Тема: Конечные поля

Конечные поля

- Теория конечных полей является центральной математической теорией, лежащей в основе помехоустойчивого кодирования и криптологии.
- Конечные поля используются при кодировании, в современных блоковых шифрах таких как IDEA и AES, в поточных шифрах (сдвиговые регистры в мобильных телефонах), а также в открытых криптосистемах, например в протоколе обмена ключами Diffie- Hellman и Elliptic Curve Cryptosystems.

Определение

- Пусть *F есть множество с двумя бинарными операциями + и *.*
- *F называется полем, если*
- *1) F есть абелева группа по сложению +*
- *2) F* = F\ {0} есть абелева группа по умножению **
- 3) Выполняется дистрибутивность для всех *a,b и c из F*

  a*(b + c) = a*b + a*c

  (a+b)*c = a*c + b*c

Определение

- Если число элементов F конечно, то F называется конечным полем

Арифметика по модулю

- **Обозначим:** $Z_n = \{0, 1, \ldots, n-1\}$
- **a mod n есть остаток от деления a на n**
- ***Пример*:7mod2=1, 7mod4=3, 21mod7=0**

если (a+b)=(a+c) mod n

то b=c mod n

Если ab = ac mod n

то b=c mod n только если a и n взаимно просты

a+b mod n = [a mod n + b mod n] mod n

Теорема: Z_p (p – простое число) с операциями сложения и умножения целых чисел по модулю p есть конечное поле

Пример конечного поля

- Конечное поле из двух элементов 0 и 1: $Z_2 = GF(2)$

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

Пример конечного поля (продолжение)

Определелим поле GF(5) на множестве Z_5 (5 – просое число) с операциями сложения и умножения. Как в таблице

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
–a	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

Циклические группы

- *Определение*: Элемент g конечной группы G называется порождающим или примитивным элементом, если все элементы группы являются степенями g. Такие группы называют циклическими
- Таким образом $G = \{g, g^2, \ldots, g^n\}, \quad g^n = e, \quad e -$ нейтральный элемент группы.
- **Обозначение:** $G = \langle g \rangle$

Определение

- **Порядок группы** G – число элементов группы (обозначение |G|).
- **Порядок элемента** g ϵ G – наименьшее n так что $g^n = e$ (обозначается ord g).

Теорема 1: Z_n^* является циклической только если n есть одно из чисел $2, 4, p^n, 2p^n$, где p есть нечетное простое число и n – положительное целое число.

Теорема 2: Все циклические группы одного размера изоморфны.

Теорема 3: Пусть G – циклическая группа из n элементов и g – порождающий элемент (т.е. $G = \langle g \rangle$). Тогда порядок подгруппы $\langle g^k \rangle$ равен $\frac{n}{нод(n,k)}$

Теорема 4: Пусть G есть циклическая группа из n элементов и $d_1, d_2, ..., d_k$ являются делителями n, тогда $\varphi(d_i)$ существуют в точности элементов порядка d_i

Конечные поля F_{q^n} ($GF(q^n)$)

- **Эварист Галуа(**1811 -1832)

Многочлены

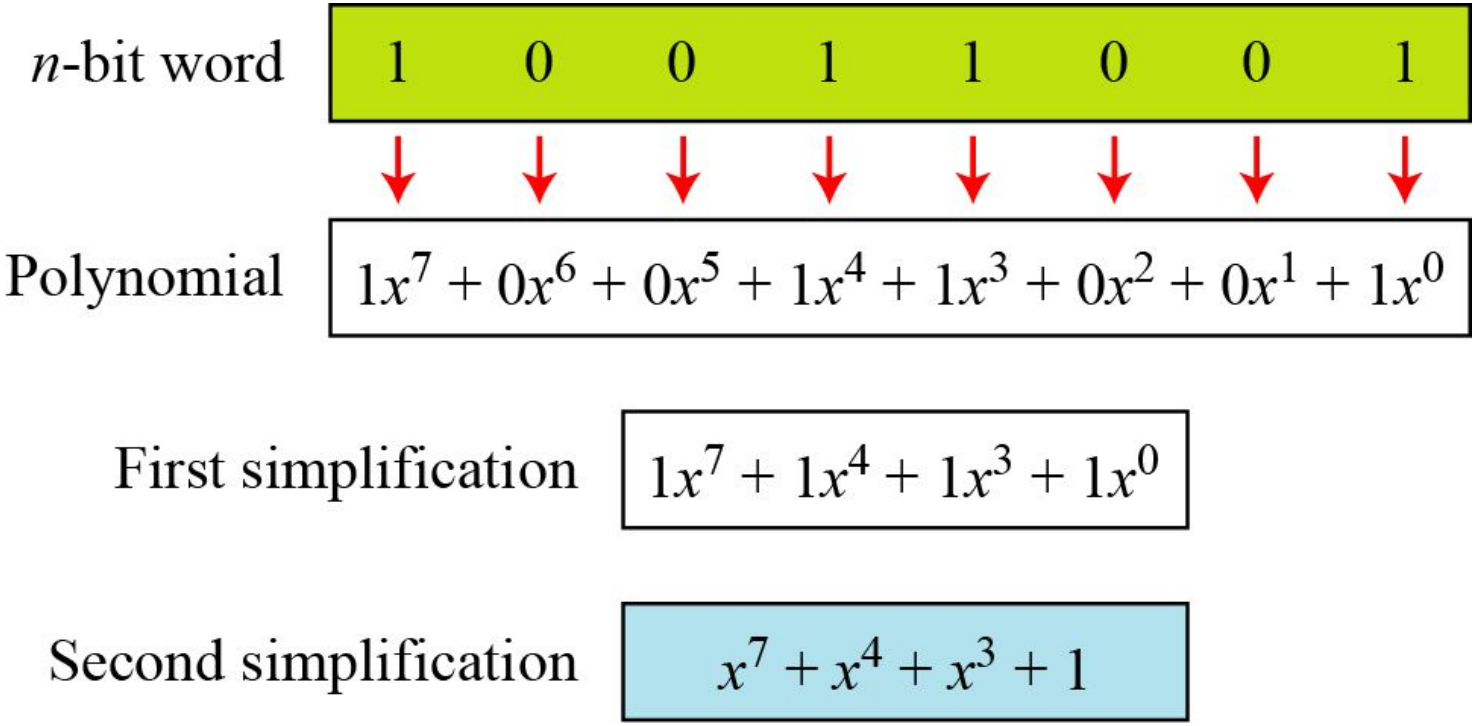
Многочлен степени n

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

a_i – коэффициенты из некоторого множества (поля)

Многочлены (продолжение)

Следующий рисунок иллюстрирует, как можно 8-разрядное слово (10011001) представить в виде многочлена.



Расширенные конечные поля

Конечные поля существуют только для порядков $q=p^m$ (p – простое, m – натуральное).

Простое поле порядка p, $GF(p)$, можно трактовать как множество $\{0, 1, \ldots, p-1\}$ остатков от деления целых чисел на p с операциями сложения и умножения по модулю p.

Расширенные конечные поля

Подобно этому расширенное поле $GF(p^m)$ порядка $q=p^m$ при $m>1$ можно ассоциировать с множеством остатков от деления полиномов над $GF(p)$ на некоторый неприводимый полином $f(x)$ степени m с операциями сложения и умножения по модулю $f(x)$.

Другими словами, поле $GF(p^m)$ можно представить всеми полиномами над простым полем $GF(p)$ степени не выше $m-1$ с обычным полиномиальным сложением.

Умножение же в нем выполняется в два шага – сперва как обычное умножение полиномов, но с удержанием в качестве конечного итога лишь остатка от деления полученного произведения на неприводимый полином $f(x)$.

Расширенные поля Галуа

Определим поле GF(2^2) , состоящее из 4 двухразрядных слов: {00, 01, 10, 11}. Определим операции сложения и умножения следующим образом.

Addition

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

Multiplication

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

Многочлены - модули

Для построения поля GF(2^n) используются многочлены – модули над полем GF(2), которые должны быть неприводимыми.

Degree	*Irreducible Polynomials*
1	$(x + 1)$, (x)
2	$(x^2 + x + 1)$
3	$(x^3 + x^2 + 1)$, $(x^3 + x + 1)$
4	$(x^4 + x^3 + x^2 + x + 1)$, $(x^4 + x^3 + 1)$, $(x^4 + x + 1)$
5	$(x^5 + x^2 + 1)$, $(x^5 + x^3 + x^2 + x + 1)$, $(x^5 + x^4 + x^3 + x + 1)$, $(x^5 + x^4 + x^3 + x^2 + 1)$, $(x^5 + x^4 + x^2 + x + 1)$

Пример. Обратимся к полиному $f(x)=x^3+x+1$(неприводимый), $\deg(f(x))=3$, тогдае го можно использовать для построения расширенного поля $GF(2^3)=GF(8)$.

Для $a(x)=x^2+x+1$ и $b(x)=x+1$

сумма в поле $GF(8)$ $a(x)+b(x)= x^2+x+1+x+1= x^2$

произведение в GF(8) $(x^2+x+1)(x+1) = x^3+x^2+x^2+x+x+1 = x^3+1$, после чего разделим полученный результат на $f(x)$ с последующим удержанием только остатка: $x^3+1=q(x)f(x)+r(x)=1\cdot(x^3+x+1)+x$. Таким образом, $a(x)b(x)=(x^2+x+1)(x+1)=x$.

×	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Мультипликативный порядок элементов поля. Примитивные элементы

В любом поле $GF(q)$, будь оно простым или расширенным, можно перемножать любые операнды, в том числе l-кратно умножать элемент α на себя. Естественно называть такое произведение l-й **степенью** элемента α, обозначив его как

$$\underbrace{\alpha\alpha\ldots\alpha}_{l \text{ раз}} = \alpha^{l}.$$

$$\alpha^{l}\alpha^{s} = \underbrace{\alpha\alpha\ldots\alpha}_{l \text{ раз}}\underbrace{\alpha\alpha\ldots\alpha}_{s \text{ раз}} = \underbrace{\alpha\alpha\ldots\alpha}_{l+s \text{ раз}} = \alpha^{l+s}$$

$$\alpha^{l} / \alpha^{s} = \underbrace{\alpha\alpha\ldots\alpha}_{l \text{ раз}} / \underbrace{\alpha\alpha\ldots\alpha}_{s \text{ раз}} = \underbrace{\alpha\alpha\ldots\alpha}_{l \text{ раз}}\underbrace{\alpha^{-1}\alpha^{-1}\ldots\alpha^{-1}}_{s \text{ раз}} = \alpha^{l-s}.$$

Возьмем некоторый ненулевой элемент $\alpha \in GF(q)$ и рассмотрим его степени α^1, α^2, …, α^l, … . Поскольку все они принадлежат конечному полю $GF(q)$, в рассматриваемой последовательности рано или поздно появятся повторения, так что для некоторых l и s $(l>s)$ $\alpha^l = \alpha^s$, а значит, $\alpha^{l-s}=1$. Назовем минимальное натуральное число t, для которого

$$\alpha^t = 1$$

мультипликативным порядком элемента α.

Пример 1.

Элемент 2 поля $GF(7)$ имеет мультипликативный порядок $t=3$ поскольку для него $2^1=2$, $2^2=4$, $2^3=1$. Подобно этому, как легко видеть, для элемента 3 $t=6$, для 4 t =3, *для 5* $t=6$, для 6 $t=2$. Все найденные мультипликативные порядки делят число $p-1=6$ ненулевых элементов поля.

Пример.2.

В поле $GF(8)$ число ненулевых элементов поля – простое: $8-1=7$, а, значит, его делители – только числа 1 и 7. Так как единственный элементом мультипликативного порядка 1 – единица поля, все остальные ненулевые элементы имеют максимальный мультипликативный порядок, равный 7.

Структура конечных полей

- Пусть f(x) – неприводимый многочлен степени n над полем F и α - корень f(x). Тогда поле F[x]/(f(x)) можно представить как

  $F[\alpha]=\{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_i \text{ из } F\}$
- Пусть α есть корень неприводимого многочлена степени m над полем GF(q), тогда α является также порождающим элементом поля

$$GF(q^m) = \{a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} : a_i \in GF(q)\}$$

$$= \{0, \alpha, \alpha^2, \ldots, \alpha^{q^m - 1}\}$$

Структура конечных полей

- Пример:
  α корень многочлена $1+x+x^3$ над GF(2) , то есть $1+x+x^3 \in GF(2)[x]$. Следовательно, GF(8)=GF(2)[α]. Порядок α есть делитель 8-1=7. Поэтому ord(α)=7 и α – примитивный элемент.

$$\text{Элементы поля } F_8$$

$$0=0 \qquad 1=\alpha^7=\alpha^0 \qquad \alpha=\alpha^1 \qquad \alpha^2=\alpha^2$$

$$1+\alpha=\alpha^3 \quad \alpha+\alpha^2=\alpha^4 \quad 1+\alpha+\alpha^2=\alpha^5 \quad 1+\alpha^2=\alpha^6$$

- Тогда:
  $\alpha^3+\alpha^6 = (1+\alpha)+(1+\alpha^2) = \alpha+\alpha^2 = \alpha^4$
  $\alpha^3\alpha^6 = \alpha^9=\alpha^2$

Структура конечных полей

- *Таблица логарифмов Zech:*
  - Пусть α – примитивный элемент GF(q). Для каждого $0 \leqq i \leqq q-2$ или $i = \infty$, мы определяем и заносим в таблицу элемент z(i) такой что $1+\alpha^i=\alpha^{z(i)}$. (примем $\alpha^{\infty} = 0$)
  - Для любых двух элементов α^i и α^j , $0 \leqq i \leqq j \leqq q-2$ в поле GF(q).

$$\alpha^i+\alpha^j = \alpha^i(1+\alpha^{j-i}) = \alpha^{i+z(j-i) \pmod{q-1}}$$

$$\alpha^i\alpha^j = \alpha^{i+j \pmod{q-1}}$$

Структура конечных полей

Таблица логарифмов для F_{27}

i	z(i)	i	z(i)	i	z(i)
∞	0	8	15	17	20
0	13	9	3	18	7
1	9	10	6	19	23
2	21	11	10	20	5
3	1	12	2	21	12
4	18	13	∞	22	14
5	17	14	16	23	24
6	11	15	25	24	19
7	4	16	22	25	8

Теорема: Произвольный неприводимы многочлен над полем GF(2) делит многочлен X^n+1, где

n = 2^m-1 и ***m*** есть степень многочлена

Примитивные многочлены

- Неприводимый многочлен p(X) степени ***m*** называется примитивным, если ***n*** – наименьшее положительное целое число такое что p(X) делит $X^{n}+1$ и $n=2^{m}-1$
- Пример
  - $p(X)=X^{4}+X+1$ делит $X^{15}+1$ но не делит никакой многочлен $X^{n}+1$ для $1 \leq n < 15$ **(Primitive)**
  - $p(X)= X^{4}+X^{3}+X^{2}+X+1$ делит $X^{5}+1$ **(Irreducible but Not Primitive)**

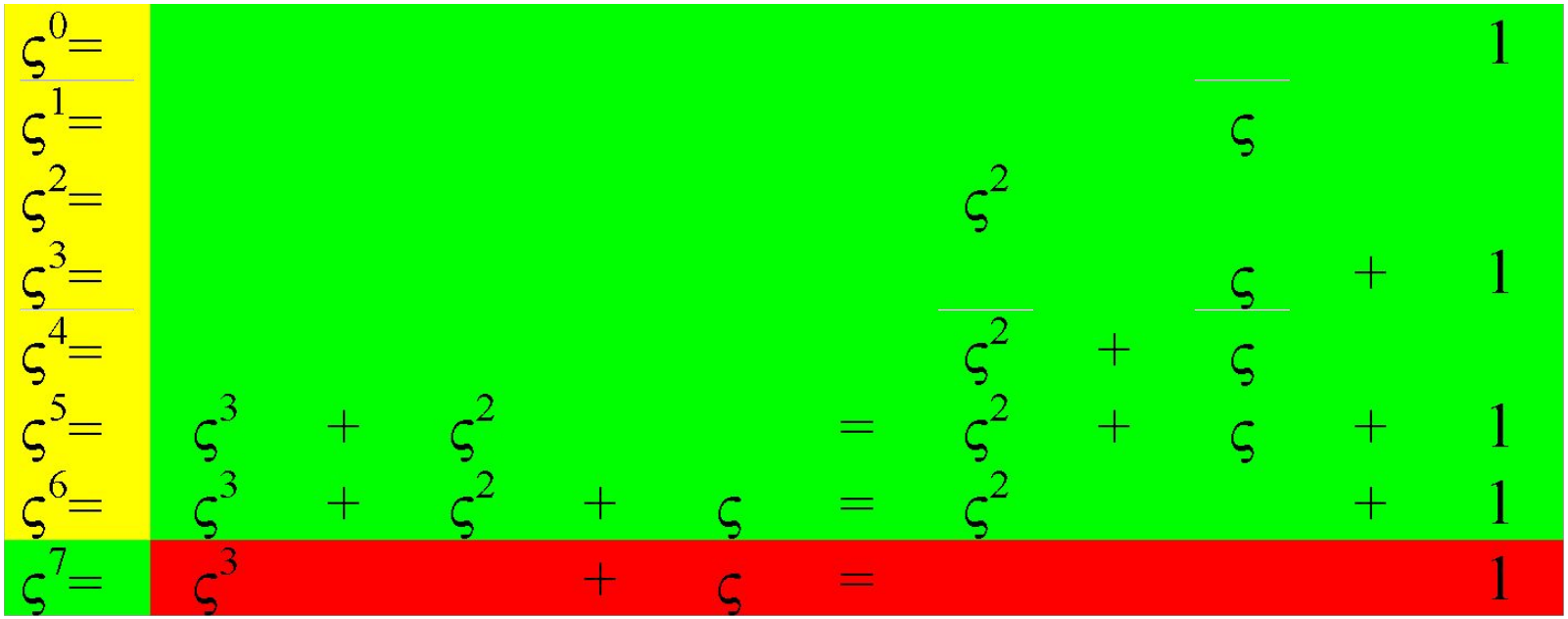
Пример.

Элементы 3 и 5 поля $GF(7)$ являются примитивными, тогда как остальные ненулевые элементы непримитивны. Действительно, $p-1=6$ степеней элемента 3 различны: $3^1=3$, $3^2=2$, $3^3=6$, $3^4=4$, $3^5=5$, $3^6=3^0=1$. Для непримитивного элемента поля, например 2, подобные вычисления дают $2^1=2$, $2^2=4$, $2^3=1$, $2^4=2$, $2^5=4$, $2^6=1$, так что возведением 2 в различные степени можно получить лишь некоторые (но не все!) ненулевые элементы $GF(7)$.

Построение расширенного поля $GF(p^m)$ в виде таблицы степеней примитивного элемента начинается с выбора примитивного полинома степени m над простым полем $GF(p)$: $f(x)=x^m+f_{m-1}x^{m-1}+\ldots+f_0$. Подобные полиномы либо даются в специальных таблицах, либо маркируются особой меткой в таблицах неприводимых полиномов.

Для m-й степени элемента x по модулю $f(x)$ имеет место равенство $x^m = -f_{m-1}x^{m-1}-f_{m-2}x^{m-2}-\ldots-f_0$.

Пример. Полином $f(x)=x^3+x+1$ примитивен над $GF(2)$. Учтя, что в $GF(8)$ построенном с помощью $f(x)$, $x^3= x+1$ и обозначив $x=\varsigma$, имеем $\varsigma^3=\varsigma+1$. Вычислив следующие степени ς, придем к таблице



Перемножая два элемента поля, например $\varsigma+1$ and $\varsigma^2+\varsigma+1$, можно воспользоваться представлениями $\varsigma+1=\varsigma^3$ и $\varsigma^2+\varsigma+1=\varsigma^5$, так что $\varsigma^3\varsigma^5=\varsigma^8=\varsigma^7\varsigma=\varsigma$.

Некоторые свойства расширенных конечных полей

Теорема 1. **Среди всех элементов расширенного поля** $GF(2^m)$ **лишь элементы основного подполя** $GF(2)$ **, т.е.** 0 **и** 1**, удовлетворяют равенству**

$$\alpha^2 = \alpha.$$

Теорема 2. **Для любых элементов** α, β **поля** $GF(2^m)$

$$(\alpha+\beta)^2 = \alpha^2 + \beta^2.$$

Построение полиномов с заданными корнями

Одно из фундаментальных положений классической алгебры утверждает, что любой полином $f(x)$ степени m с действительными или комплексными коэффициентами всегда имеет ровно m действительных или комплексных корней x_1, x_2, …, x_m, что означает справедливость разложения (при единичном старшем коэффициенте)

$$f(x) = \prod_{i=1}^{m} (x - x_i).$$

Пример 1. Рассмотрим полином $g(z)=z^3+z^2+1$. Легко убедиться, что у него нет корней в $GF(2)$: $g(1)= g(0)=1$. Вместе с тем, обратившись к таблице поля $GF(8)$ в примере 8.2.4, можно видеть, что $g(\varsigma^3)=\varsigma^9+\varsigma^6+1=\varsigma^2+\varsigma^2+1+1=0$, и значит, ς^3 является корнем $g(z)$ в поле $GF(8)$.

Двоичный полином наименьшей степени, для которого элемент $\alpha \in GF(2^m)$ является корнем, называется **минимальным полиномом** α. Введем для него обозначение $g_\alpha(z)$ и сформулируем следующее утверждение.

Теорема 1. Пусть l – длина сопряженного цикла элемента α. Тогда

$$g_\alpha(z) = \prod_{i=0}^{l-1} (z - \alpha^{2^i}).$$

Теорема 2. Пусть $GF(q)$ - расширение $GF(2)$, где $q=2^m$. Тогда все ненулевые элементы $GF(q)$ являются корнями бинома $z^{q-1}-1 = z^{q-1}+1$.

Как следствие этой теоремы справедливо следующее равенство

$$z^{q-1} - 1 = \prod_{i=0}^{q-2} (z - \varsigma^i),$$

где все $q-1$ ненулевых элементов $GF(q)$ выражены как степени примитивного элемента ς.

Алгоритмы

- Алгоритм Евклида нахождения НОД
- Расширенный алгоритм Евклида
- Возведение в степень

Векторное пространство(V,F, +, .)

- F - поле
- V множество элементов(векторов)
- Сложение векторов(коммутативное, ассоциативное)

$$\exists 0, \forall \alpha \in V, \alpha + 0 = 0. \quad \forall \alpha \exists ! - \alpha, \alpha + (-\alpha) = 0.$$

- Умно$(c, \alpha) \mapsto c\alpha, c \in F, \alpha \in V$

$$1\alpha = \alpha, (c_1 c_2)\alpha = c_1(c_2\alpha), c(\alpha + \beta) = c\alpha + c\beta, (c_1 + c_2)\alpha = c_1\alpha + c_2\alpha$$

- Линейная зависимость, базисы, подпространства

Источники

- Ленг С. Алгебра -М:, Мир, 1967
- Р. Лидл, Г. Нидеррайтер. Конечные поля. В 2-х томах. - Москва, "Мир", 1988.
- Э.Берлекэмп, Алгебраическая теория кодирования, Мир, Москва, 1971.
- Р.Блейхут, Теория и практика кодов, контролирующих ошибки, Мир, Москва, 1986.
- http://www.ksu.ru/f9/index.php?id=20