при вычислениях без дробей переставляем местами 1 и 3 столбцы, 1 и 3 строки

$$\begin{pmatrix} 1 & -3 & 4 & 2 \\ 5 & -8 & 5 & 4 \\ 8 & -12 & 6 & 5 \\ 2 & -3 & 1 & 2 \end{pmatrix} \to \begin{pmatrix} 8 & -12 & 6 & 5 \\ 5 & -8 & 5 & 4 \\ 1 & -3 & 4 & 2 \\ 2 & -3 & 1 & 2 \end{pmatrix}.$$

Следуя алгоритму, получаем

$$AP^{-1} = \begin{pmatrix} -4 & 6 & 6 & -7 \\ -5 & 7 & 5 & -6 \\ -7 & 9 & 4 & -6 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad A^1 = \begin{pmatrix} -4 & 6 & 6 & -7 \\ -5 & 7 & 5 & -6 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Характеристический многочлен есть $(\lambda^2 - 3\lambda + 2)^2$.

Метод Леверье. $s_i = \lambda_1^i + .. + \lambda_n^i = sp(A^i),\ i = 1, .., n$ Отсюда по формулам Ньютона находим коэффициенты характеристического многочлена

$$p_k = -\frac{1}{k}(s_k + p_1 s_{k-1} + ... + p_{k-1} s_1).$$

Аннулирующий многочлен.

Определение. Многочлен f(x) называется аннулирующим для матрицы A, если $f(A) = 0$.

Утверждение 11. (Теорема Гамильтона-Кэли) Каждая квадратная матрица является корнем своего характеристического многочлена.

Доказательство. Пусть $\Delta(\lambda) = \det(\lambda E - A)$, а $B(\lambda)$ – присоединенная матрица к $\lambda E - A$. Тогда справедливо равенство

$$(\lambda E - A)B(\lambda) = \Delta(\lambda)E. \tag{1}$$

Записав λ-матрицы $B(\lambda)$ и $\lambda E - A$ в виде матричных многочленов и сделав подстановку $\lambda = A$ получаем $\Delta(A) = 0$, что и требовалось.

Аннулирующий многочлен наименьшей степени называется минимальным.

Утверждение 12. Минимальным многочленом матрицы A является инвариантный множитель $e_n(\lambda)$ ее характеристической матрицы.

Доказательство. Сокращая обе части равенства (1) на $D_{n-1}(\lambda)$, получим

$$(\lambda E - A)B^1(\lambda) = e_n(\lambda)E, \qquad (2)$$

следовательно, $e_n(\lambda)$ - аннулирующий многочлен. Пусть $f(\lambda)$ - минимальный многочлен, тогда $e_n(\lambda) = f(\lambda)d(\lambda)$ и, согласно обобщенной теореме Безу, существует $S(\lambda)$ такая, что

$$(\lambda E - A)S(\lambda) = f(\lambda)E. \qquad (3)$$

Умножая обе части последнего равенства на $d(\lambda)$ и вычитая из (2), получим

$$(\lambda E - A)(B^1(\lambda) - d(\lambda)S(\lambda)) = 0.$$

Следовательно, $B^1(\lambda) = d(\lambda)S(\lambda)$, т.е. $d(\lambda)$ есть общий делитель элементов матрицы $B^1(\lambda)$ поэтому равен 1.