Иванов

Лекция
10.10.06.

Если конечное поле состоит из q элементов, то будем его обозначать F_q, или $GF(q)$.

Если поле поле F_q расширено с помощью неприводимого m то такое поле будем обозначать F_q^m или $GF(q^m)$

Обозначение конечных полей

Строение конечных полей

а) примеры и корни.

В конечных полях большое количество неприводимых, кот. делятся в поле F_q (для F_q^m) и кот. при старшей степени $=1$. Все элементы поля являются корнями уравнения

$$x^{q^m} - x \qquad (2.1)$$

Часто (2.1) рассматривают относительно мультипликативной группы поля с кол-вом элементов $n = 2^m - 1$ тогда (2.1) можно трактовать как разложение полинома $x^n - 1$ на линейные множители.

Т.е.

$$(x^n - 1) = (x-1)(x-2)(x-3)\dots(x-n)$$

Если поле F_{q^m}, тогда „-" заменяется на „+" т.к. эти операции совпадают. Элемент поля также явл. корнями полинома меньшей степени с коэф. из F_q.
Полином min степени для ∀ элемент $a \in F_{q^m}$ явл. корнем с коэф. из F_q с 1 при старшей степени назыв. min полиномом элемента a и обозначается $m_a(x)$.
Произв. всех min полиномов $= x^{n}-1$.
Степень min полинома или max и $= m$, или нацело делит m.

б) сопряженный ряд элементов

Пусть поле F_{q^m}, $a \in F_{q^m}$, назовем a - ведущим элементом ряда.

След. посл. называется послед. сопряженных элементов
$$a, a^q, a^{q^2} \dots a^{q^{(m-1)}} \quad (2.2)$$

В ряде (2.2) элементы все различны, если степень $m_a(x)$ - max и равна m.
Если же min полином имеет степень r, то неповторяющаяся часть имеет вид
$$a, a^q, a^{q^2} \dots a^{q^{r-1}} \quad (2.3.)$$
(2.3) повторяется в последов-ти $\frac{m}{r}$ - раз. Все сопряженные элементы имеют одинаковый порядок.

с) циклоклассы

Рассмотрим в поле F_{q^m} все классы сопряженных элементов. Выпишем из них классы с неповторяющимися элементами, а в ост. оставим неповтор. часть. Тогда все поле разобьется на непересекающиеся классы, называемые циклоклассами. Элементы одного циклокласса являются корнями своего min полинома.

D) функция след в поле F_{q^m}

Каждому элементу поля $a \in F_{q^m}$ след. число tr, назыв. следом из поля F_{q^m} в подполе F_q

$tr_{F_{q^m}/F_q}$ (след из поля F_{q^m} в F_q)

$$tr_{F_{q^m}/F_q}(a) = a + a^q + a^{q^2} + \dots + a^{q^{m-1}} \quad (2.4)$$

Значение функции след лежит в поле F_q.
„отображение след" является гомоморфизмом в поле F_q. Причем операция сложения сохраняется, т.е.

$tr_{F_q^m/F_q}(a+b) = tr_{F_q^m/F_q}(a) + tr_{F_q^m/F_q}(b)$

$tr_{F_q^m/F_q}(ca) = c\,tr_{F_q^m/F_q}(a)$

$a \in F_q^m \qquad c \in F_q$

$tr_{F_q^m/F_q}(a^q) = tr_{F_q^m/F_q}(a)$

$a \in F_q^m$

Значение следа элементов в одному классу одинаково.

Е) базис поля

Рассмотрим поле F_q^m можно рассматривать как векторное пространство размерности m => будет базис в этом пр-ве общее подобного 2 вида базиса:

1. канонический базис

пусть θ - примитивный (образующий элемент) примитивного поля группа, тогда канон. базис

$1, \theta, \theta^2, \theta^{m-1}$

2. нормальный базис - он строится над элементом $a \in F_q^m$ и имеет вид

$a, a^q, a^{q^2} \ldots a^{q^{m-1}}$

Нормальный базис - это один из элементов максимального порядка, причем сам элемент a принадлежит не должен быть равен 0.

Если $b_1, b_2 \ldots b_m$ - базис, тогда любой элемент поля может быть представлен в виде

$a_1 b_1 + a_2 b_2 + a_m b_m$, где

$a_1, a_2 \ldots a_m \in F_q$

Ж) Автоморфизмы поля F_q^m

Автоморфизмом называется отображение поля в себя, если при этом остается неизменным элемент поля F_q. Один из важных автоморфизмов называется автоморфизм Фробениуса, а также в соотв. $a \in F_q^m$ число a^{q^j}, где $0 \le j \le m-1$

след элементов a и a^{q^j} - одинаков

З) циклотомические классы

Пусть имеем поле F_q^m, рассмотрим число $n = q^m - 1$, перечислим все числа, взаимно простые по модулю m, меньшие 0. Выберем элемент s. Построим след. ряд элементов

$s, sq, sq^2, \ldots sq^{n_s - 1}$

$mod\ (2^m - 1)$, где

n_s - длина последоват-ти — это такое число, что

$$s q^{n_s} = s \bmod (2^m - 1)$$

причем $n_s = m$ или является делит.

Данная послед. назыв. циклотомическим классом. Все вычеты по mod m разбиваются на циклотомич. классы (не пересекающиеся)

если в мн-ве классов есть класс, у к. n_s - не max длина — это значит, что в поле F_{q^m} есть единств. подполе с кол-вом элем. $F_{q^{n_s}}$ — изоморфное полю $F_{q^{n_s}}$.

$q^{n_s} = V$, тогда можно вычисл. все следы из поля F_{q^m} в поле F_V с кол-вом элементов

$$tr_{F_{q^m}/F_V}(a) = a + a^V + a^{V^2} + \dots + a^{V^{k-1}}$$

учитывая, что $(q^{n_s})^k = q^m$

Пример: В поле F_{2^4} один циклокласс длины 2. След. имеется подполе, состоящ. из элементов этого циклокласса + элементы 0 и 1. Поле, изоморфное полю F_{2^2}.

(полец чэт) и 1 цикл. длина 2

Поле F_{2^6} $m=6$, 2 циклокласса длины 3. Они с добавлением 0 и 1 образуют подполе

Поле $GF(7^4)$ обр. полиномом

$$x^4 + 3x^3 + 5x^2 + 3x + 5$$

имеется един. подполе изомор. полю $GF(7^2)$, т.е. имеется 21 циклокласс длины 2 + 7 элементов поля F_7.

В дальнейшем будем рассм. поле F_{2^m} и при необх. указыв. если $q \neq 2$

Циклоклассы соотв. циклотомич. классам.

Циклотомические приведенные полиномы.

В теории кодиров. широко используются полиномы $P(x)$ с коэф. из поля F_{2^m}, у к. свободный член $=0$, а степень не превышает величину $2^m - 2$. Обозначим это множ-во как $K[x]$. Если делать подстановки $x = a$, где $a \in F_{2^m}$ в полином $P(x)$, то можно посчитать след элемента.

Если след вычисляется в основное поле F_2, то оно назыв. абсолютным следом и обознач.

F_2, $tr_m(a) = Tr_{F_{2^m}/F_2}(a)$

$tr_m[P(x)]$

Пусть $P(x)$ и $Q(x) \in K[x]$

$P(x)$ и $Q(x)$ цикл. эквив. по сиру, если при всех значениях $tr_m[P(x)] = tr_m[Q(x)]$

Циклотомическим прибл. полиномом называется полином вида $P(x) = \sum_S a_S x^S$ (2.5)

Рассмотрим все циклотомич. классы, взятые из каждого из них по одному представителю – пусть число их n и это кол-во обозначим Π_n, тогда в 2.5 суммирование будет вестись по всем $S \in \Pi_n$, т.е. если $S \in$ циклотом. классу не нах. в Π_n, то $x^S \in$ порожденному в этом числе и эквивалентен циклокласса.

Приведение полинома к циклотомически приведенному виду

Пусть $P(x) = \sum_{i=1}^{2^m-1} a_i x^i$ (2.6)

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

Воспользуемся тем, что представители циклотомических классов S, т.е. $i = S \cdot 2^j$, где $j \geq 0$, $0 \leq j \leq n_S - 1$, тогда (2.6) примет вид

$$P(x) = \sum_{S \in \Pi_n} \sum_{j=0}^{n_S-1} a_{S2^j} x^{S2^j} \quad (2.7)$$

$$P(x) = \sum_{S \in \Pi_n} P_S(x)$$

$$P_S(x) = \sum_{j=0}^{n_S-1} a_{S2^j} x^{S2^j} \quad (2.8)$$

циклотомический однор. полином.

Рассмотрим след полинома $P_S(x)$, применив автоморфизм Фробениуса к тождеству (2.8), получим полином, эквив. по сиру $P_S(x)$, т.е.

$$tr\left[\sum_{j=0}^{n_S-1} a_{S2^j} x^{S2^j}\right] = tr\left[\sum_{j=0}^{n_S-1} a_{S2^j}^{2^t} \cdot x^{S2^{j+t}}\right] \quad (2.9)$$

Выберем $t = n_S - j$, тогда (2.9) примет вид

$$tr_m\left[\sum_{j=0}^{n_S-1} a_{S2^j}^{2^t} x^{S2^{j+t}}\right] = tr_m\left[\sum_{j=0}^{n_S-1} a_{S2^j}^{2^{n_S-j}} x^{S2^{n_S}}\right] = tr_m\left[\sum_{j=0}^{n_S-1} a_{S2^j}^{n_S-j} x^S\right] =$$

$$= tr_m\left[x^S \sum_{j=0}^{n_S-1} a_{S2^j}^{n_S-j}\right] \quad (2.10)$$

т.к. $S \cdot 2^{n_S} = S$ (см. 4)

Из (2.10) видно, что циклотомич. однородный полином $P_s(x)$ эквивалентен по следу моному

$$x^s \sum_{j=0}^{ns-1} a^{ns-j}_{s\cdot 2^j}$$

Аналогично рассматривая остальные циклотомич. однородные полиномы, приводим весь полином $P(x)$ к циклотомически эквивал. полиному.

Каждому полиному $P(x)$ соотв. циклотомич. приведённый полином.

Использование преобр. в теории кодирования

Наиболее часто используется преобр. Фурье - Мэтсона - Соломона (ФМС) и преобразование Уолша.

Для правильного их использования необход. учесть их природу.

Преобразов. ФМС.

Пусть имеется циклическая группа порядка n с образующим элементом a.

e - нейтр. элемент

$e, a, a^2, a^3 \ldots a^{n-1}$

$a^n = e$

Необходимо реализовать преобр. порядка n вектора, компонент α из поля F_{2^m}, при этом в мультиплик. группе поля F_{2^m} дол. б. подгруппа порядка n, т.е.

$\frac{2^m-1}{n}$ на цело. Допустим это выполнено.

Будем рассм. компоненты преобр. вектора как ф-ю, которая из α определена все элементы группы. При этом образов значений в поле F_{2^m} отображение [illegible] элементов группы изоморфно в поле F_{2^m}

Пусть $a \xrightarrow{F} \alpha$, где $\alpha \in F_{2^m}$

$\Gamma(a) = \alpha$

учитывая, что $\Gamma(a)$ - изоморфизм, то $\Gamma(a^2) = \Gamma(a)\Gamma(a) = \alpha^2$

$\Gamma(a^3) = \alpha^3$ и т.д. $\Gamma(a^{n-1}) = \alpha^{n-1}$

$\Gamma(a^n) = \Gamma(e) = \alpha^n = 1 \Rightarrow$

$\alpha^n = 1$

$\alpha = \sqrt[n]{1}$ F_{2^m}

Из n корней из единицы, вкл. саму единицу. Эти корни образуют цикл. группу с образ. элементом ε.

$1, \varepsilon, \varepsilon^2 \ldots \varepsilon^{n-1}$

Фазовая группа – изоморфна исходной. Рассм. сторона ней. представлением исходной группы.

Известно, что для коммутативной группы с кол-вом элементов n, можно построить столько представл., сколько элементов в группе. При этом составл. таблица

$e, a, a^2 \dots a^{n-1}$

Γ_1 1 1 1 … 1

Γ_2 1 ε $\varepsilon^2 \dots \varepsilon^{n-1}$

Γ_3 1 ε^2

Γ_n 1 ε^{n-1}

Из анализа видно, что представление имеет n-элементов-характеров, а образованн. степенями корня n-ой степени из 1, поэтому все характеры можно построить, рассмотрев один корень и определив его степени, соотв. элементу исходной группы.

Вычисляя все степени элементов получ. таблицу характера. Строки в этой таблице можно рассм. как лин. незав. векторы. преобр. вектор раскладываемого по этим векторам получ. матрица – наз. матрицей преобразования.

В поле F_{2^m} в качестве образ. элемента ε принимаем $\varepsilon = 2$. Тогда получаем ФМС матрицу, у α элементы имеют вид $2^{\alpha k}$, где $\alpha, k = 0, 1, 2 \dots n-1$

Лекция
11.10.06.

Частное деление x^n+1 на $x+a$ имеет вид

$x^{n-1}+ax^{n-2}+a^2x^{n-3}+\dots+a^{n-2}x+a^{n-1}=$
$=A(x)$

Рассмотрим строку коэф.:

$1 \quad a \quad a^2 \quad a^3 \dots a^{n-2} \quad a^{n-1}$

Строка коэф. совпадает со строкой ФМС матрицы.

Построим полином, у α x старшей степени с коэф. a^{n-1}

$a^{n-1}x^{n-1}+a^{n-2}x^{n-2}+a^{n-3}x^{n-3}\dots$

$\dots a^2x^2+ax+1$ (3.1)

$\overleftarrow{A}(x)\cdot\frac{a}{a}$ $\qquad a^{-1}=b$

$\overleftarrow{A}(x)=b[x^{n-1}+a^{n-1}x^{n-2}+a^{n-2}x^{n-3}$

построить поси-ю всех попарно различных корней и определить его степени, соотв. эл-ту исходной группы.

Вычисл. все степени дан. эл-та и получ. таблицу характеров.
Строки в этой табл. – сист. неравнокомпонентных векторов, преобраз. век-р. расм-ся по этим векторам.
Получ. матрица – мат. преобраз. i

В F_{2^m} (Галуа) в кач-ве образ-го эл-та $\varepsilon = \alpha \Rightarrow$ FMC матрица, у кот-й элементы имеют вид α^{ik}, где $i, k = 0, 1, 2 \dots n-1$.

Свойства матрицы FMC

11.10.06

Пусть дано поле F_{2^m}, $n = 2^m - 1$.
Для данного поля полином $x^n + 1$.

$x^n + 1 = (x+1)(x+2)\dots(x+n)$, $a \in F_{2^m}$
разделим "уголком" $x^n + 1$ на $x + a$.
Обозначим инд-м i шаги деления

$$\begin{array}{l} x^n + 1 \\ \underline{x^n + ax^{n-1}} \quad i = 1 \\ ax^{n-1} + 1 \\ \underline{ax^{n-1} + a^2x^{n-2}} \quad i = 2 \\ a^2x^{n-2} + 1 \\ \underline{a^2x^{n-2} + a^3x^{n-3}} \quad i = 3 \\ a^3x^{n-3} + 1 \\ \dots \\ i = n \qquad a^{n-1}x + 1 \\ \underline{a^{n-1}x + a^n} \\ 0 \end{array}$$

$$\begin{array}{l} \left[x + a \right. \\ x^{n-1} + ax^{n-2} + a^2x^{n-3} + \dots \\ \quad + a^{n-1} \end{array}$$

$a^n = 1$.

Частное от деления $(x^n + 1)$ на $(x + a)$ имеет вид $= A(x)$

$$x^{n-1} + ax^{n-2} + a^2x^{n-3} + \dots + a^{n-2}x + a^{n-1} = \quad 4$$

Рассмотрим строку коэф-в:
$1\ a\ a^2\ a^3 \dots a^{n-2}\ a^{n-1}$

Стр-ка коэф. совп-т со строкой РМС матрицы.

Построим полином, у кот-го x в старш. степени с коэф a^{n-1} — $\overleftarrow{A}(x)$

$$a^{n-1}x^{n-1} + a^{n-2}x^{n-2} + \dots + a^2x^2 + ax + 1 \quad (3.1)$$

$\overleftarrow{A}(x) \cdot \frac{a}{a}$, где $a^{-1} = \beta$

$$\overleftarrow{A}(x) = \beta\left[x^{n-1} + a^{n-1}x^{n-2} + \dots + a^3x^2 + a^2x + a\right] \quad (3.2)$$

$a^n = 1$.

$a^{n-1} \cdot a = a^n = 1. \Rightarrow a^{n-1} = a^{-1} = \beta$

$a^{n-2} = a^{n-1}a^{-1} = \beta^2$

$a^{n-3} = \beta^3$

Запишем (3.2) в виде.

$$\overleftarrow{A}(x) = \beta\left[x^{n-1} + \beta x^{n-2} + \beta^2 x^{n-3} + \dots + \beta^{n-2}x + \beta^{n-1}\right] \quad (3.3)$$

Содержимое кв. скобки имеет стр-ку полинома $A(x)$

Ранее было получено:

$$A(x) = \frac{x^n + 1}{x + a}$$

$$\overleftarrow{A}(x) = \beta\left[\frac{x^n + 1}{x + \beta}\right] \quad (3.4).$$

Если сост-ть полиномиц строки РМС матрицы, где x в старш. степени имеет коэф a^{n-1} имеет вид (3.4)

$\Rightarrow$ сб-во сдвиг мат-цы РМС

Преобразование Фурье

Примем ту же модель, что и для РМС преобр., сделав изменения:

– обл. значения ф-й, кот. сами: модель значений преобр-го вектора, стр-ми в обл. комп. чисел.

Пусть даны группы G_1 и G_2, тогда G – генерируем, внешним, декарт. произв. G_1 на G_2

$G = G_1 \otimes G_2 \Rightarrow$

$\Rightarrow$ эл-ты $g \in G$ имеют вид $g = (g_1, g_2)$

$g_1 \in G_1$, $g_2 \in G_2$.

$g' = (g_1', g_2')$

$g'' = (g_1'', g_2'')$, $g', g'' \in G$, тогда

$g' \cdot g'' = (g_1' \cdot g_1'', g_2' g_2'')$, где

опер-я $g_1' g_1''$ стр-ся группой G_1

$g_2' g_2''$ стр-ся группой G_2

Данный вид произв. можно распр-ть на любое кол-во групп G_i

Рассмотрим постр-е преоб-й на примере преоб-я 8.

$8 = 2^3$

Пусть дана H_2, сост-я из эл-в e, a

Постр-м H_8 2го порядка как внеш. произв. H_2

$H = H_2 \otimes H_2 \otimes H_2$

Тогда эл-ми гр-пы H будут

(e,e,e) ...

(e,e,a) ...

(e,a,e) ... (a,a,a)

Построение матрицы преобраз-й Адам. группы.

Осущ. отображ. группы H_2 с эл-ми е, а в поле компл. чисел, т.е. в группу кв-х корней из 1

$\sqrt{1} = +1, -1$, $\varepsilon = -1$ — образ-й эл-т.

Если $H = G_1 \otimes G_2 \otimes G_3$, то хар-ры этой гр. рассмат-ся как

$$X = \varepsilon_1^{\alpha_1 k_1} \varepsilon_2^{\alpha_2 k_2} \varepsilon_3^{\alpha_3 k_3}$$

Найдем хар-р для гр-пы $H = H_2 \times H_2 \times H_2$ и обозначим $\alpha_i \to u_i$, $k_i \to x_i$

$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon = -1$.

$X = (-1)^{\sum_{i=1}^{3} x_i u_i}$ (3.5) => расшр-е на большее число сомн-х H_2

Введем в-р x, как совокуп. компон. x_i

$x = (x_1, x_2, x_3)$

$u = (u_1, u_2, u_3)$

Тогда Σ можно рассм-ть как скаляр. произв. этих в-в. $\langle x, u \rangle$ =>

=> $X = (-1)^{\langle x,u \rangle}$ (3.6)

Рассмотр. знач-я двоич. в-ра u. Упоряд-м в-ры x и u в соотв. с их ест-м двоич. порядком. При данном значении u подст. посл-но знач-я x в (3.6) получим строку хар. мат-цы. Изменяя u получаем всю мат-цу => мат-ца преобраз-я Уолша — Адамара.

Она состоит из эл-в 1 и -1. Если взять двоич. вектор длиной 2^3, то с помощью мат-цы можно реализ. преоб-е Уолша — Адамара.

При рассм-ии двоич. век-в након. его компо-ты считают знач-ем булевой ф-ии при конкр-м знач. x. (с ест-м порядком сумм-я x) Пусть это ф-я $f(x)$, тогда назовем преобр-е У-А I-го рода

$$W_f(u) = \sum_{\forall x} f(x)(-1)^{\langle x,u \rangle} \quad (3.7)$$

нет куска...

т.е. несколько полиномов м. определять одну и ту же ф-ю. Поэтому будем реализ. булеву ф-ю с помощью циклотомич. приведенных полиномов.

Рассм. их к-во:

пусть поле F_{2^m} имеет $m = p$, где p — простое число, тогда все циклотомич. классы имеют одинак. длину.

F_{2^5}

6 циклот. классов по 5 элементов,

$m_s = 5 = const$, тогда различных циклот. прив. полиномов будет $2^5 \cdot 2^5 \cdot \ldots \cdot 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^5 =$ (шесть классов)

$= 2^{30}$.

При $m = 5$ $2^{2^5} = 2^{32}$ — функций [illegible].

Пусть $m \neq p$

F_{2^4} 3 циклот. класса длиной 4

$\Rightarrow$ Неприводимых полиномов не хватает.

Пусть $m \neq p$. $F_2^4 \Rightarrow$ 3 неприводимых класса длиной $n_s = 4$ и 1 класс $n_s = 2$
Число неприводимых приведённых полиномов:
$2^4 \cdot 2^4 \cdot 2^4 \cdot 2^2 = 2^{14}$
Булевых ф-ий:
$2^{2^4} = 2^{16}$
Если $m = p$, то все неприводимые приведённые полиномы не являются полиномами по следу.
Если m - непростое число как F_2^4, то полином $a_s x^s$, где $s \in$ классу не тех длины не все являются неприводимыми последовательностями

Для реализации всех булевых функций введём $c_0, c_{2^m-1} \in F_2$
$\alpha \in F_{2^n}$ примем $tr_m(\alpha) = 1$.
$P'(x) = c_0 \cdot \alpha + P(x) + c_{2^m-1} \alpha x^{2^m-1}$.
$\Rightarrow$ полиномов хватает

Векторное пространство

Рассмотрим мн-во A эл-тов кот-го назовем векторами и опр-м Σ двух век-в.

Пусть F - поле и $\alpha \in F$, $\beta \in F$, $a, b \in A$
$\Rightarrow$ мн-во A - векторное пр-во, если

1. Элементы мн-ва A с Σ - т Абелеву группу по сложению.
2. Дистр-ти $\alpha a \in A$
3. Выполн-ся след. соотн-я
   $\alpha\beta a = \alpha(\beta a) = (\alpha\beta)a$
   $(a+b)\alpha = a\alpha + b\alpha$
   $(\alpha+\beta)a = \alpha a + \beta a$

1. Подпространства

Подмн-во A_1 явл. подпростр-ва, если для $a, b \in A_1$, $(a+b) \in A_1$,
$\alpha a \in A_1$
В век-м пр-ве опр-м базис $\Rightarrow \forall$ век-р однозначно разложить по базису и своим коорд-там

Ортогональное дополнение подпростр-ва

Пусть A - пр-во и A_1 - подпр-во
Пусть канд. б-р $a \in A_2 \perp \forall b \in A_1$.
Тогда A_2 - подпр-во $\perp A_1$
каждый базисный б-р $\perp \forall$ базис. б-ру A_1
Подпр-во A_2 будет ортогон-м дополн. A_1, если $A = A_1 + A_2$, т.е. $\forall$ б-р $c \in A$ опр-ся как Σ б-ров $a \in A_2$, $b \in A_1$

Афинные пространства

Введем в векторном пр-ве понятие $(\cdot)$.

С каждым вектором связаны 2 (·) одного начало и конец.
Вект-е пр-во, дополн-е мн-м (·) — аффинное пр-во, если выполн-ся 2 условия:

1. $\forall$ (·) M и вектора $\vec{x}$ с началом в дан. (·) всегда найдется (·) N $\overline{MN} = \vec{x}$

2. $\forall$ 3 (·) M, N, P найд-ся 3 таких вектора, что $\overline{MN} + \overline{NP} = \overline{MP}$

Каждой (·) можно пост-ть в соотв. вектор, исход. из начала коорд в дан. (·), тогда при суб. базисе можно ввести коорд. (·)

Пусть коорд (·) $x_i \in A$, разм-ть вект. пространства — n $\Rightarrow$ каждая (·) хар-ся строкой коорд: $(x_1, x_2, \dots x_n)$

Все аффин. пр-ва суб-ные одному и разным. только полям пр-м.

Плоскости.

Рассм. аффин. пр-во A^n
Запишем СУ:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}$$

Рассм. $x_1, x_2 \dots x_n$ как (·)
Пусть ранг матрицы коэф. в левой части $= r$.
Пусть $k = n - r$

Тогда мн-во (·) — реш-е ур-ий $\Rightarrow$
k-мерная плоскость.
Если $k = 1$ — прямая
$k = n-1$ — гиперплоскость