Лекции по фундаментальной и компьютерной алгебре

Печатала: Ткаченко Анастасия

8 июня 2018 г.

Теория полей.

Поле - множество с двумя алгебраическими операциями, которые обычно называют сложением и умножением, удовлетворяющие 10 аксиомам, а не формально: в поле определены все 4 арифметические операции. По сравнению с другими математическими объектами, полей очень мало.

Поля бывают конечными и и бесконечными. Конечные поля открыл Галуа. На этих полях построенна вся современная криптография.

Характеристика поля.

Определение. Минимальное натурально число k, называется характеристикой поля, если $\forall$ ненулевого $\in p$.

$$ka = a + a + \ldots + a = 0$$

А если такого k не существует, то говорят, что характеристика равна нулю. Пример. Поле Q, R, C, все эти проя имеют нулевую характеристику. Как связаны конечность и бесконечность с характеристикой ?

Теорема. Если поле имеет нулевую характеристику, то оно обязательно бесконечно и более того, содержит в качестве подполя поле рациональных чисел.

Доказательство. Пусть e - нейтральный элемент по умножению, т.е. мультипликативная единица. Т.к. поле имеет нулевую характеристику, то $e, e+e, \ldots, ne$ - всё это ненулевые элементы, более того попарно различные. Допустим для каких-то n, m $ne = me$, $n < m$. Т.к. это поле, то у элемента e есть обратный по сложению: $(m-n)e = 0$. Если это равенство умножить на любой a, то $m - n$ делится на характеристику, а значит характеристика ненулевая. Таким образом последовательность бесконечна и все её элементы разные, значит поле бесконечное.

Сконструируем внетри поля P поле Q. Элементу e будем ставить в соответствие 1, т.е.

$$e \mapsto 1$$

$$ne \mapsto n$$
$$\frac{ne}{me} \mapsto \frac{n}{m}$$

Легко проверить, что ... поля выполняется 10 аксиом и это поле по математическим свойствам совпадёт с полем Q.

Теорема. Если поле конечное, то его характеристика обязательно ненулевая.

Доказательство. Пусть e - нейтральный элемент по умножению. Рассмотрим последовательность e, 2e, 3e,. . . ,ne. Т.к. поле конечное, то в последовательности будут встречаться одинаковые элементы: $ne = me$, рассуждая как и выше вычитает $(m - n)e = 0$, значит характеристика ненулевая.

Замечание. Обратное утверждение неверно. Пример бесконечного поля характеристики 2:

$$Z_2 = \{0, 1\}$$

Построим кольцо многочленов. Оно бесконечное, но характеристика = 2, а затем берём поле дробей $Z_2[x]$, оно тоже будет иметь характеристику 2.

Теорема о характеристике поля. Если характеристика ненулевая, то она обязательно является простым числом.

Доказательство. Пусть P - поле и k - его характеристика, т.е. $ke = 0$, где e - нейтральный по умножению. Пусть k - непростое число, т.е. раскладывается на два числа s и r: $k = s \cdot r$ $(s \cdot r) = \ldots$ - Умножение в кольце целых.

$$\ldots = (e + \ldots + e) \cdot (e + \ldots + e)$$

- Умножение в поле. Т.к. в поле нет делителей нуля, то $se = 0$ или $re = 0$. Допустим $se = 0$. Если s - непростое, то продолжим эту же процедуру. По основной теореме арифметики мы обязательно доберёмся до простого числа.

Пусть p - простое число. Существует ли поле с простой характеристикой.

Первая теорема Галуа. Для любого простого числа p, существует поля из p элементов, имеющие характеристику p.

Доказательство. Возьмём кольцо вычетов $Z_p = \{0, 1, \ldots, p-1\}$, т.к. оно коммутативное кольцо с единицей, то для того чтобы стать полем, нужно проверить наличие обратного по умножению: $0 < a < p$. Т.к. p - простое, то НОД(a,p)=1 и по следствию из алгоритма Евклида существуют u и v такие, что: $ua + vp = 1$ $ua = 1 - pv$. Т.е. остаток от деления на p делит $ua = 1$ в Z_p. Т.е. и обратный по умножению к a. Таким образом Z_p - это поле $GF(p)$.

Расширение полей.

Если поле P содержит поле F: $P > F$, то говорят, что F - подполе поля P, а P - расширение.

Первое утверждение. Поле P, является векторным пространством над полем F.

Доказательство. Пусть $a, b \in P$ $\alpha, p \in F$. Нужно проверить 4 аксиомы коммутативной группы, но ведь P - поле, значит она выполнены, и 4 аксиомы действия:

1. $\alpha(a+b) = \alpha a + \alpha b$ - Дистрибутивность (в данном случае).

2. $(\alpha+\beta)a = \alpha a + \alpha b$ - Тоже дистрибутивность.

3. $(\alpha\beta)a = \alpha(\beta a)$ - Ассоциативность умножения.

4. $1a = a$

Определение. Размерность пространства $dim_f P = \mid P : F \mid$, называется степенью расширения поля. Если размерность бесконечная, то расширение называется бесконечномерным. Если у нас есть последовательность расширений: $K > P > F$, то это называется башней расширений.

Теорема о башне конечных расширений. Пусть $K > P > F$ - башня конечных расширений, тогда размерность: $\mid K : F \mid = \mid K : P \mid \cdot \mid P : F \mid$

Доказательство. Пусть размерность $\mid K : P \mid = n$ и $\mid P : F \mid = m$
По определению размерности: поле K над полем P имеет базис из n элементов, а поле P над полем F из m элементов. Чтобы проверить $a_i b_i$ $i = 1$ $j = 1$ K над F, являются базисом $\mid K : F \mid$.
Нужно проверить:

1. Что они порождающее множество.

2. Что они линейно независимы.

По определению базиса $c \in K$ $c = \alpha_1 a_1 + \ldots + \alpha_n a_n$ $\alpha_i \in P$ А коэффициент из P, можно выразить через $b_1 \ldots b_n$
В итоге он выразится через $a_i b_i$ с коэффициентами из F. Докажем линейную независимость: пусть напротив, они линейно зависимы.

$$\sum_{i,j} \sigma_{ij} a_i b_j = 0$$

$$i, j \in F$$

Запишем эту сумму как линейную комбинацию с коэффициентами из

$$\sum_{i,j} a_i (\sigma_{ij} b_j) = 0$$

Т.к. a_i - линейно независимые, то отсюда $\Rightarrow \sum \sigma_{ij} b_j = 0$, но m и b_j, тоже линейно независимы, отсюда $\Rightarrow \sigma_{ij} = 0$.

Определение. Пусть P - некоторое конечное расширение поля рациональных чисел $P > Q$. Число α, называется алгебраическим, если оно является корнем некоторого многочлена с целыми коэффициентами. Если

не является, то трансцендентное. Алгебраических чисел, счётное число, т.к. назых многочленом с целыми коэффициентами, счётное число.

В конце 19 века было доказано, что pi и e - трансцендентные.

Теорема. Если P - конечное расширение поля Q, то все его элементы - алгебраические числа.

Доказательство. $a \in P \mid P : Q \mid = n$, то существует $\alpha_i \in Q$
Т.к. элементов $n + 1$, а разерность пространвства n, то они должны быть линейно зависимы, т.е.

$$\alpha_0 + \alpha_1 a + \ldots + \alpha_n a_n = 0$$

Находим НОК знаменателей, умножаем на него обе части и получаем многочлен с целыми коэффициентами.

Замечание. Конечное расширение всегда алгебраическое, но среди алгебраических расширений есть и бесконечные.

Поле разложения.

Многочлен называется неприводимым над полем P, если он не разлагается в произведение многочленов меньшей степени. Простые числа и неприводимые многочлены - это ...

Пусть P - произвольное поле. Возьмём многочлен f(x):

$$Pf(x) \in P[x]$$

Задача. Нужно построить такое поле F, в котором наш многочлен разлагается на линейные множители. Это называется полем разложения.
Рассотрим множество остатков от деления на многочлен x:

$$Q_f\{g(x)|stepen \cdot g(x) < a \cdot f(x)\}$$

Идейно, ситуация повторяет кольцо вычетов Z_n, только вместо деления на n, берётся деление на многочлен. Зададим на множестве Q_f операции сложения и умножения. Сложение - это обычное сложение. Операция умножения - обычное умножение, а затем деление с остатком на $f(x)$. Также как и в кольце Z_n проверяется, что Q_f - это коммутативное кольцо, в котором единицей является 1 inP, а нулём $0 \in P$
Проверим, что Q_f - это на самом деле поле: как и в случае с Z_n, произвольный многочлен $g(x)$ и $f(x)$ НОД$(g(x), f(x)) = 1$. По следствию из алгоритма Евклида: существуют $u(x), v(x)$, такие, что:

$$u(x) \cdot g(x) + v(x) \cdot f(x) = 1$$

$$u(x) \cdot g(x) = 1 - v(x) \cdot f(x)$$

Значит остаток от деления на f(x), произведение $u(x) \cdot g(x) = 1$, т.е. $u(x) = g(x)^{-}1$ $Q_f > p$

Первый шаг. Для многочлена $f(x) \in P[x]$, x - это просто символ для записи многочлена, а в формуле f(x)=0, x - это остаток принадлежащий Q_f, т.е. конкретный многочлен. Из чисто методических соображений: этот вновь приобретённый корень, чтобы в одном тексте на использовать один и тот же символ в двух разных формулах, этот остаток x, обозначим как α: $f(\alpha) = 0$, тогда:

$$Q_f = \{g(\alpha) | stepen\ g < stepen\ f\}$$

Добавим один корень - это первый шаг.

Второй шаг. $Q_f\ f(x) = Q_f[x] \to (x - \alpha)^k \cdot g(x)$
Этот $g(x)$, разлагаем на неприводимые множители и к этим множителям применяем первый шаг. Добавим корни β, γ и т.д. В конце концов $f(x)$ разложится на множители.

Пример. Пусть поле P - поле действительных чисел, а $f(x) = x^2 + 1$, т.к. $f(x)$ не имеет корней, то он неприводим.

$$Q_{x^2+1} = \{a, ax + b | a, b \in R\}$$

Чтобы не менять традицию, поле остатков Q_{x^2+1}, будем обозначать, используя вместо x, символ i.
$\alpha^2 + 1 = 0$
$\alpha^2 = -1$
$i = \sqrt{-1}$

$$Q_{x^2+1} = \{a + ib | a, b \in R\}$$

$$(a + ib)(a_1 + ib_1) = \alpha a_1 + i(ab_1 + b_1 a)$$

Для поля разложения Q_{x^2+1}, есть специальное обозначение - C (Поле комплексных чисел).

Определение C. $C = \{a + bi | i^2 = -1\ a, b \in R\}$
C - рассмотренное как векторное пространство над полем P, имеет размерность 2 и базис - единицу.
$Z = a + ib$, a - действительная часть, i - мнимая.
Если есть ещё число $Z_1 = a_1 + ib_1$, тоих сумма будет суммой векторов: $Z + Z_1 = (a + a_1) + i + (b + b_1)$. Если изменить знак: $a - ib = \bar{Z}$, то получим сопряжённое число. Сумма $Z + Z_1 = a \in R$, будет действительным числом.

$$Z \cdot \bar{Z}_2 = (a + bi)(a - bi) = a^2 - i^2 b^2 = a^2 + b^2 \in R$$

$$|Z| = \sqrt{Z\bar{Z}} = a^2 + b^2$$

Упражнение. Проверить свойства сопряжённого.

$$Z \bar{\cdot} Z_1 = \bar{Z} \cdot \bar{Z}_1$$

$$Z \bar{+} Z_1 = \bar{Z} + \bar{Z}_1$$

Нахождение обратного по умножению.

$$Z \cdot \bar{Z} = a^2 + b^2$$

$$\frac{Z \cdot \bar{Z}}{a^2 + b^2} = 1 \Rightarrow Z^{-1} = \frac{\bar{Z}}{Z \cdot \bar{Z}}$$

$z \cdot \bar{z} = a^2 + b^2$ - действительное.

Комплексные числа

$$z = a + ib$$

РИСУНОК

Декартова(прямоугольная) система координат, удобна для графического изображения двумерных векторов. Горизонтальная ось будет называться действительной, а вертикальная - мнимой. В декартовой системе координат, хорошо моделируется сложение комплексных чисел - это сложение векторов.

Определение. Полярной системой координат, называют направленный луч с началом в точке O, которое называется началом координат. Координатные точки Z, однозначно определяются полярным углом φ(против часовой стрелки), $\varphi \in [0; 2\pi)$ и полярным радиусом ρ. (φ, ρ) РИСУНОК

Чтобы установить связь между этими системами, совместим полярную и декартову системы координат на одном рисунке. РИСУНОК

Пусть даны полярные координаты, выразим через них декартовы:

$$a = \rho \cdot cos\varphi$$

$$a = \rho \cdot sin\varphi$$

$$z = \rho(cos\varphi + i \cdot sin\varphi)$$

Это называется тригонометрической записью числа. Обратно:

$$\rho = \sqrt{a^2 + b^2}$$

$$sin\varphi = \frac{b}{\sqrt{a^2 + b^2}}$$

$$\varphi = arcsin\frac{b}{\sqrt{a^2 + b^2}}$$

Ещё необходимо знать чему равен косинус(или хотябы его знак), чтобы определительв какой четверти находится угол.

Применение. Пусть дано два комплексных числа:

$$z_1 = \rho_1(cos\varphi_1 + isin\varphi_1)$$

$$z_2 = \rho_2(cos\varphi_2 + isin\varphi_2)$$

$$z_1 \cdot z_2 = \rho_1\rho_2[(cos\varphi_c os\varphi_2 - sin\varphi_1 sin\varphi_2) + i(cos\varphi_1 sin\varphi_2 + cos\varphi_2 sin\varphi_1)] =$$

$$= \rho_1\rho_2(cos(\varphi_1 + \varphi_2) + isin(\varphi_1\varphi_2))$$

Геометрический смысл умножения. При умножении комплексных чисел, их модули перемножаются, а углы складываются.

Пусть мы хотим найти степень комплесного числа:

$$z = \rho(cos\varphi + isin\varphi$$

$$z = a + ib$$

$$z^n = (a+ib)^n = a^n - C_n^2 a^{n-2}b^2 + C_n^4 a^{n-4}b^4 -$$

...

Возведём в n степень:

$$z^n = \rho(cos\varphi + i \cdot sin\varphi)^n = \rho^n(cos(n\varphi) + i \cdot sin(n\varphi))$$

$$\sqrt[n]{z} = \sqrt[n]{a+ib}$$

При извлечении корней, декартовы координаты, также уместны как "банный лист в антарктиде".

$$\sqrt[n]{z} = \sqrt[n]{\rho^n} \cdot \sqrt{cos\varphi + i \cdot sin\varphi}$$

Т.к. ρ - положительное, действительное число, то под корнем тоже понимают положительное действительное число и называют арифметическим числом.

$$z_1 = \cos\psi + i\sin\psi$$

Т.к.

$$z_1^n = \cos\varphi + \sin\varphi$$

$$n\psi = \varphi \Rightarrow \psi = \frac{varphi}{n}$$

Замечание. Т.к. sin cos - периодичные и этот период равен 2π, то кроме этого базового решения будет ещё $n-1$ решение

$$\psi = \frac{\varphi + 2\pi k}{n}$$

$$k = 0, 1 \ldots n-1$$

Вывод: формула Абрахима де Муавра.

$$\sqrt[n]{z} = \sqrt[n]{\rho}(\cos\psi + i\sin\psi)$$

$$\psi = \frac{\varphi + 2\pi k}{n}$$

$$k = 0, 1 \ldots n-1$$

Частный случай.

Пример. Пусть дано комплексное

$$z = 1 + i \cdot 0 = 1 \cdot (\cos 0 + i \cdot \sin 0)$$

$$\sqrt[n]{1} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$$

$$k = 0, 1 \dots n-1$$

$$\psi = \frac{2\pi}{n}$$

Корни n степени, являются веринами правильного n-уголника, у которого начальные вершины имеют координаты (1;0).

Определение. Поле P, называется алгебраически замкнутым, если любой многочлен с коэффициентами в этом поле, разлагается на линейные множители.

Другое определение. P - алгебраически замкнуто, если любой многочлен имеет этом поле хотя бы один корень.

Основная теорема алгебры.
Поле комплексных чисел, является алгебраически замкнутым.

Определение. Расширение поля P до поля F, называется алгебраическим, если любой элемент поля F, является многочленом с целыми коэффициентами из поля P, поэтому у поля комплексных чисел нет расширения.

Комплексные числа.

$P[x]$, как мы знаем - это кольцо евклидово, с евклидовой нормой

$$\rho(f(x)) = stepenf(x)$$

$$x_1, x_2 \dots x_n$$

Простые, называются неприводимыми

$$P[x_1 \dots x_n]$$

$$\sum_{i_1 \dots i_n}^{k} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$$

$$a_{i_1 \dots i_n} \in P$$

Т.к. множество многочленов, образует кольцо, то нужно ввести некоторые понятия, актуальные для всех колец.

Гомоморфизм и изоморфизм.

$$G - *;$$

$$H - \circ$$

$$\varphi : G \mapsto H$$

, отображение φ, называется гомоморфизмом, если для любого $g_1, g_2 \in G$

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2)$$

$G - *; H - \circ; K - +, *; L - \oplus$(На самом деле это плюс в кружочке), $\circ$

$$\varphi : K \mapsto L$$

Для любых $k_1, k_2 \in K$

$$\varphi(k_1 + k_2) = \varphi(k_1) \oplus \varphi(k_2)$$

$$\varphi(k_1 \cdot k_2) = \varphi(k_1) \circ \varphi(k_2)$$

Определение. Еслиотображение φ, является биекцией, то гомоморфизм φ, называется изоморфизмом.

Гомоморфизм = это интерпритация одних объектов терминами других объектов и других отношений.

Гомоморфизмы колец и идеалов.

Кольцо, является группой по сложению и полугруппой по умножению, и гомоморфизм сохраняет обе операции. Базовое в кольце - это операция сложения и прежде всего необходимо изучить гомоморфизм коммутативной группы по сложению.

Структура гомоморфизма групп ($\varphi : G \mapsto H$).

Определение. Ядром гомоморфизма φ, называется такое подмножество группы G, что

$$Ker\varphi = g \in G | \varphi(g) = e_H$$

Свойство 1. Ядро является подгруппой.
Докажем по критерию подгруппы: пусть

$$g_1, g_2 \in Ker\varphi$$

$$g_1 \cdot g_2 \in Ker\varphi$$

$$g_1^{-1} \in Ker\varphi$$

$$\varphi(g_1 g_2) = \varphi(g_1)(g_2) = e_H \cdot e_H = e_H$$

$\varphi(g_1 g_2)$ - умножение в группе G.
$\varphi(g_1)(g_2)$ - умножение в группе H.
По определению обратного элемента:

$$g_1 \cdot g_1^{-1} = e_G$$

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \in H$$

Т.к. H - группа, то у элемента $\varphi(e_G)$, есть обратный. Умножаем на него обе части равенства. $\varphi(e_G) = e_H$
Таким образом: единичный переъодит в единичный.

$$e_H = \varphi(e_G) = \varphi(g_1 \cdot g_1^{-1}) = \varphi(g_1) \cdot \varphi(g_1^{-1}) \Rightarrow \varphi(g_1^{-1}) = e_H$$

Определение. Пусть G - группа, L - её подгруппа

$$\varphi : G \mapsto H$$

$$G \geq L$$

Знаки $\geq, \leq$, означают, что подмножество имеет согласованную структуру с объемлющим множеством.

Подгруппа, называется нормальной, если: $g^{-1}hg = h^g$, называется сопряжением элемента H с элементом L.

Другая формулировка. Нормальная подгруппа выдерживает все сопряжения в группе G.

Утверждение 2. Ядро, является нормальной подгруппой.

Доказательство. Пусть $f \in Ker\varphi$, а $g \in G$. Нужно проверить, что $\varphi(g^{-1}fg) = e_H$
По определению гомоморфизма:

$$\varphi(g^{-1}fg) = \varphi(g^{-1}\varphi(f)\varphi(g) = \varphi(g)^{-1}\varphi(f)\varphi(g) =$$

, т.к. при гомоморфизме обратный элемент переходит в обратный, то:

$$= \varphi(g)^{-1}e_H\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_H$$

Группа, называется простой, если в ней нет нетривиальных нормальных подгрупп. Простая группа - это единичная и вся группа. Основная задача теории подгрупп ...
Бесконечные групп не описаны. В теории конечных групп задача "вроде"решена. Было найдено 17 бесконечных серий простых групп и 26 внесерийных, спорадических групп.

Фактор кольцо, фактор группа.

Пусть $G \geq H$(только вместо $>$, треугольник), обозначает нормальную подгруппу.

$$gH = g \cdot h | G \in H$$

, называют смешанными классами. Смешанные классы не пересекаются и имеют бесконечную мощность.

$$h \mapsto g \cdot h$$

На множестве смежных классов, введём операцию умножения:

$$g_1H \cdot g_2H = (g_1g_2)H$$

В смежном классе ... элемент g, называется представителем. В качестве предствителя можно взять любой элемент этого смежного класса.
Необходимо проверить корректность задания операции, т.к. она определена через представителей. Убедимся, что заменив представителей мы получим тот же результат.

$$g_1 H = g_1'$$

$$g_2 H = g_2'$$

,где

$$g_1' = g_1 h_1 \in H$$

$$g_2' = g_2 h_2 \in H$$

$$(g_1 h_1)(g_2 h_2)H = (g_1 \cdot g_2)(g_2^{-1} h_1 g_2) h_2 H = g_1 g_2 H$$

Т.к. группа нормальная, то $g_2^{-1} h_1 g_2 \in H$, $h1 = h3$,
для любых $h \in H$ $h \cdot H = H$

Определение. Группа, элементами которой являются смежные классы, а операция задана как указано выше, называется фактор группой (G/H).

Ассоциативность следует из ассоциативности ... $gH^{-1} = g^{-1}H$. Когда мы целое множество воспринимаем как единичный объект, стандартная идея при ... $G/H = L$. Говорят, что группа G, является расширением группы H, при помощи группы L. Всё можно свестик простым группам. Даже зная все простые группы...

Идеалы и фактор кольца.

K$\geq$ L, L - подкольцо и подгруппа по сложению. Подкольцо, называется идеалом, если для любых $k \in K$ $k \cdot L = \{k \cdot l | \ldots\}$, т.е. L выдерживает умножение и слева и справа. Идеал - это обобщение нуля.

$$K + L$$

$$k \in K$$

$$(k_1 + L) + (k_2 + L) = (k_1 + k_2)L$$

$$(k_1 + L) \cdot (k_2 + L) = k_1 k_2 + L$$

Т.к. и здесь операции задаются при помощи представителей, то нужно проверить корректность:

$$k_1' + L = k_1 + L$$

$$k_2' + L = k_2 + L$$

6 марта. K $I \Delta K$, I - идеал.
$I \cdot K \leq I$
$I + I = I$

Если кольцо не коммутативное, то различают левый и правый идеалы. Идеал, называется максимальным, если он не содержится ни в каком большем идеале. В дальнейшем будем считать, что наше кольцо коммутативно.

$$K + I = \{k + i | i \in I\}$$

, называется смежным классом по идеалу, а множество всех смежных идеалов с заданными на них операциями сложения и умножения, называется фактор кольцом.

Пример. В качестве кольца K, возьмём K/I

$$nZ = \{0, \pm n, \pm 2n \dots\}$$

$$Z/nZ = Z_n = \{0, 1 \dots n-1\}$$

Теория разрешения уравнений, построения полей расширений, основывается на теории идеалов.

Определение. Идеал, порождающийся одним элементом, называется главным.

Теорема. Любое евклидово кольцо, является кольцом главных идеалов.

Доказательство. Пусть у нас есть произвольный идеал, состоящий из $I = \{i_1, i_{2i} \dots i_n\}$, необходимо выбрать такой элемент i, через который можно выразить все остальные i. Т.к. кольцо евклидово, то в нём любые два элемента имеют НОД:

$$d = NOD(i_1, i_2)$$

$$i_1 = d \cdot i'_1$$

$$i_2 = d \cdot i'_2$$

Таким образом i_1 и i_2, попадут в идеал порождённый d.

Ответ. Порождающим элементом I, будет НОД всех этих элементов.
Пусть P - некоторое поле и f(x) - неприводимый многочлен над этим полем. Требуется построить такое поле, в котором этот многочлен будет иметь хотябы один корень. В кольце многочленов P[x], рассмотрим идеал I, порождённый этим многочленом

$$I = ug(f(x)) = \{f(x) \cdot g(x) | g(x) GP(x)\}$$

, это δ из всех кратных многочлена f(x). Т.к. многочлен неприводим, то идеал порождённый этим многочленом, будет максимальным, и т.к. многочлену f(x) соответствует ноль в этом кольце, это и означает, что корень ноль. При рассуждениях, когда брались остатки от деления на многочлен, мы также работали со смежными классами.

Основная теорема алгебры. Поле комплексных чисел, является алгебраически замкнутым, т.е. в нём любой многочлен с целыми коэффициентами раскладывается на простые множители.

Симметрические многочлены и теорема Виета.

Пусть P - поле. Рассмотрим кольцо многочленов от n перестановочных переменных:

$$P[x_1, x_2 \dots x_n]$$

$$f(x_1, x_n) = \sum \alpha_{I_1 \dots I_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$$

Каждое такое слагаемое, называется мономом.

Пример. $x_1^5 x_2^7 x_3^{16}$ - моном общей степени 28.

Когда у нас всего одна переменная, то мономы можно легко сравнить, но когда переменных несколько, то упорядочить их можно очень многими способами.

Способ упорядочения, который принят в словарях, называется лексикографическим. Допустим на множестве мономо, мы ввели линейное упорядочение. Самый большой моном, в смысле этого упорядочени, называется старшим мономом.

Второе условие. Упорядочение должно быть таким , чтобы количество мономов меньше старшего было конечно. В начале будем сравнивать мономы по общей степени, а когда степень совпадёт, то лексико-графический.

Определение. Многочлен от n переменных, называется симметрическим, если он не изменяется при любой перестановке входящих в него символов.

Пример.

$$S_1 = x_1 + x_2 \dots x_n$$

$$S_2 = x_1 x_2 + x_1 x_3 + \dots x_{n1} x_n$$

$$S_n = \sum \dots x_i x_j x_k$$

, их называют элементарным симметрическим многочленом.

Теорема. Любой симметрический многочлен, может быть выражен через элементарные симметрические.

Теорема Виета. Пусть $x_1, x_2 \dots x_n$ - корни многочлена $f(x_n)$

Раскрывая скобки, получаем:

$$x^n - S_1 x^{n-1} + S_2 x^{n-2} \dots (-1)^n S_n$$

Коэффициентами при степенях многочлена, с точностью до знака, являются элементарные симметрические многочлены от его корней. Комбинируя теорему Виета и основную теорему ассиметрических многочленов, мы можем не находя корней многочлена, вычислить некоторые функции от этих корней.

Пример.

$$x^3 - 2017x + 1$$

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1 x_2 + x_1 x_2 + x_2 x_3) = \dots$$

Т.к. нам требуется изучать перестановки переменных, необходимо ввести обозначение и терминологию из теории групп перестановок.

Записывают двумя способами.
1. Табличная запись. НАДО СДЕЛАТЬ МАТРИЦУ

$$\pi =$$

Произведение перестановок - это их обычная суперпозиция как отображение. Полная талбичная запись, крайне расточительна. **2. Запись в виде циклов.** НАДО СДЕЛАТЬ ДВЕ ПЕРЕСТАНОВКИ
Принято циклы длиной 1, не записывать, а длиной 2, называют транспозицией.

13 марта 2017г. Базис Грёбнера - это обобщение на случай нескольких переменных.

Определение определителя. По индукции: НАПИСАТЬ ОПРЕДЕЛИТЕЛЬ $A =$

$$n = 1$$

$$A = (a_{11}) \neq a_{11}$$

$$|A| = a_{11}$$

Пусть det матрицы $n-1 \times n-1$, уже введён. Дадим определение разложению по первой строке:

$$|A| = (-a)^{1+1} a_{11} |A_{11}| + (-1)^{1+2} a_{12} |A_{12}| + \dots (-1)^{1+n} a_{1n} |A_{1n}|$$

Написанные маленькие матрицы, называются минорами.

Детерминанты. По индукции: $n = 1$ $|A| = a_{11}$

$$|A| = \sum_{i=1}^{n} (-1)^{1+i} a_{1i} |A_{1i}|$$

1 Вопрос. Как вычислить этот определитель ?
2 Вопрос. Сколько в нём слагаемых ?
3 Вопрос. Какова структура этих слагаемых ?
$n = 1$ - 1
$n = 2$ - 2
$n = 3$ - $3! = 6$, тогда по индукции:

$$(n-1)!$$

$$n : n \cdot (n-1)! = n!$$

Вывод. Определитель n-ого порядка, состоит из n! слагаемых, каждый из которых, является произведением n элементов, половина из них с плюсом, половина с минусом.

Сложность вычисления. Примем сложность сложения за 1, а умножения за t. $t \gg 1$ - намного больше. $t \approx 10^8$

Какова сложность вычисления определителя n-ого порядка ?
Сложение: $n! \cdot 1$
Умножение: $(n-1) \cdot n! \cdot t$
При $n = 1000$, матрица доставки фирмы "Магнит прямое вычисление детерминанта, исключено даже на суперкомпьютерах.

Техническая часть. Как вычислять детерминант ? Перечесление его свойств. Матрица, называется верхней треугольной, если она имеет следующий вид: МАТРИЦА

Используя индуктивное определение детерминанта несложно вычислить, что определитель этой матрицы, равен произведению диагональных эдементов. Это наблюдение подсказывает нам способ нахождения детерминанта, а именно при помощи элементарных преобразований, по методу Гаусса, привести матрицу к диагональному виду.

Вопрос. Что будет происходить с детерминантом, если к нему применять элементарные преобразования строк ?

1 Элементарное преоразование. Умножение строки на элемент α. Если эта строка - первая, то все коэффициенты a_{1i}, будут умножены на α, а значит и весь определитель умножится на α.

1 Свойство определителя. При умножении строки или столбца на элемент α, определитель умножается на α.

2 Элементарное преоразование. К i-ой строке прибавляют h-ую, умноженную на α.

2 Свойство определителя. При втором элементарном преоразовании, определитель не изменяется.

3 Свойство определителя. Если две строки/столбца поменять местами, то определитель сменит знак.

4 Свойство определителя. Если в матрице есть две одинаковые строки, то её определитель равен нулю.

Доказательство 4 свойства. Поменяв местами одинаковые строки, мы изменим знак определителя, а так как строки одинаковые, то знак не изменится, и если характеристика $\neq 0$, то определитель равен 0.

Интрига!!! А если характеристика равна 2 ?

Ответ. Определитель тоже равен нулю, но нужно изменить способ доказательства.

Определение. Матрица, называется полуспавшейся, если она имеет вид: ДВЕ МАТРИЦЫ

5 Свойство определителя. Определитель полураспавшейся матрицы равен $|A| = |B| \cdot |C|$

6 Свойство определителя. Определитель произведения матриц, равен произведению определителей. ($|AB| = |A| \cdot |B|$)
Другими словами: $det : M_n(p) \to p^*$, является гомоморфизмом группы матриц по умножению в мультипликативную группу поля.

7 Свойство определителя (Иногда берётся как определение детерминанта. Определитель - это сумма n! слагаемых, каждый из которых, является произведением n элементов, взятых по одному из каждой строки,

а знак определяется чётностью перестановки, заданой номерами строк и столбцов, из которых взяты эти элементы.

$$|A| = \sum_{\pi \in S_n} (-1)^{chetnost(\pi)} a_{1i_1} a_{2i_2} \dots a_{ni_n}$$

$$\pi =$$

ПЕРЕСТАНОВКА

8 Свойство определителя. Определитель матрицы, равен определителю транспонированной матрицы: $|A| = |A^t|$

Группы перестановок. Чётные и нечётные перестановки.

$\pi =$ ПЕРЕСТАНОВКА

Определение. Беспорядком, называется случай, когда меньший элемент, находится после большего. S_1 - количество беспорядков для 1
S_2 - количество беспорядков для 2 и т.д.

Определение. Если количество беспорядков чётное, то перестановка называется чётной и наоборот.

Определение. Перестановка, называется транспозицией, если это перестановка ровно двух элементов.

Упражнение. Пусть π - некоторая перестановка, проверим, что π, умноженное на транспозицию, изменяет чётность перестановки.

Произведение чётных перестановок - чётно.

Произведение двух нечётных перестановок - чётно.

Произведение чётной и нечётной перестановок - нечётно.

Доказательство. Чтобы воспользоваться 1 и 2 упражнениями, необходимо произвольную перестановку, представить как произведение транспозиций.

1 Шаг. ПЕРЕСТАНОВКА (16745)(23)
Разложим её в произведение независимых циклов.

Определение. Циклы - независимые, если они не имеют общих элементов.

2 Шаг. Чтобы разложить всю перестановку, достаточно разложить каждый цикл. Не теряя общности: $(12 \dots n) = (12)(13)(14) \dots (1n)$

Вывод. Каждая перестановка, есть произведение траспозиций, и если циклов n, то транспозиций будет $n - 1$, так как каждая транспозиция, в смысле чётности - это -1, то получаем

$$1 \cdot (-1) = -1$$

$$-1 \cdot (-1) = 1$$

и т.д.

Группы перестановок.

Определение. Любая биекция множества на себя, называется перестановкой, если множество состоит из n элементов, то группы перестановок обозначаю S_n и в этой группе будет n элементов, операция - суперпозиция отображений, а нейтральный элемент - i=ПЕРЕСТАНОВКА

Формы записи перестановок:

1. Табличная, в виде двух строк. Первая строка - сами n элементов, а вторая - их образы. Данная запись крайне не экономна и мало информативна.

2. В виде произведения независимых циклов.

Если цикл длины S, то его порядок равен S. Очевидно, что порядок двух перестановок, есть НОК. Т.к. транспозиция - нечётная перестановка и умножение на транспозицию меняет чётность, то...
Цикл длины n, имеет чётность $n-1$, поэтому если перестановка раскладывается на циклы $S_1 \dots S_k$

Перемножение перестановок в форме циклов и запись ответа в форме циклов. Как находить обратную перестановку при разложении на циклы ? Нужно найти обратный к каждому циклу. Чётные перестановки образуют подгруппу, обозначаемую A_n и эта подгруппа имеет индекс 2, т.е. всего 2 смежных класса(чётные и нечётные). Все группы A_n, являются простыми, а группа A_5 - это самая маленькая некоммутативная простая группа (60 элементов).

Доказательство свойств определителя. A=МАТРИЦА - развёрнутая форма определителя.

$$|A| = \sum_{\substack{\pi PERESTANOVKA \\ a_{1i_1}a_{2i_2}\dots a_{ni_n}}} (-1)$$

Определитель - сумма n! слагаемых, каждый из которых, является произведением n элементов, взятых по одному из каждой строки и каждого столбца, а знак определяется чётностью перестановки их индексов, т.е. половина их них положительные, половина отрицательные.

Доказательство(индукция по n).

База индукции: $n = 2$ ОПРЕДЕЛИТЕЛЬ= $a_{11}a_{22} - a_{21}a_{12}$

Предположение индукции: пусть для $n-1$ утверждение доказано. По определению детерминанта:

$$|A| = \sum_{i=1}^{n} (-1)^{1+i} a_{1i} A_{1i}$$

$|A_{1i}|$ - минор, когда у матрицы A, вычеркнуты 1 строка и i столбец. По предположению индукции: каждый минор, является суммой $(n-1)!$ слагаемых,

каждый из которых есть произведение $n-1$ элемента, взятых по одному, из каждой строки, начиная со 2 и каждого столбца, за исключением i, т.е. им не хватает...
Таким образом в нашей сумме, будет n! слагаемых, причём сомножители взяты по одному из каждой строки каждого столбца. ...
Фактически в минорах происходит перенумерация, т.е. переход к изоморфному объекту, а потом возвращение к исходному.

Вычислить количество беспорядков в первой формуле, потом во второй и добавить к ней 1 или -1. В первой формуле дополнительные беспорядки создаёт $i-1$, а во второй беспорядки добавляет -1^{i+1}.

Доказательство остальных свойств:

1. Если поменять две строки местами, то определитель изменит знак.

Доказательство. Пусть мы поменяли k и l строки, тогда в наших сомножителях поменяются k и l сомножители, т.е. перестановка π, умножится на транспозицию kl, которая нечётная и изменит знак и все слагаемые изменят знак.

2. Определитель транспонированной матрицы равен исходной.

Доказательство. При транспонировании, строки и столбцы меняются местами, значит и перестановка π, в сумме перейдёт в обратную, а обратная и исходная имеют одинаковую чётность, значит знак не изменится.

3. $|A \cdot B| = |A| \cdot |B|$

Доказательство. Рассмотрим матрицу $2n \times 2n$ ОПРЕДЕЛИТЕЛЬ МАТРИЦЫ $= |A| \cdot |B|$, т.к. эта матрица полураспавшеейся, то её определитель равен произведению диагональных клеток, осталось проверить, что он равен произведению $|A| \cdot |B|$. Элементарными преобразования строк, мы обнулим..., использую второе элементарное преобразование. При помощи $n+1$, обнуляем первый столбец, при помощи $n+2$ - второй, при помощи n - 2n столбец.
МАТРИЦ= - Чтобы сделать матрицу полураспавшейся, поменяем 1 столбец с $n+1$, 2 столбец с $n+2$, n столбец с $2n$. ПЕРЕНОС РАВНО= $(-1)^n$ ОПРЕДЕЛИТЕЛЬ, т.к. матрица полураспавшаяся, то получаем: $(-1)^n|AB| \cdot (-1)^n = |AB|$

$2^5 - 1$ Простое число, называется простым числом Мерсенна, если оно имеет вид $2^p - 1$. Если показатель - составное число, то разность $2^p - 1$, тоже будет составное, поэтому необходимым условием простоты, является простота показателя.
$2^{2n} + 1$ - Простые числа Ферма.

Определение. Графом, называется фигура, состоящая из точек - вершин и отрезков - рёбер.

Определение. Граф, называется полным, если в нём любые две вершины соединены ребром.
Граф - планарный (плоский), если он можеть изображён на плоскости без пересечения рёбер. Граф - двудольный, если множество его вершин разбивается на два подмножества, а рёбра соединяют только вершины из разынх подмножеств.
Пример непланарного графа: РИСУНОК.

Теорема. Граф непланарный $\leftrightarrow$, когда в нём есть подграф, изоморфный этому. Если граф не планарный, то электрическая сеть им заданная, погибнет от короткого замыкания. Любая деятельность и любая математическая система, может быть описана, как граф, вершинами которого являются ... системы, а их отношения - рёбрами

Если ребро от А к В, отличается от ребра из В в А, то граф, называется ориентированным. Граф, называется мультиграфом, если вершины могут быть соединены несколькими рёбрами. Мультиграф, называется нагруженным, если движение по рёбрам имеет некий вес (ценность). Практически любую ситуацию, можно смоделировать, как нагруженный мультиграф. **Разложение по i-ой строке. Свойства:**

1. Имеет место определитель:

$$|A| = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} |A_{ij}|$$

Доказательство. i-ую строку меняем с i-1, потому с i-2 и т.д. ... с 1. При каждой такой замене определитель меняет знак, таких замен i-1.

$$(-1)^{i-1}(-1)^1 = (-1)^i$$

2. Разложение по i-ому столбцу.

Упражнение. Написать формулу ...

Доказательство. С одной стороны, при транспонировании определитель не меняется, а с другой - столбцы становятся строками, и мы можем применить предыдущее свойство.

Определители специального вида:

1. Определитель Вандермонда: РИСУНОК $\neq 0$ $\leftrightarrow$, когда все иксы попарно различны.

Доказательство (Индукция по n).

База индукции: $n = 2$ ОПРЕДЕЛИТЕЛЬ $= x_2 - x_1$

Предположение индукции: пусть для n-1, утверждение доказано.

Шаг индукции: проверим утверждение для n. Избавимся от первой переменной. Предпоследнюю строку умножаем на x_1 и вычитаем из последней. Определитель при этом не меняется. РИСУНОК.

Раскладывая определитель по первому столбцу, у нас останется определитель Вандермонда степени $n - 1$.

2. Циркулянт: РИСУНОК

Каждая следующая строка, является сдвигом вправо на один элемент предыдущей строки. Е - корни из -1, т.е. $\sqrt[n]{-1}$.

$$f(x) = a_1 + a_2 x + \dots a_n x^{n-1}$$

Лучше всего считать, что определителем над полем комплексных чисел, т.к. поле комплексных чисел, все n корней, попарно различны.

Доказательство. Используется определитель Вандермонда. В=МАТРИЦА

$$2012^{2017}$$

, т.к. корни попарно различны, то определитель Вандермонда $\neq 0$. Умножение первой строки на первый столбец, даёт $f(E_1)$. ОПРЕДЕЛИТЕЛЬ
, т.к. вторая строка, является сдвигом первой, а ..., то вторая строка итоговой матрицы совпадёт с первой, а E - "выскочат наружу". Используя Элементарное преобразование ...= $f(E_1)f(E_2)\dots f(E_n)\cdot|B|$
По свойству, что определитель произведения, равен произведению определителей, получаем: $|AB| = |A|\cdot|B| = f(E_1)\dots f(E_n)\cdot|B|$, т.к. определитель B, не равен нулю, то сокращаем на него обе части равенства и получаем требуемое выражение.

Нахождение обратной матрицы - Формула Крамера.

Алгебраическое дополнение.

Запишем развёрнутое определение детерминанта:

$$|A| = \sum_{\pi=OPREDELITEL} (-1)^{chetnost\pi} a_{1i_1}a_{2i_2}\dots a_{ni_n}$$

Сумма n! слагаемых, каждый из которых, является произвдением n элементов, а знак зависит от чётности перестановки индекса. Рассмотрим этот определитель, как многочлен от n^2 переменных. Выберем все слагаемые, которые содержат в качестве сомножителя< элемент a_{ij}, таких слагаемых будет $(n-1)!$ Вынесем элемент a_{ij} за скобки, а всё, что получится в скобках, называется алгебраическим дополнением: $a_{ij}() = |A|_{ij}$.

Алгебраическое дополнение - это многочлен. Нахождение его вида, практически безнадёжная задача.

Свойства алгебраических дополнений:

1. Разложение определителя по 1 строке:

$$|A| = \sum_{i=1}^{n} a_{1i}|A|_{1i}$$

Из определений детерминанта и алгебраического дополнения, получаем такое разложение

$$|A| = \sum_{i=1}^{n} a_{1i}|A|_{1i}$$

.

2. Связь алгебраического дополнения с минором: $|A|_{ij} = (-1)^{i+j}|A_{ij}|$
Минор и алгебраическое дополнение совпадает с точностью до знака.

Доказательство. Напишем разложение определителя по i-ой строке по минорам, тогда при элементе a_{ij}, будет правая часть равенства. При разложении по i-ой строке по алгебраическим дополнениям, будет левая часть равенства.

3. О верности алгебраических дополнений своим элементам.

$$|A| = \sum_{\pi \in S_n}^{chetnost(\pi)} a_{1i_1} \dots a_{ni_n} =$$

ПЕРЕСТАНОВКА

$|A_{ij}|$ = Минор - матрица, у которой вычеркнута i-ая строка и j-ый столбец. $|A|_{ij}$ - Алгебраическое дополнение, если развёрнутое определение детерминанта рассматривать, как многочлен от n^2 элементов. После этого, выбрать все слагаемые, содержащие элементы aij (их $(n-1)!$ элементов), вынести этот сомножитель за скобку, то оставшийся в скобках многочлен, называется алгебраическим дополнением элемента a_{ij} и обозначается $|A|_{ij}$. Из определения алгебраического дополнения $\Rightarrow$

$$|A| = \sum_{k=1}^{n} a_{ik}|A|_{ik}$$

$$|A| = \sum_{k=1}^{n} (-1)^{i+k} a_{ik}|A_{ik}|$$

- Разложение по i-ой строке. Индукция по n из этих 2 разложений легко вынести. $|A|_{ik} = (-1)^{i+k}|A_{ik}|$, алгебраическое дополнение и минор отличаются только знаком.

Расшифровка:

1. Если матрица зафиксирована, то все n^2 элементов - некоторые числа, подставляя их в алгебраическое дополнение многочлена, получим число, которое будет связано с этим равенством.

2. На минор, используя развёрнутое определение детерминанта, можно смотреть, как на многочлен от $(n-1)^2$ элементов $\Rightarrow$ наше равенство, будет равенством многочленов.

1. - Равенство функций.

2. - Равенство многочленов.

Если многочлены равны, то и задаваемые ими функции равны, а обратнон - неверно (разные многочлены, могут задавать одну и туже функцию).

Основное свойство алгебраических дополнений.

$$\sum_{k=1}^{n} a_{ik} =$$

СИСТЕМА |A|, если i=j

0, если $i \neq j$

Если алгебраическое дополнение, умножается на свои элементы< то получается определитель, иначе - ноль.

Доказательство. Пусть $i = j$, тогда по определению алгебраического дополнения, получаем разложение по i-ой строке.

Пусть $i \neq j$, тогда разложение по i-ой строке матрицы A, в которой i-ая и j-ая строки совпадают $\Rightarrow$ определитель такой матрицы равен нулю.

Обратная матрица и правило Крамера.

Исторически детерминант, возник как ответ на вопрос, как по коэффициентам линейной системы, сразу написать ответ в общем случае это невозможно, но когда матрица имеет обратную по умножению.

$$A_x = b \Rightarrow x = A^{-1} \cdot b$$

Чтобы написать ответ, надо найти обратную матрицу.

1. Квадратная матрица A имеет обратную $\leftrightarrow$, когда её определитель не ноль. В случае, если матрица рассматривается над полем или над коммутативным кольцом, то имеем обратную $\leftrightarrow$, когда определитель, является обратным в кольце.

Пример. Над кольцом целых чисел матрица будет обратимой $\leftrightarrow$, когда её определитель равен ± 1.

Пример (Над кольцом). Z_{16}, когда детерминант - нечётное число до 15.

Доказательство. Пусть матрица a, задана над коммутативным кольцом A. Пусть она обратима и матрица B - ей обратная.

$$A \cdot B = E \Rightarrow det|AB| = 1$$

С одной стороны, т.к. детерминант - произведения матриц, равен произведению определителей, получаем: $|A| \cdot |B| = 1 \Rightarrow$ определитель A, является обратимым в кольце K. Мы докажем в одну сторону: если матрица обратима, тогда её определитель обратим. Пусть детерминант A - обратимый элемент кольца K. Мы явно построим обратимую матрицу.

$$A^{-1} = \frac{1}{|A|} \cdot$$

МАТРИЦА
Эта формула законна, т.к. определитель a, обратим. Остаётся проверить, что это обратная матрица.

Прямая проверка с использованием основного свойства алгебраического дополнения: $A \cdot A^{-1} = \frac{1}{|A|}$ МАТРИЦА

Замечание! Эта формула имеет теоретический характер, по ней вычислить обратную матрицу, размера n>4, невозможно. Оценим трудоёмкость вычисления по этой формуле: для матрицы размера $n \times n$, нужно будет вычислить $n62$ определителей $(n-1)(n-1)$ и один определитель $(n \times n)$.

Нахождение обратной матрицы по алгоритму Гаусса, равносильно нахождению двух определителей $n \times n$. Для нахождения определителей, базисов, решение СЛУ, самый экономный метод - метод Гаусса.

Правило Крамера. Если в формулу $x = A^{-1} \cdot b$, вместо A^{-1} записать формулу, то получится явное выражение для каждой переменной. Используем основное свойство алгебраических дополнений. $x_i = \frac{|A_i|}{A}$, $i = 1, 2 \ldots n$ $|A_i|$ - матрица A, где i-ый столбец заменён на столбец b.

Применение правила Крамера в вычислении, очень длительно, вместо одного определителя, находится (n+1). Детерминант, как отображение из кольца $n \times n$ над коммутативным кольцом k - само кольцо K. det $M_n(k) \to k$, при этом: det $|A \cdot B| = detA \cdot detB$ - это отображение, является гомоморфизмом мультипликативных групп. Если матрицу представить, как совокупность строк, то из свойства, что при смене строк местами, меняется знак определителя, мы получаем, что изображение поссасимметрично. При умножении строки на элемент, и определитель умножается на элемент. Если строку представить, как произведение двух строк, то определитель будет представлен линейно. Это применимо в любую сторону - полиссимметричность.

Определитель E матрицы = 1 - нормированность.

Абстрактное описание детерминанта. Если матрицу рассматривать, как совокупность строк, то det - полилинейное поссасимметрично-линейное отображение кольцо K, является гомоморфизмом мультипликативных групп матрицы n, кольца k. Отображение с таким свойством единственно.

Теория многочленов. Линейные отображения.

Пусть v, w - 2 вектора пространства над полем P.
$\varphi : v \to w$ $\alpha, \beta \in P$, для любых $v, w \in V$

$$\varphi(\alpha u + \beta v) = \alpha\varphi(u) + \beta\varphi(v)$$

- линейное/гомоморфизм линейного пространства.

$$\varphi : V \to w$$

- Можно определить сумму этих отображений ?

Множество линейных отображений образуют линейное пространство.
Пусть $e_1, e_2 \dots e_n$ - базис v
$f_1, f_2 \dots f_n$ - базис w
Т.к. отображение линейное, мы можем описать вектор:

$$v = \alpha e_1, \dots \alpha e_n$$

$$\varphi(v) = \alpha_1\varphi(e_1) + \dots \alpha_i\varphi(e_i)$$

Теорема. Линейное отображение однозначно определяется своим действием на базисных векторах. Т.к. пространство W, имеет размерность m, то каждый образ $\varphi(e_i)$, можно рассматривать, как m - размерный столбец.

$$[\varphi]_{m \times n} = (\varphi(e_1) \dots \varphi(e_n))$$

, у которой i-ым столбцом, является образ $\varphi(e_i)$, тогда координаты вектора $[\varphi(v)]$ - матрица $\varphi(e_i)$·координаты вектора. Т.к. $[\varphi]$, зависит от базисов, то она $[\varphi]^{e_1 \dots e_n}_{f_1 \dots f_n}$. Ненулевой вектор x, называется собственным вектором отображения φ, отвечающим собственным значениям x, если: $\varphi(x) = \alpha x$, $x = \bar{0}$.

Если существует базис из собственных векторов отображения φ, $\alpha_1 \dots \alpha_n$ - соответствующие собственным значениям, то базис из собственных векторов, имеет диагональный вид: $[\varphi]$ = МАТРИЦА

Базисы собственных векторов встречаются крайне редко.

90% математических приложений - это линейные методы: матрицы, системы и линейные отображения, интегрирование, дифференцирование и методы приближений - это, как правило, линейные отображения, т.к. любой процесс на малом отрезке времени, может быть описана, как линейное.Получается, при последовательном приближении, начинают рассматривать производные от процессов, затем производные от производных и т.д. и появляются ...(Ряды Тейлора).

Пусть v и w - два векторных пространства над одним и тем же полем. Отображение $\varphi : V \to W$, называется линейным, если оно является гомоморфизмом векторных пространств. При гомоморфизме, сохраняются все математические свойства объектов. Т.к. в векторном пространстве, есть сложение векторов и действие поля на вектора, то:

$$\forall v_1, v_2 \in V$$

$$\varphi(V_1 + V_2) = \varphi(V_1) + \varphi(V_2)$$

$\forall v \in V$ и $\forall \alpha \in p$

$$\varphi(\alpha v) = \alpha\varphi(v)$$

$\varphi(\alpha v_1 + pv_2) = \alpha\varphi(v_1) + p\varphi(v_2)$

Упражнения.

1. Вывести из 1 и 2 формулы 3.

2. Вывести из 3 формулы 1 и 2.

Свойства.

1. При линейном отображении, нулевой вектор, всегда переходит в нулевой.

$$\varphi(\bar{0}) = \varphi(\bar{0} + \bar{0}) = \varphi(\bar{0}) + \varphi(\bar{0})$$

, т.к. в W у любого вектора, есть обратный по сложению, в том числе и для нуля, получаем: $\varphi(\bar{0}) = \bar{0}$

2. Обратный, переходит в обратный: $\varphi(-v) = \varphi(v)$, используем: $-v = (-1)v$

3. **Определение.** Ядром линейного отображения φ, обозначается $Ker\varphi = \{v \in V | \varphi(v) = \bar{0}\}$

Утверждение. $Ker\varphi$ - подпространство пространства V, т.е. $Ker\varphi \leq V$

Доказательство. Используем критерий подпространства и предыдущие 2 свойства.

$\forall v_1, v_2 \in V$; $V_1, V_2 \in Ker\varphi$

$\forall \alpha, \beta \in P$; $\alpha v_1 + \beta v_2 \in Ker\varphi$

Определение. $Im\varphi = \{w \in W |$Существует $v \in V$, Im - образ, такой, что: $\varphi(v) = w\}$; $Im\varphi \leq w$

Доказательство. Используем критерий подпространства. $w_1, w_2 \in Im\varphi$; $\alpha, \beta \in P$
$\varphi(v_1) = w_1$
$\varphi(v_2) = w_2$
$\alpha v_1 + v_2$

Определение. Когда ядро состоит из одного нулевого вектора, значит разные вектора переходят в разные, при этом $Ker\varphi = \{bar0\}$; $Im\varphi = w$, V ИЗОМОРФНО W , т.е. с математической точки зрения - идентичны.

Как задавать линейное отображение ?

В V: $e_1, e_2 \dots e_n$ - базис

В W: $f_1, f_2 \dots f_m$ - базис

Если $n = m$, то такое отображение, называется функционалом. Пусть вектор V ("Живой"вектор) $= \alpha e_1 + \dots \alpha e_n$
$[V] = (\alpha_1, \alpha_2 \dots \alpha_n)$, т.к. отображение - линейное, то $\varphi(v) = \alpha_1\varphi(e_1) + \dots + \alpha_n\varphi(e_n)$, таким образом, оно однозначно задаётся образами своих базисных векторов. Т.к. $(e_1) \in W$, то $\varphi(e_i) =$ СТОЛБЕЦ
$\varphi\_m \times n$ - матрица линейного отображения.

Пример. В качестве пространства V, рассмотрим многочлен порядка не выше 3: $V = \{1, x, x^2, x^3\}$, а в качестве W, не выше 2: $W = \{1, x, x^2\}$.

$$\varphi : v \to w$$

В качестве φ - дифференцирование
$\varphi(1) = 0$
$\varphi(x^2) = 2x$
$[\varphi] =$ МАТРИЦА

Вывод. координаты образа вектора V, будут являться $[\varphi(v)] = [\varphi] \cdot [v]$

Замечание. Вид матриц линейного отображения, зависит от базиса в пространстве V и W. Как изменится эта матрица, если сделать замену базиса ? Базисы меняют, для того, чтобы матрица линейного отображения< была максимально простой, в идеале - диагональной.

V $e_1, \dots e_n$
V' $e'_1, \dots e'_n$

Замену базиса, тоже можно рассматривать, как линейное отображение двух копий V. Один со старым, вторая с новым. Новые выражаем через старые: $V' \to V$

Возникающая матрица, называется матрицей перехода и обозначается T. Матрица T, имеет размер $n \times m$, в ней первый столбец e'_1 ; $T = (e'_1, \dots e'_n)$

$$[V] = T[V]'$$

Эта формула, при естественности определения матрицы T, имеет обескураживающий результат, когда известные координаты без штриха, получаем из неизвестных со штрихом. $[V]' = T^{-1}[V]$, т.е. для нахождения новых координаты< необходимо найти матрицу обратную T. Пусть φ - линейное отображение: $\varphi : V \to V$; $[\varphi]$ - его матрица.

Пусть мы перешли к новому базису с матрицей T.

Вопрос. Как будет выглядеть матрица в новом базисе ?
Ответ....
Доказательство.

$$[\varphi]' = T^{-1}[\varphi]T$$

$$[\varphi(v)] = [\varphi][v]$$

$$[\varphi(v)]' = [\varphi]'[v]'$$

$$[v] = T[v]'$$

ВСЁ ЭТО В СИСТЕМЕ.
Выразить φ', через φ.

Определение. Матрицы A и B, называются сопряжёнными, если существует такая матрица, что: $A = T^{-1}BT$.

Линейные отображения.

Пусть V - вектор пространства над полем P.
$e_1, \ldots, e_n$
$e'_1, \ldots, e'_n$
$\varphi : V \to V$ - гомоморфизм векторных пространств.
$v = \alpha_1 e_1 + \ldots \alpha_n e_n$ - живой вектор
$[v] = (\alpha_1 \ldots \alpha_n)$ - паспорт
$[v]'$ - вектор тот же самый, а набор координат другой.
$\varphi(v) = \alpha_1\varphi(e_1) + \ldots \alpha_n\varphi(e_n)$ - однозначно задаётся на базисных векторах.
$[\varphi]$ = МАТРИЦА - матрица линейного отображения.
$[\varphi(v)] = [\varphi] \cdot [v] \to$ вектор столбец.

На смену координат, можно смотреть, как на тождественные отображения. Первичным, является старый базис, вторичным - новый. $\Rightarrow$ новые базисные вектора, мы выражаем через старые.
$v' \to v$

Возникающая при этом матрица, называется матрицей перехода.
T= МАТРИЦА.

её столбцами, являются образы векторов в старом базисе. Формула один, в этом случае, будет выглядеть так: (2) $[v] = T[v]'$, мы выражали новые координаты через старые, а получилась формула, в которой старые, выражены через новые. Если на самом деле нам известны только старые координаты, то $[v]' = T^{-1}[v]$ - формула нахождения новых координат через старые.
$\varphi : V \to v$
$e_1 \ldots e_n$
$[\varphi(v)] = [\varphi][v]$ (1)
$e'_1 \ldots e'_n$
$[\varphi(v)]' = [\varphi][v]'$ $(1)'$

T - матрица перехода от старого базиса к новому.
$[v] = T[v]'$ $(2)'$
$[\varphi(v)] = T[\varphi(v)]'$ $(2)'$

Используя эти четыре формулы, нам нужно найти связь между координатами, через $[\varphi]$ и $[\varphi]'$

Подставим формулы (2) и (2)$'$ в формулу (1).

$$(1) \Rightarrow T[\varphi(v)]' = [\varphi] \cdot T[v]' \Rightarrow [\varphi(v)]' = (T^{-1}[\varphi]T)[v]'$$

$$[\varphi]' = T^{-1}[\varphi]T$$

Функции совпадают $\leftrightarrow$, когда у них: и у левой, и у правой части области определения - всё пространство V. Т.к. V пробегает всё это пространство и на каждом v, имеет место равенство, значит левая и правая части, как функции совпадают.

Формула замены матрицы линейного отображения при замене базиса:

$$[\varphi]' = T^{-1}[\varphi]T$$

Первичные линейные отображения. Матрица - это удобный математический аппарат для их описания.

Операции над линейными отображениями. Сумма двух линейных отображений - это обычная поточечная сумма двух функций.

$\varphi : v \to v$

$\psi : v \to v$

$(\varphi + \psi)v = \varphi(v) + \psi(v)$

$$[\varphi + \psi][v] = [\varphi][v] + [\psi][v] = ([\varphi] + [\psi])[v]$$

$[\varphi + \psi] = [\varphi] + [\psi]$ - сумма.

Матрица суммы равна сумме матриц.

Суперпозиция линейных отображений.

$$(\varphi \circ \psi)(v) = \psi(\varphi(v))$$

$$[\varphi \circ \psi][v] = [\psi][\varphi(v)] = [\psi][\varphi][v] \Rightarrow$$

Суперпозиция отображений соответствует произведениям матриц.

Собственные и корневые вектора отображения. В каком базисе матрица линейного отображения, будет диагональной ?

$[\varphi]$ = МАТРИЦА

$e_1, \dots e_n$

$\varphi(e_1) = \lambda_1 e_1 \dots \varphi(e_n) = \lambda_n e_n$

Определение. Ненулевой вектор x, называется собственным вектором линейного отображения собственного значения λ, если $\varphi(x) = \lambda x$.

Замечание. Собственный вектор, обязательно не равен нулю, а собственное значение, может быть равно нулю.

Свойство 1. Собственный вектор, имеет единственно собственное значение.

Доказательство. $\lambda \neq \mu$

$\varphi(x) = \lambda x$

$\varphi(\lambda) = \mu^{ll} x = (\lambda - \mu)x = \bar{0}$, $x \neq 0$

$\lambda - \mu = 0 \Rightarrow \lambda = \mu$

Свойство 2. Множество векторов, отвечающих данному собственному значению, образуют подпространства.

Доказательство. Если $\bar{x}$ и $\bar{y}$ - два собственных вектора, отвечающие собственному значению λ, то:
$\forall \alpha, \beta \in P$
$\alpha x + \beta y \rightarrow$ тоже собственный вектор, отвечающий собственному значению.

$$\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y) = \alpha\lambda x + \beta\lambda y = \lambda(\alpha x + \beta y)$$

Свойство 3. Собственные вектора, отвечающие разным собственным значениям, линейно независимы.

Доказательство. База индукции: n=1, т.к. собственный вектор - ненулевой< то он линейно независимый. Пусть:
$\lambda_1, \dots \lambda_{n-1}, \lambda_n$ - собственные значения.
$x - 1, \dots x_{n-1}, x_n$

Предположение индукции: пусть (n-1) векторов - линейно независимы.

Шаг индукции: пусть напротив, существует $\alpha_1, \dots \alpha_n$
$\alpha_1 x_1 + \dots + \alpha_{n-1} x_{n-1} + \alpha_n x_n = \bar{0}$ (1), при этом не все $\alpha_n = 0$. Применим к этому вектору отображение φ:

$$\bar{0} = \varphi(\bar{0}) = \alpha_1\lambda_1 x_1 + \dots \alpha_{n-1}\lambda n - 1 x_{n-1} + \alpha_n\lambda_n x_n = \bar{0}$$

(2)

Умножим уравнение (1) на α_n и вычтем из второго уравнения. $\alpha_1(\lambda_1 - \lambda_n)x_1 + \dots \alpha_{n-1}\lambda_{n-1}x_{n-1} = \bar{0}$
$(\lambda_1 - \lambda_n) \neq 0$
$\alpha_1 = \dots = \alpha_{n-1} = 0$

В формуле (1), остаётся $\alpha_n x_n = \bar{0}$, т.к. $\bar{x}_n \neq \bar{0}$, то $\Rightarrow \alpha_n = 0$ - Противоречие.

Обобщение собственных векторов - это корневые векторы.

$$\varphi(x) = \lambda x \Rightarrow (\varphi - \lambda\varepsilon)(v) = \bar{0}$$

$\varepsilon(v) = v$
$[\varepsilon] = E$

Определение. Вектор, называется корневым, высоты h, если $(\varphi - \lambda\varepsilon)^h(v) = \bar{0}$
$(\varphi - \lambda\varepsilon)^{h-1}(v) \neq 0$

В этой терминологии, собственный вектор - это корневой вектор, высотой $h = 1$.

Как найти собственное значение λ ?
$\varphi(x) = \lambda x$
$(\varphi - \lambda\varepsilon)(x) = \bar{0} \Rightarrow$ Прейдя к координатам $[\varphi - \lambda\varepsilon][x] = \bar{0}$, $\bar{0}$ - столбец из нулей.
$[\varphi] = A$ - матрица линейного отображения.
$(A - \lambda\varepsilon)x = \bar{0}$ - однородная система линейных уравнений. Чтобы система имела ненулевое решение, а собственный вектор - ненулевой $\leftrightarrow$, чтобы

определитель матрицы этой системы был нулевым. Чтобы найти собственное значение x, $det|A - \lambda\varepsilon|$ - ?
где λ - ? неизвестное
$F(\lambda) = |A - \lambda\varepsilon|$ - характеристический многочлен линейного отображения φ.

Теорема. Многочлен, на самом деле, характеристический, т.к. он не зависит от того в каком базисе записана матрица A линейного отображения.

Пусть T - матрица перехода, тогда в новом базисе, матрица отображения:

$$|T^{-1}AT - \lambda E| = |T^{-1}AT - \lambda T^{-1}AT| = |T^{-1}(A \cdot \lambda E)T| =$$

т.к. определитель произведения матрица равен произведению определителей: $\Rightarrow$

$$|T^{-1}| \cdot |A \cdot \lambda E| \cdot |T| = |A - \lambda E| = f(\lambda)$$

, он не меняется при замене базиса.

Корневые вектора.

Пусть V - векторное пространство над полем P. Отображение $\varphi : V \to V$, называется линейным(гомоморфизм линейных пространств), если:

$$\forall \alpha, \beta \in P,$$

$$\forall u, v \in V$$

$$\varphi(\alpha v + \beta u) = \alpha\varphi(v) + \beta\varphi(u)$$

$[\varphi]$ = МАТРИЦА

$e_1, e_2, \dots e_n$

$[v] = (v_1 \dots v_n)$ - координаты

$[\varphi(v)] = [\varphi][v]$

Если мы произвели замену координат $(e_1, e_2, \dots e_n)$, то возникает матрица перехода T, у которой столбцы - это новые базисные вектора< выраженные через старые: T = МАТРИЦА

$$[v] = T[v]'$$

$$[v]' = T^{(} - 1)[v]$$

$$[\varphi]' = T^{(} - 1)[\varphi]T$$

, такие матрицы, называются сопряжёнными.

Определение. $x = \bar{0}$, называется собственным значением λ, если $\varphi(x) = \lambda x$ (λ, может равняться нулю). Если существуют базисы собственных векторов $e_1, e_2, \dots e_n$, то ... $\lambda_1 \dots \lambda_n$

$[\varphi]$ = МАТРИЦА

Характеристический многочлен $f(\lambda) = |\lambda E - A|$.

Алгоритмы нахождения собственных векторов:

1. Выбираем некоторый базис и находим в нём матрицу A, линейного отображения φ.

2. Вычисляем определитель $\lambda E - A$, который является многочленом n-ой степени и называется характеристическим.

3. Находим корни характеристического многочлена.

4. Пусть λ - некоторый корень характеристического многочлена.

Решаем однородную систему уравнений: $(\lambda_i E - A)\bar{x} = \bar{0}$

Множество её фундаментальных решений, т.е. базис пространства решений и есть множество собственных векторов, отвечающих собственному значению λ_i.

Замечание. Всё очень сильно зависит от свойств поля P. Может оказаться так, что характеристический многочлен вообще не имеет корней. Если поле P, не имеет корней, то нужно построить поле разложения характеристического многочлена, тогда появятся все корни.

Идеальный вариант, взять алгебраически замкнутое поле, например поле комплексных чисел. Но даже если поле алгебраически замкнуто и многочлен имеет n корней, то ...

Определение. Ненулевой вектор x, называется корневым, высоты h, отвечающим собственному значению λ.

$$(\lambda\varepsilon - \varphi)^h(x) = \bar{0}$$

$$(\lambda\varepsilon - \varphi)^(h-1)(x) \neq \bar{0}$$

ε - тождественное отображение $[\varepsilon]$ = МАТРИЦА

$$(\varphi - \lambda\varepsilon)(X) = \bar{0}$$

$$\varphi(x) = \lambda x = \lambda\varepsilon x$$

Собственный вектор - это корневой вектор высоты 1.

Свойства:

1. **Теорема.** Множество корневых векторов, отвечающих данному собственному значению, образуют подпространство.

2. Подпространство собственных векторов, отвечающих ..., имеют нулевое пересечение.

Доказательство 1. Воспользуемся критерием подпространства:

$V_(\lambda)$

$x, y \in V_(\lambda)$. По критерию подпространства, нужно проверить, что

$$\forall\alpha, \beta \in P$$

$$\alpha x + \beta y \in V_(\lambda)$$

Пусть высота $x = hx$, $y = hy$.

$$(\lambda\varepsilon - \varphi)^(hx)(x) = \bar{0}$$

$$(\lambda\varepsilon - \varphi)^(hy)(y) = \bar{0}$$

Пусть x - $max\{hx, hy\}$, тогда:

$$(\lambda\varepsilon - \varphi)^h(\alpha x + \beta y) = \alpha(\lambda\varepsilon - \varphi)^h(x) + \beta(\lambda\varepsilon - \varphi)^h(y) = \alpha\bar{0} + \beta\bar{0} = \bar{0}$$

Доказательство 2. $\lambda \neq \mu$

Доказать: $V_\lambda \cap V_\mu = \{\bar{0}\}$. Пусть некоторый вектор $z \in V_\lambda \cap V_\mu$. Т.к. $z \in V_\lambda$, то существует $h_\lambda \in N$, такое что: $(\lambda\varepsilon - \varphi)^(h_\lambda)(z) = \bar{0}$ и $(\lambda\varepsilon - \varphi)^(h_\mu)(z) = \bar{0}$

Рассмотрим эти выражения, как многочлены от символа φ, где λ, μ - элементы поля V. h_μ, h_λ - натуральные числа. Т.к. λ и μ - различные, значит эти многочлены будут взаимно простыми, а значит по следствию из алгоритма Евклида: найдутся такие многочлены, что: $u(\varphi) \cdot f(\lambda) + v(\varphi) \cdot (\mu) = 1$. На эти многочлены, опять смотрим как на линейное отображение и единица справа превратится в тождественное отображение. Применим эти отображения к вектору z, получаем, что: $\bar{0} = z$.

Теорема. Векторное пространство, раскладывается в прямую сумму корневых векторных пространств. Т.е. если $\lambda_1, \lambda_2, \ldots \lambda_n$ - разные корни характеристического многочлена ... $v = v_\lambda \oplus v_\lambda$

Операции над подпространствами. Пусть V - векторное пространство, а u и w - его подпространство.

Определение. Пересечение подпространств u и w, называется их пересечение как множеств: $u \cap w = \{v \in V | v \in u, v \in w\}$

Упражнение: по критерию подпространства доказать, что пересечение подпространств, само является подпространством.

Определение. Сумма подпространств, является подпространством.

$$u + w = \{u + w | v \in u, w \in W\}$$

Доказательство.

$$u_1 + w_1, u_2 + w_2 \in u + w$$

$$\forall \alpha, \beta \in P$$

$$\alpha(u_1 + w_1) + \beta(u_2 + w_2) \in u + w$$

$$(\alpha u_1 + \beta u_2) + (\alpha w_1 + \beta w_2) = u + w \in u + w$$

Определение. Сумма подпространств, называется прямой и обозначается $u \oplus w$ и $u \cap w = \{\bar{0}\}$, если эта подпространства, имеют нулевое пересечение.

Определение. Сумма подпространств $V_1, V_2, \ldots V_n$, называется прямой и обозначается $V_1 \oplus V_2 \oplus \ldots V_n$, если

$$\forall i \in \{1 \ldots k\}$$

$$V_i \cap (V_1 + V_2 + \ldots + V_(i-1) + V_(i+1) + \ldots + V_n) = \{bar0\}$$

Идея доказательства теорем о сумме корневых подпространств: в каждом корневом подпространстве, есть корневой вектор максимальной высоты h.

$$V_(\lambda_1) + \ldots + V(\lambda_n) + \ldots + V_(\lambda_k)$$

$$h_(\lambda_1) + \ldots + h(\lambda_n) + \ldots + h_(\lambda_k)$$

, тогда каждому из этих подпространств, соответствует $(\lambda_i\varepsilon - \varphi)^(h_(\lambda_1))$ - линейное отображение, д**вающее все его вектора. На линейное отображение φ, будем смотреть как на символ. Снова используем следствие из алгоритма Евклида и скомбинируем из них...

Определение. Жорданова клетка. Пусть λ - некоторое собственное значение, тогда матрица вида: МАТРИЦА, называется жордановой клеткой.

Жорданова клетка - это максимально простой вид матрицы, если её нельзя сделать диагональной.

Теорема Жордана. В базисе из корневых векторов, матрица линейного отображения, имеет клеточно-диагональный видМ т.е. по диагонали у неё идут клетки и эти клетки, являются жордановыми, а сама такая форма матрицы, называется жордановой.

Краткий обзор основных алгебраичеких понятий.

Определение.

Бинарной алгебраической операцией на множестве A, называется отображение $f : A * A \to A$ (Из прямого произведения в себя).

Если $f : A^n \to A$, то операция называется n-арной и ей занимается полиномиальная алгебра.

Пример.

det матрицы размерности $n \times n$, можно рассматривать как n-ую операцию, если разбить матрицу на строки или столбцы. И можно рассматривать как n^2-арную, если рассмотреть матрицу поэлементно. При $n = 1$, т.е. когда $f : A \to A$, операция называется унарной. Взятие обратного элемента - унарная операция.

Определение.

Бинарная операция, когда двум элементам множества A, ставится в соответствие третий элемент этого множества. $f : (a, b) \mapsto C$

Вместо длинных слов: бинарная алгебраическая операция, обычно говорят: умножение или сложение.

Операция называется коммутативной, если: $\forall a, b \in A \ f(a, b) = f(b, a)$ $ab = ba$

Коммутативную операцию, обычно называют сложением, но не всегда.

Виды колец:

1. Если умножение ассоциативное, то кольцо называется ассоциативным.

Примеры.

Кольцо целых чисел, кольцо многочленов от любого числа переменных, кольцо матриц над ассоциативным кольцом.

2. Не ассоциативные кольца.

Примеры.

Трёхмерное пространство векторов, где сложение - это сложение векторов, а умножение - это векторное произведение, называется кольцом кольцом Ли, Ёрдановы кольца, Мардоновы.

Т.к. суперпозиция функций - ассоциативная, а большинство процессов в природе и науке - это отображение, то чаще всего встречается ассоциативные кольца.

3. Ассоциативное кольцо с коммутативным умножением, называется коммутативным кольцом.

Пример.

Кольцо матрицы размером > 1, всегда не коммутативное.

Определение.

Если в кольце ненулевые элементы по умножению, образуют некоммутативную группу, то такое кольцо называется телом.

Полю действительных чисел добавим мнимую единицу:

$$R; i, j, k$$

$$i^2 = j^2 = k^2 = -1$$

$$i - j = k$$

$$j \cdot k = i$$

$$j \cdot i = -k$$

1. Абстрактное строение.

Рассмотрим идеал порождённый множеством $f(x)$, т.е. $I = u \cdot g(f(x))$ - это главный идеал состоящий из всех кратных многочленов $f(x)$

$I = ug(f(x)) = \{L(x)|l(x) = f(x) \cdot h(x),\ h(x) \in p[x]\}$

Рассмотрим фактор-кольцо $p[x]/ug(x)$ (По этому идеалу).

По теореме о построении поля разложения, у нас получится поле в котором многочлен $f(x)$, имеет хотя бы один корень, мы можем считать, что это наш α.

2. Символьное описание простого расширения.

У нас есть поле p и символ α, который является корнем многочлена, т.е. $f(\alpha) = 0$. Рассмотрим степени $\alpha, 1, \alpha, \alpha^2, \ldots, (\alpha)^(n-1)$. Т.к. многочлен $f(x)$, имеет n-ую степень, то возникает соотношение: $\alpha^n + a_(n-1)(\alpha)^(n-1) + \ldots + a_0 = 0$, отсюда α^n можно выразить через элементы меньшей степени, таким образом поля $P(\alpha) = \{b_0 + b_1\alpha + \ldots + b_(n-1)\alpha^(n-1)|b_i \in p\}$ или другими словами является векторным пространством размерности n над полем P. Базис $1, \alpha, \ldots, \alpha^(n-1)$.

$\alpha^n = -a_(n-1)\alpha^(n-1) - \ldots - a_0$ - это соотношение задаёт умножение в поле. Степени выше n, получаются при умножении на α этого равенства с последующим использованием этого же равенства.

Теорема 1.

Простое алгебраическое расширение $P(\alpha)$ - изоморфно $\approx P[x]/ug(f(x))$, где $f(x)$ - минимальный многочлен $f(x)$ и $P(\alpha) = a_(n-1)\alpha^(n-1) - \ldots a$.

Теорема 2.

$\forall$ p - простое число и $\forall n \in N$ $\exists$ поле $GF(p)$, содержащие p^n элементов.

Теорема 3 (О структуре подполей поля Галуа).

Пусть $GF(p^n)$ - некоторое поле Галуа, а $CF(p^n)$ - какое-нибудь другое поле, тогда $CF(p^n) \geq GF(p^n) \iff$, чтобы $m|n$, т.е. структура подполей определяется структурой делителей числа n.

9 октября 2017г.

Теорема (Описание неприводимых многочленов).

Пусть $f(x) \in GF(p)[x]$ - неприводимый многочлен, его степень $f(x) = m$.

Утверждение.

Многочлен $f(x) \iff$ делит множество $(x^(p^m) - x)$, когда $m|n$

Вывод из теоремы.

Все неприводимые многочлены степени m, если $m|n$, находятся как сомножители $b(x^(p^m) - x)$.

Доказательство.

1. Пусть $f(x)|(x^(p^m)-x)$, значит его поле разложения $GF(p^m)$ - сходится внутри поля разложения $GF(p^n)$, т.е. $GF(p^m) \triangle GF(p^n) \Rightarrow m|n$

Обратно: пусть $m|n$, тогда поле разложения $GF(p^m) < GF(p^n)$, значит все корни множества f, являются корнями большего многочлена, значит он делит его.

Пример.

Пусть $p = 3, n = 2$

Рассмотрим многочлен $(x^(3^2) - x)$ над $GF(3)$. Перечислим все неприводимые многочлены второй степени над полем $GF(3)$. Они имеют вид: $x^2 + \alpha x + \beta$, α и $\beta \in GF(3)$

Если многочлен второй степени - неприводим, значит у него нет корня.

Теорема о примитивном элементе.

Определение.

Порождающий элемент мультипликативной группы поля, называется примитивным.

Теорема.

В любом конечном поле $GF(p^n)\exists$ примитивный элемент, т.е. мультипликативная группа этого поля - циклична.

Доказательство.

$h = p^n - 1$ - порядок мультипликативной группы. $h = p^n - 1 = p^(\alpha_1)_1 - p^(\alpha_5)_5$ - разложение на простые множители. Для каждого i, рассмотрим многочлен $x^(h/p_i) - 1$. Т.к. этот многочлен, имеет степень $< h$, то не все ненулевые элементы, являются его корнями. Пусть a_i - не корень, т.е.

$$a^(h/p_i)_i \neq 1$$

$$b_i = a^(\frac{h}{p_i k_i})_i$$

. По теореме Лагранжа: каждый элемент в степени равной порядку группы, равен 1. $b^(p^(\alpha_i)_i)_i = 1$, но его порядок, может быть и меньше, однако если $b^(p^(\alpha_(i-1))_i)_i = a^(h/p_i)_i \neq 1 \Rightarrow$ порядок элементов $p_i = p^(\alpha_i)_i$

Элемент $b = b_1 b_2 \dots b_5$ и есть примитивный элемент. Т.к. порядки всех b - взаимно просты между собой, то их НОК равно: $h = p^n - 1 = p^(\alpha_1)_1 \dots p^(\alpha_5)_5$

Если по этой теореме искать примитивный элемент, то нужно перебрать все элементы в поле (ЖУТЬ).

Алгоритм нахождения примитивного элемента.

1. Порядок мультипликативной группы h, раскладывается на простые множители $h = p^n - 1 = p^(\alpha_1)_1 \dots p^(\alpha_5)_5$

Если находимся в простом поле $GF(p)$, то по порядку перебираем $g = 2, 3, 5, 7, 11, 13, 17$

$$g^(\frac{h}{p_i})$$

, $i = 1 \dots 5$

5 раз возвести в степень $\frac{h}{p_i}$. Тот элемент, для которого эти степени $\neq 1$ и будет примитивным.

Сколько примитивных элементов ?

Ответ: $\varphi(h-1)$

Задачи.

1.

$$p = 19$$

$$p - 1 = 18 = 2 \cdot 3^2$$

Нужно проверить $g^(3^2) = g^9; g^6$

$$2^2 = 4$$

$$2^4 = 4^2 = 16$$

$$2^8 = 2^3 \cdot 2 = 9 \cdot 2 = 18$$

$$2^6 = 2^4 \cdot 2^2 = 64 = 7 \neq 1$$

$$GF(2)$$

$$x^2 + x + 1$$

Т.к. все многочлены данной степени делят многочлен $x^p - x$, то какой бы из них мы не взяли, поля разложения будут одинаковыми.

$$x^3 + x + 1$$

$$GF(2^3) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

Добавим корень обозначенный через α.

$$\alpha, \alpha^2, \alpha^4$$

$$\alpha, \alpha^2, \alpha^2 + \alpha$$

Соотношения

$$\alpha^3 + \alpha + 1$$

$$\alpha^4 = \alpha^2 + \alpha$$

Т.к. в поле ненулевых элементов 7 и 7 - простое число $\Rightarrow$ примитивным элементом, будет любой не единичный

$$(\alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1)$$

Нахождение примитивных элементов. Логарифм Якоби. Решения уравнения в конечных полях.

Теорема.

Если поле P, содержит u элементов, то количество разложений примитивных элементов $\varphi(q-1)$

Функция Эйлера - мультипликативна, т.е. если $n = m \cdot k$ $(m,k) = 1$ (взаимно простые), то $\varphi(n) = \varphi(m)\varphi(k)$, поэтому $n = p^(\alpha_1)_1 \dots p^(\alpha_5)_5$, то $\varphi(n) = \varphi(p^(\alpha_1)_1 \dots \varphi(p^(\alpha_5)_5$

Несложно заметить, что каждое p-ое число делится на p, значит: $\varphi(p^\alpha) = p^\alpha - p^(\alpha - 1)$

$$\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 8$$

Таким образом: в $GF(17)$, примитивным является каждый второй ненулевой элемент.

Возьмём поле $GF(2)$, его расширение $x^3 + x + 1$ - неприводимо, т.к. нет корней. Пусть $\alpha^3 = \alpha + 1$, α - его корень.

$$GF(2^3) = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

, в этом поле, примитивными будут все кроме 0 и 1.

$$GF(3)$$

$$x^2 + 1$$

$$\alpha^2 = 2$$

$$GF(3^2) = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

, тогда мультипликативная форма: $|GF^*(3^2)| = 8$

$$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$$

- приводимых.

Для нахождения приводимого $a^n \neq 1$

$$\alpha, \alpha^2 = 2$$

,

$$\alpha^4 = \alpha^2 = 1$$

Как строится поле расширения ?

Берём неприводимый многочлен (не раскладывая на множители) и добавляем формальный корень (например α)

$$^(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$$

$$(\alpha+1)^4 = (2\alpha)^2 = 1 \cdot \alpha^2 = 2 \neq 1$$

В алгоритме AES:

$$GF(2^2)$$

$$x^8 + x^4 + x^2 + x + 1$$

Логарифм Якоби.

Пусть P - поле, a - примитивный элемент, тогда любой ненулевой элемент этого поля, может быть представлен в виде: $b = a^i$, $0 < i < |p|$.

Операцию умножения всегда стремятся заменить сложением и примитивный элемент - идеальное средство. $= a^j \ bc = a^(i + j)$

При использовании примитивного элемента, умножение сводится к сложению показателей.

Определение.

Если a - примитивный элемент: $b = a^i$, то $\log_a b = i$

Возникает проблема со сложением $b + c = a^i + a^j = a^i(1 + a^(j - i)$

Проблема: чему равняется $1 + a^k = a^L(k)$

$L(k)$ - Логарифм Якоби.

31 октября 2017г.

$$GF(7)$$

$$a = 3$$

$$GF(3^2)$$

$$\alpha^2 = 2$$

$$a = \alpha + 1$$

Вторая строка - это показатель степени 3 в случае, когда степень равна соответствующему элементу поля GF(17).

Таблица Якоби

3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
i	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
$L(i)$	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8	#

$$3^1 = 3, 3^2 = 9, 3^3 = 9 \cdot 3 = 27 \ldots 10$$

$$3^4 = 10 \cdot 3 = 30 = 13$$

(по |17|)

$$3^5 = 13 \cdot 3 = 39 = 5$$

$$3^6 = 5 \cdot 3 = 15$$

$$3^7 = 15 \cdot 3 = 45 = 11$$

$$3^8 = 11 \cdot 3 = 33 = 16 = -1$$

$$3^9 = -1 \cdot 3 = -3 = 14$$

$$3^{10} = -3 \cdot 3 = -9 = 8$$

$$3^{11} = 8 \cdot 3 = 7$$

$$3^{12} = 7 \cdot 3 = 21^{-17} = 4$$

$$3^{13} = 4 \cdot 3 = 12$$

$$3^{14} = 12 \cdot 3 = 36 = 2$$

$$3^{15} = 2 \cdot 3 = 6$$

$3^1 + 1 = 4 = 3^1 2$
$L(1) = 12$
$3^2 + 1 = 2^8 + 1 = 16 + 1 = 0$
$L(8) = \#$ - не существует.

Применение логарифма Якоби.

1. Примитивный элемент умноженный по модулю P, сводит к сложению по модулю p-1. Алгоритм Якоби мат. сложения, заменяет сложением показателей.

$GF(17)$ $x^2 + 2x + 11$ $x = \frac{-2+\sqrt{2^2-4 \cdot 11}}{2}$

1. Все элементы заменяем на степени через примитивные:
$-2 = 15 = 3^6$
$2 = 3^1 4$, $2^{-1} = 3^2$
$4 = 2^{12}$
$-4 - 13 = 3^{14}$, $11 = 3^7$
$(3^6 + \sqrt{2^{12} + 3^4 \cdot 3^7}) \cdot 3^2 = 3^8 + 3^2\sqrt{3^7}$
$3^{12} + 3^{11} = 3^{11}(3^1 + 1) = 3^{11} \cdot 3^{12} = 3^{23}(-16) = 3^7$
Если $\sqrt{3^7}$ - корень извлекается, то такой $a \leq x < 16$, что
$(3^x)^2 = 3^{17}$
$2x = 7(16)$
$GF(3^2)$
$\alpha^2 = 2$

$a = \alpha + 1$	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
i	8	4	6	1	7	2	3	5
$L(i)$	4	#	1	7	6	3	5	2

$(\alpha + 1)^1 = \alpha + 1$
$(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$
$(\alpha + 1)^3 = 2\alpha \cdot (\alpha + 1) = 2\alpha^2 + 2\alpha = 1 + 2\alpha$
$(\alpha + 1)^4 = (2\alpha + 1)(\alpha + 1) = 2\alpha^2 + \alpha + 2\alpha + 1 = 4 + 1 = 2$
$(\alpha + 1)^5 = 2(\alpha + 1) = 2\alpha + 2^2$
$(\alpha + 1)^6 = (2\alpha + 2)(\alpha + 1) = 2\alpha^2 + 2\alpha + 2\alpha + 2 = \alpha$
$(\alpha + 1)^7 = \alpha(\alpha + 1)\alpha^2 + \alpha = \alpha + 2$
Считаем L(1):
$(\alpha + 1)^1 + 1 = \alpha = (\alpha + 1)^6$
$LogTo(\text{"}Test.gap\text{"})$;

$M := [1, 1, 01, 0, 0]$;
$Length(M)$;
$Ni := Set(M)$;
Матрица задаётся построчно и разделяется между собой запятыми.
$n := [[1, 2, 2017]]$;
$[0, 1, 2^A 0], [0, 1, 17]$;
$B := A^n(-1)$;
Алгебраически числа.
$x^3 + x + 1$ Рассмотрим над полем $GF(2)$ (Самое маленькое).
Добавим $\alpha^3 = \alpha + 1$
$GF(2^3) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$
Многочлен после добавления, разложится на: $(x - \alpha)(x - \alpha^2)(x - \alpha^4)$ $\alpha^4 = \alpha^2 + \alpha$
Предположим, что этот многочлен над полем $Q : y = x^3 + x + 1$ $\alpha = -0,0162$
У этого многочлена есть единственный корень $\approx -0,0162$
Построим поле разложения для этого многочлена: $\frac{x^3+x+1}{x-\alpha} = x^2 + \alpha x + (a + \alpha^2)$
$x^3 + x + 1 = (x^2 + \alpha x + a + \alpha^2)$
$\beta = \frac{-\alpha \pm \sqrt{\alpha^2 - 4 - 4\alpha^2}}{2} = -\frac{\alpha}{2} \pm \frac{\sqrt{-4-3\alpha^2}}{2} =$
$Q(\alpha) = \{a_2, a^2 + a, \alpha + a_4, \ldots \in Q\}$
Поэтому добавляя один корень неприводимого многочлена 3 степени, 2 группа у нас автоматически не появится. $= -\frac{\alpha}{2} \pm i\sqrt{3\alpha^2 + 4}$
$|Q(\alpha, \beta) : Q| = 6$
Норма и след элементов в конечном поле.
Пусть α - корень некоторого неприводимого многочлена характеристики p, тогда $\alpha, \alpha^p, \alpha^{p^2}, \ldots \alpha^{p^{n-1}}$ - остаточные корни.
Нормой: α $N(\alpha) = \alpha\alpha^p \ldots \alpha^{p^{n-1}} \in \Gamma$
След: $Tr(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}} \in \Gamma$
Несложно проверить, что и след, и норма принадлежат исходному полю расширения которых $f(x) \in P[x]$
$N(\alpha, \beta) = N(\alpha)N(\beta)$
$Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$
$P(\alpha)$
$1, \alpha, \ldots \alpha^{n-1}$ - базис этого поля над полем P. Тогда при помощи элемента α, мы можем задать линейное отображение $\alpha : p(\alpha) \to p(\alpha)$
$\alpha : x \mapsto \alpha x$
Пусть P - Некоторое поле. $S_0, S_1, \ldots$ - некоторая последовательность. Последовательность называется рекуррентной k, если $S_{n+k} = a_{k-1} \cdot S_{n+k-1} + \ldots$
Т.к. первые k элементов, не связаны никакими ограничениями, то вектор $\overline{S_0} = (S_0, S_1, \ldots S_{k-1}$, называют вектором инициализации. Разных векторов инициализации может быть q^k.
Матричная запись регистра сдвига.
A=МАТРИЦА
$\overline{S_n} = S_0 A^n$

Если матричная степень степень станет единичной, то последовательность станет = 0 (будет повторяться).

Теорема.

Если D не делит b, то уравнение не имеет решения, если делит< то решений будет d штук.

Доказательство.

1 Случай.

Если d не делит b, то вычитая из ax любое кратное число n, всегда будет получаться число делящееся на d. Значит b никогда не получится.

2 Случай.

$a = da_0$

$b = db_0$

$n = dn_0$

$a_0x = b_0(n_0) \Rightarrow$ т.к. НОД $(a_0, n_0) = 1$, то по следствию из алгоритма Евклида, у a_0, есть обратный по умножению.

$x_0 = a_0^{-1}b_0(n_0)$

Непосредственно проверяется, что все суммы вида $x = x_0 + in_0$ $0 \leq i < d$, является корнем $ax = b(n)$

Система из k уравнений по различным модулям:

$a_1x = b_1(n_1)$

$a_2x = b_2(n_2)$

...

$a_nx = b_n(n_n)$ - ЭТО СИСТЕМА

Пример.

$S_{n+1} = S_{n+3} + S_{n+2} + S_{n+1} + S_n$ $GF(2)$

$\overline{S_0} = (1, 0, 0, 0)$

$x^4 + x^3 + x^2 + x + 1 \neq (x^2 + ax + 1)(x^2 + bx + 1)$

В нашем случае многочлен - неприводим, т.е. у него нет множителей второго порядка. Поэтому по теореме о корнях неприводимого многочлена, его корнями будут: $\alpha, \alpha^2, \alpha^4, \alpha^8$

$\alpha^4 = \alpha^3 + \alpha^2 \neq \alpha + 1$

$\alpha^8 = \alpha^3$ $\alpha^5 = 1$

Т.к. мультипликативная группа поля, значит α, не является примитивным элементом. Что делать, если многочлен разложения в произведение двух неприводимых многочленов, как найти корни ?

Пример.

$|GF(2^4)^*| = 15$

$GF(3)$

$x^2 + 1$ - неприводимый

$x^2 + x + 2$ - неприводимый (т.к. нет корней из GF(3))

Допустим если характеристический многочлен $f(x) = (x^2+1)(x^2+x+2)$

По теореме о корнях неприводимых многочленов поля Галуа ... все остальные многочлены многочлены данной степени. Из соображений удобства вычислений полю GF(3), мы добавляем корень α первого многочлена, который будет удовлетворять: $\alpha^2 = 2$. По теореме о корнях неприводимого многочлена, корнями будут α и α^3

$GF(3^2) = \{0, 1, 2, \alpha, 2\alpha, \alpha+1, 2\alpha+1, 2\alpha+2; \alpha+2\}$
$x^2 + 1 = (x - \alpha)(x - 2\alpha)$

Теперь среди 9 элементов поля $GF(3^2)$, нужно найти корни второго многочлена.

1 Способ.

Просто перебрать все 6 элементов не принадлежащих $GF(3^2)$, подствить их в многочлен и проверить кто корень.

2 Способ.

Найти корни по формуле квадратного уравнения:
$\frac{-1+\sqrt{1^2-4^2}}{2} = (2 + \sqrt{2}) = 1 + 2\sqrt{2}$
$\sqrt{2}$ - принадлежит полю $GF(3^2)$
$\sqrt{2}$ - это такой элемент а, что $a^2 = 2$, значит $\sqrt{2}$ - это α
$x_{1,2} = 1 \pm 2\alpha$
$x + x + 2 = (x - 1 - \alpha)(x - 1 - +\alpha)$
$x_1 = 1 + 2\alpha$
$x_1 = 1 - 2\alpha$
$GF(2^4)$
$\alpha, \alpha^2, \alpha^3, \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1;\ \alpha^5 = 1$
$15 = 5 \cdot 3\ g^3 \neq 1, g^5 \neq 1$
$\varphi(15) = \varphi(3)\varphi(5) = \varphi \cdot 4 = 8$
Примитивных элементов: 8 штук.
$g = \alpha + 1\ g^2 = (\alpha + 1)^2 = \alpha^2 + 1$
$g^3 = (\alpha^2 + 1)(\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1 \neq 1$
$g^4 = (\alpha + 1)^2\alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1 + 1 = \alpha^3 + \alpha^2 + \alpha + 1$
$g^5 = (\alpha^3 + \alpha^2 + \alpha)(\alpha + 1) = \alpha^4 + \alpha = \alpha^2 + \alpha + 1\alpha = \alpha^3 + \alpha^2 + 1 + 1$

Теперь нужно составить таблицу его степеней, чтобы записать все элементы поля $GF(2^4)$

3	1	2	3	4	5	6	7	8	9	
$(\alpha+1)^i$	$\alpha+1$	α^2+1	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+1$	α^3	$\alpha^2+\alpha+\alpha$	α^3+1	α^2	

Будем использовать упрощение, что самый длинный элемент равен α^4, причём $\alpha^5 = 1$

Для нахождения n-ого члена рекурентной последовательности, нам необходимо решить систему из 4 неизвестных, в которой столбец свободных членов - вектор инициализации, в нашем случае импульсная функция.

$\alpha, \alpha^2, \alpha^4, \alpha^8$
$\alpha_1 = \alpha\ \alpha_2 = \alpha^2\ \alpha_2 = \alpha^3\ \alpha_1 = \alpha^4$
$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 1$
$\beta_1\alpha_1 + \beta_2\alpha_2 + \beta_3\alpha_3 + \beta_4\alpha_4 = 0$
$\beta_1\alpha_1^2 + \beta_2\alpha_2^2 + \beta_3\alpha_3^2 + \beta_4\alpha_4^2 = 0$
$\alpha^4 + \alpha^3 = \alpha^2 + \alpha + 1$ Во второй строчке