5 Конечные поля

5.1 Конечные поля

Определение 5.1. *Кольцом* $\langle R, +, *\rangle$ называется множество R с двумя бинарными операциями $+$ и $*$ такими, что

1) $\langle R, +\rangle$ — абелева группа;

2) операция $*$ ассоциативна, т. е. $(a * b) * c = a * (b * c)$ для всех $a, b, c \in R$;

3) выполняются законы дистрибутивности:

$$a * (b + c) = a * b + a * c, \quad (a + b) * c = a * c + b * c, \quad a, b, c \in R.$$

Определение 5.2. Кольцо $\langle R, +, *\rangle$ называется *полем*, если $R \neq \{0\}$, где 0 — единица $\langle R, +\rangle$, и

4) $\langle R \setminus \{0\}, *\rangle$ — абелева группа. □

Для группы $\langle R, +\rangle$ будем использовать аддитивную запись, а для группы $\langle R \setminus \{0\}, *\rangle$ — мультипликативную. Напомним соответствующие системы обозначений:

	мультипликативная запись	аддитивная запись
операция	$a * b$, ab	$a + b$
единица	e, 1, id	0
обратный элемент	a^{-1}	$-a$
кратный	a^n	na
кратный обратный	a^{-n}	$-na$
применение обратного	ab^{-1}, a/b	$a - b$

Упражнение 5.1. Доказать, что $0 * a = a * 0 = 0$ для всех $a \in R$ (R — кольцо). □

Упражнение 5.2. Доказать, что множества $\mathbb{R}$, $\mathbb{C}$ с обычными операциями сложения и умножения являются полями. Указать, какие из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ являются кольцами, какие полями. □

Отметим, что если в последнем определении $\langle R \setminus \{0\}, *\rangle$ просто группа (не обязательна абелева), то соответствующая структура называется *телом*. Знаменитая теорема Веддербёрна (1903) гласит, что *каждое конечное тело является полем*. Как видим, введенная система аксиом обладает внутренней логикой, которая позволяет получать нетривиальные выводы. Далее мы, опираясь на аксиомы, исчерпывающим образом опишем строение конечных полей.

Теорема 5.1. Если p — простое, то $\mathbb{Z}_p$ — конечное поле.

Доказательство. Действительно, $\mathbb{Z}_p$ — кольцо, т. е. выполнены аксиомы 1 – 3. Дополнительно, $\langle \mathbb{Z}_p^*, *\rangle$ — абелева группа и $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, т. е. выполнена аксиома 4. □

Подчеркивая, что $\mathbb{Z}_p$ — поле, будем писать $\mathbb{F}_p$ вместо $\mathbb{Z}_p$.

Пример 5.1. Поле $\mathbb{F}_2$ состоит из двух элементов: 0 и 1. Правила сложения: $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$. Правила умножения: $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$. Иногда, чтобы подчеркнуть, что сложение выполняется по модулю 2 вместо $+$ пишут $\oplus$. □

5.2 Многочлены

Многочленом над кольцом R называется выражение вида:

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,$$

где $a_i \in R$, а x — некоторая (формальная) переменная. Если $a_n \neq 0$, то n — степень многочлена ($\deg a = n$), a_n — старший коэффициент. Степень нулевого многочлена ($a_0 = a_1 = \ldots = a_n = 0$) полагается равной -1. *Постоянный* многочлен — многочлен степени $\leqslant 0$.

Арифметика многочленов регулируется обычными законами: если $g(x) = b_0 + b_1x + \ldots + b_nx^n$, то

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n,$$
$$f(x)g(x) = c_0 + c_1x + \ldots + c_{2n}x^{2n}, \quad c_k = \sum_{i+j=k} a_ib_j.$$

При таком выборе операций множество всех многочленов над R оказывается кольцом, которое называется *кольцом многочленов* и обозначается через $R[x]$.

Далее нас будут интересовать в основном многочлены из кольца $F[x]$, где F — конечное поле.[1] Напомним некоторые факты и определения, связанные с многочленами из $F[x]$:

A. Деление многочлена f на g: $f = gh + r$, $\deg r < \deg g$. Если $r = 0$, то g делит f: $g \mid f$. Будем писать $r = f \mod g$.

   Для $f_1, f_2 \in F[x]$ пишем $f_1 \equiv f_2 \pmod g$, если $g \mid f_1 - f_2$.

B. При замене в $f(x)$ всех вхождений переменной x на b получаем значение $f(x)$ при $x = b \in F$.[2] Если при этом $f(b) = 0$, то b — *корень* f. Для такого корня

   $$f(x) = (x - b)h(x) \text{ или } (x - b) \mid f(x)$$

   Многочлен f может иметь не более $\deg f$ корней. [3]

C. Многочлен f называется *неприводимым* (над полем F или в кольце $F[x]$), если он имеет положительную степень и равенство $f = g_1g_2$, $g_i \in F[x]$, означает, что один из многочленов является постоянным. Всякий многочлен положительной степени можно представить в виде $f_1^{n_1} \ldots f_k^{n_k}$, где f_i — неприводимые многочлены.

Теорема 5.2 (о существовании неприводимых многочленов). Для каждого конечного поля F и каждого натурального n в кольце $F[x]$ существует неприводимый многочлен степени n.

Пример 5.2. Многочлен x^2+x+1 неприводим над $\mathbb{F}_2$. Действительно, в противном случае $x^2+x+1 = (x+\alpha)(x+\beta)$ для некоторых $\alpha, \beta \in \mathbb{F}_2$. Но тогда $\alpha\beta = 1 \Rightarrow \alpha = \beta = 1$ и $\alpha + \beta = 1$, противоречие. $\square$

Упражнение 5.3. Доказать, что многочлен $x^3 + x + 1$ неприводим над полем $\mathbb{F}_2$. $\square$

5.3 Конечные поля из p^n элементов

Пусть F — поле и $f(x) \in F[x]$. Рассмотрим множество

$$F[x]/(f) = \{g(x) \in F[x] \colon \deg g < \deg f\}$$

с операциями сложения и умножения по модулю $f(x)$ (такая алгебраическая структура называется *фактор-кольцом*).

---

[1] Кольцо $F[x]$ в этом случае является целостным, т. е. коммутативным (относительно умножения) кольцом с единицей (мультипликативной), в котором из равенства $fg = 0$ следует, что $f = 0$ или $g = 0$.

[2] Важно, что многочлен $f(x)$ отличается от функции $b \mapsto f(b)$. В частности, одна и та же функция может задаваться различными многочленами.

[3] *Кратностью* корня b называется максимальное k такое, что $(x - b)^k \mid f(x)$. При $k = 1$ корень является *простым*, а при $k > 1$ — *кратным*. Корень b является кратным тогда и только тогда, когда он одновременно является корнем многочлена $f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$.

Теорема 5.3 (существование конечного поля). Если F — конечное поле из q элементов, $f(x) \in F[x]$ — неприводимый многочлен степени n, то $P = F[x]/(f)$ — поле из q^n элементов.

Доказательство. Для P очевидно выполнены аксиомы кольца. Постоянный многочлен 0 является аддитивной единицей, а постоянный многочлен 1 — мультипликативной единицей P. Операция умножения ассоциативна и достаточно доказать, что для любого $g \in P \setminus \{0\}$ найдется $h \in P$ такой, что $gh \equiv 1 \pmod{f}$.

От противного, пусть $gh \not\equiv 1 \pmod{f}$ для всех h. Тогда найдутся различные $h_1, h_2 \in P$ такие, что

$$gh_1 \equiv gh_2 \pmod{f} \Rightarrow g(h_1 - h_2) \equiv 0 \pmod{f} \overset{f\text{ — неприводим}}{\Longrightarrow} h_1 = h_2,$$

противоречие. □

Следствие 5.1. Для любого простого p и натурального n существует поле из p^n элементов.

Доказательство. Всегда найдется неприводимый над $\mathbb{F}_p$ многочлен $f(x)$ степени n. Тогда $P = \mathbb{F}_p[x]/(f(x))$ — искомое поле. □

Отметим, что поля $\mathbb{F}_p$ и $F[x]/(f(x))$ строятся по одной и той же схеме:

кольцо	$\mathbb{Z}$	$F[x]$
элемент	m	$f(x)$
факторкольцо	$\mathbb{Z}_m = \mathbb{Z}/(m)$	$F[x]/(f(x))$
условие	$m = p$ — простое	$f(x)$ — неприводимый

Пример 5.3. Таблицы сложения и умножения в $\mathbb{F}_2[x]/(x^2 + x + 1)$:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$*$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Упражнение 5.4. Составить таблицу умножения в поле $\mathbb{F}_2[x]/(x^3 + x + 1)$. □

5.4 Подгруппы

Определение 5.3. Подмножество $H \subseteq G$ называется *подгруппой* $\langle G, * \rangle$, если H само образует группу относительно операции $*$. □

Тривиальные подгруппы: $H = \{e\}$, $H = G$. Подгруппы, отличные от тривиальных — *собственные*.

Упражнение 5.5. Доказать, что H является подгруппой тогда и только тогда, когда

1) $ab^{-1} \in H$ для всех $a, b \in H$;

2) $ab \in H$ для всех $a, b \in H$ (если G — конечная группа). □

Пример 5.4. Пусть $m = pk$, $H = \{0, p, 2p, \ldots, (k-1)p\}$. Тогда $\langle H, + \rangle$ — подгруппа $\langle \mathbb{Z}_m, + \rangle$. □

Теорема 5.4 (Лагранж). Порядок (число элементов) конечной группы делится на порядок любой ее подгруппы.

Доказательство. Пусть G — конечная группа, H — ее подгруппа. Определим *левые смежные классы* G по H — подмножества G вида aH, $a \in G$. Для них выполняется:

1) $|aH| = |H|$ (поскольку $x \mapsto ax$ — биекция);

2) если aH и bH пересекаются, то $aH = bH$ (пусть $ax = by$ для $x, y \in H$; тогда $aH = b(yx^{-1})H = bH$, поскольку $zH = H$ для любого $z \in H$.

Следовательно, G есть объединение непересекающихся левых смежных классов и $|H|$ делит $|G|$. □

Определение 5.4. Подгруппа G, составленная из всех степеней a^n, $n \in \mathbb{Z}$, элемента $a \in G$, называется *циклической* группой, порожденной элементом a, и обозначается через $\langle a \rangle$. □

Порядок группы $\langle a \rangle$ называется также *порядком элемента* a и обозначается через $\operatorname{ord} a$. Имеется две возможности:

1) все элементы $\ldots a^{-2}, a^{-1}, a^0 = e, a, a^2, \ldots$ различны и $\operatorname{ord} a = \infty$;

2) некоторые элементы повторяются: $a^{n_1} = a^{n_2}$, $n_1 > n_2$, и $a^{n_1 - n_2} = e$, $n_1 - n_2 > 0$. Пусть n — минимальное натуральное такое, что $a^n = e$. Тогда все элементы $a^0, a^1, \ldots, a^{n-1}$ различны (почему?) и $n = \operatorname{ord} a$.

Если порядок G конечен, то по теореме Лагранжа $\operatorname{ord} a$ делит $|G|$.

Пример 5.5. Порядок 3 как элемента $\langle \mathbb{F}_5, + \rangle$ равняется 5. Порядок 3 как элемента $\langle \mathbb{F}_5 \setminus \{0\}, * \rangle$ равняется 4. Следовательно, обе указанные группы — циклические. □

Пример 5.6. Пусть $a \in \mathbb{Z}_m^*$. Тогда $\operatorname{ord} a \mid \varphi(m) = |\mathbb{Z}_m^*|$ и $a^{\varphi(m)} \equiv 1 \pmod{m}$. Таким образом, доказана теорема Эйлера. □

5.5 Подполя и расширения полей

Определение 5.5 (подполе и расширение поля). Подмножество $K \subseteq F$ называется *подполем* поля $\langle F, +, * \rangle$, если $\langle K, +, * \rangle$ само является полем. При этом F называется *расширением* поля K. Если $K \neq F$, то K — *собственное* подполе F. Поле, которое не содержит собственных подполей, называется *простым*. □

Пример 5.7. $\mathbb{F}_p$ является простым полем. Действительно, всякое подполе $\mathbb{F}_p$ вместе с мультипликативной единицей 1 обязано содержать также элементы $1+1$, $1+1+1, \ldots$, т. е. совпадать с $\mathbb{F}_p$. □

Теорема 5.5 (поле как векторное пространство). Поле F является векторным пространством над всяким своим подполем K.

Доказательство. Действительно, выполняется система необходимых аксиом:

1) $\langle F, + \rangle$ — абелева группа;

2) $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$, $\alpha \in K$, $v_i \in F$;

3) $(\alpha + \beta)v = \alpha v + \beta v$, $\alpha, \beta \in K$, $v \in F$;

4) $(\alpha\beta)v = \alpha(\beta v)$;

5) $ev = v$. □

Размерность векторного пространства F над K называется *степенью расширения* и обозначается через $[F \colon K]$. Если $[F \colon K] = n$ и $a_1, \ldots, a_n$ — некоторый базис F над K, то всякий элемент F можно однозначно представить в виде

$$k_1 a_1 + \ldots + k_n a_n, \quad k_i \in K.$$

Следствие 5.2. Если F — конечное поле, K — подполе F, то $|F| = |K|^n$, где $n = [F : K]$.

Пример 5.8. $\mathbb{R}$ — подполе $\mathbb{C}$, $[\mathbb{C} \colon \mathbb{R}] = 2$, $\{1, i\}$ — базис $\mathbb{C}$ над $\mathbb{R}$. □

5.6 Характеристика поля

Определение 5.6 (характеристика поля). Пусть e — мультипликативная единица F и $\operatorname{ord} e$ — ее порядок в $\langle F, +\rangle$. *Характеристикой* поля F называется число

$$\operatorname{char} F = \begin{cases} 0, & \operatorname{ord} e = \infty, \\ \operatorname{ord} e, & \text{в противном случае.} \end{cases}$$

Упражнение 5.6. Чему равняется $\operatorname{char} \mathbb{R}$, $\operatorname{char} \mathbb{F}_p$? □

Теорема 5.6 (характеристика поля). Если F — конечное поле, то $\operatorname{char} F$ — простое число.

Доказательство. Пусть $n = \operatorname{char} F$ — составное, т. е. $n = n_1 n_2$, $n_i < n$. Тогда

$$(n_1 e)(n_2 e) = n_1 n_2 e = ne = 0.$$

Следовательно $n_i e = 0$ для некоторого $n_i < n$, что противоречит определению $\operatorname{char} F$. □

Определение 5.7. Два поля F и F' *изоморфны* ($F \cong F'$), если существует биекция $\psi\colon F \to F'$ такая, что $\psi(a+b) = \psi(a) + \psi(b)$ и $\psi(ab) = \psi(a)\psi(b)$ для всех $a, b \in F$. □

Теорема 5.7 (число элементов поля). Всякое конечное поле F состоит из p^n элементов, где $p = \operatorname{char} F$ — простое число.

Доказательство. Рассмотрим множество $K = \{0, e, \ldots, (p-1)e\} = \langle e \rangle$. Перенесем на K операции сложения и умножения поля F. Тогда $K \cong \mathbb{F}_p$ (упр.). Следовательно $|F| = |K|^n = p^n$, где $n = [F : K]$. □

При доказательстве теоремы о характеристике поля мы установили, что всякое конечное поле характеристики p содержит простое подполе $K = \langle e \rangle$, изоморфное $\mathbb{F}_p$ (изоморфизм $\psi\colon \mathbb{F}_p \to K$ задается правилом $k \mapsto ke$). Оказывается, что справедлив и более общий результат.

Теорема 5.8 (единственность конечного поля). Всякое конечное поле F из p^n элементов изоморфно полю $P = \mathbb{F}_p[x]/(f)$, где f — неприводимый многочлен степени n над $\mathbb{F}_p$.

Пример 5.9. $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$. □

Мы убедились что все конечные поля из $q = p^n$ элементов изоморфны друг другу, т. е. могут быть получены друг из друга переобозначением своих элементов. Поэтому можно считать, что мы имеем дело с одним единственным полем из q элементов. Такое поле будем обозначать через $\mathbb{F}_q$.

5.7 Лемма о степени суммы и разности

Для всякого элемента a поля ненулевой характеристики p выполняется:

$$pa = p(ea) = (pe)a = 0.$$

Воспользуемся данным фактом для доказательства следующего полезного результата.

Лемма 5.1 (о степени суммы и разности). Пусть F — поле ненулевой характеристики p. Тогда

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ и } (a-b)^{p^n} = a^{p^n} - b^{p^n}, \quad n \in \mathbb{N}.$$

Доказательство. Воспользуемся тем фактом, что для простого p и $1 \leqslant i \leqslant p-1$ выполняется

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \equiv 0 \pmod{p}.$$

Действительно, все множители в знаменатели взаимно просты с p и множитель p в числителе не может сократиться.

Поэтому

$$(a+b)^p = (a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \ldots + \binom{p}{p-1} a b^{p-1} + b^p = a^p + b^p, \qquad □$$

откуда индукцией по n получаем первое тождество. Второе тождество следует из равенства

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n}.$$

5.8 Мультипликативная группа конечного поля

Обозначим через F^* мультипликативную группу ненулевых элементов поля F.

Теорема 5.9. Группа $\mathbb{F}_q^*$ является циклической.

Для доказательства нам потребуется следующая лемма

Лемма 5.2. Пусть G — абелева группа. Если G содержит элементы порядков m и n, то G содержит также элемент порядка $[m, n]$.

Доказательство. Пусть элементы $a, b \in G$ имеют порядки $\operatorname{ord} a = m$, $\operatorname{ord} b = n$. Пусть $d = (m, n)$. Рассмотрим два случая.

Случай 1: $d = 1$. Существует обратный $r = m^{-1} \bmod n$ и $rm + sn = 1$ для некоторого целого s. Пусть $c = a^s b^r$. Имеем

$$c^m = a^{sm} b^{rm} = b^{1-sn} = b(b^n)^{-s} = b, \quad c^n = a^{sn} b^{rn} = a^{1-rm} = a(a^m)^{-r} = a.$$

Если $c^k = e$, то $c^{km} = b^k = e$ и $n \mid k$ (упр.). Аналогично, $m \mid k$ и, в совокупности, $mn \mid k$. С другой стороны, $c^{mn} = b^n = a^m = e$. Поэтому $mn = [m, n] = \operatorname{ord} c$.

Случай 2: $d > 1$. В общем случае, мы можем разложить m и n на множители

$$m = m_0 m_1, \quad n = n_0 n_1,$$

так, что $(m_0, n_0) = 1$ и $[m, n] = m_0 n_0$. Элементы a^{m_1} и b^{n_1} имеют порядок m_0 и n_0 соответственно. Следовательно, $\operatorname{ord} a^{m_0} b^{n_0} = m_0 n_0 = [m, n]$. □

Упражнение 5.7. При доказательстве леммы мы воспользовались следующим фактом: если $\operatorname{ord} a = m$ $\operatorname{ord} a^n = m/d$, где $d = (m, n)$. Доказать этот факт. □

Доказательство (теоремы). Обозначим через r НОК порядков элементов $\mathbb{F}_q^*$. В силу доказанной леммы, в группе $\mathbb{F}_q^*$ имеется элемент порядка r и группа не является циклической только если $r < q - 1$. При этом порядок каждого элемента $\mathbb{F}_q^*$ делит r и многочлен $x^r - 1$ имеет в $\mathbb{F}_q$ $q - 1 > r$ корней, что невозможно. □

Согласно теореме существует элемент $\alpha \in \mathbb{F}_q^*$ такой, что $\mathbb{F}_q^* = \langle \alpha \rangle$. Данный элемент называется *примитивным элементом* поля $\mathbb{F}_q$. Если d взаимно просто с $q - 1$, то α^d также будет примитивным элементом. Таким образом, всего имеется

$$|\mathbb{Z}_{q-1}^*| = \varphi(q-1) = (q-1) \prod_{p \mid q-1} \left(1 - \frac{1}{p}\right)$$

различных примитивных элементов поля $\mathbb{F}_q$.

Пример 5.10. В поле $\mathbb{F}_4$, построенном нами ранее, имеется $\varphi(3) = 2$ примитивных элемента: x и $x+1$. Действительно,

$$\begin{aligned} x^2 &= x + 1, \quad x^3 = 1, \\ (x+1)^2 &= x, \quad (x+1)^3 = 1. \end{aligned}$$

□

5.9 Функция «след»

Определение 5.8. Пусть K — поле из q элементов и F — расширение K степени m. *Следом* элемента $a \in F$ над K называется величина

$$\operatorname{Tr}_{F/K}(a) = a + a^q + a^{q^2} + \ldots + a^{q^{m-1}}.$$

Если K — простое подполе F, то $\operatorname{Tr}_{F/K}(a)$ называется *абсолютным следом* и обозначается просто $\operatorname{Tr}_F(a)$ или даже $\operatorname{Tr}(a)$. □

Теорема 5.10 (свойства следа). Функция $\mathrm{Tr}_{F/K}$ обладает следующими свойствами:

(1) $\mathrm{Tr}_{F/K}(a^q) = \mathrm{Tr}_{F/K}(a)^q = \mathrm{Tr}_{F/K}(a)$ для всех $a \in F$;

(2) $\mathrm{Tr}_{F/K}(a) \in K$ для всех $a \in F$;

(3) $\mathrm{Tr}_{F/K}(a+b) = \mathrm{Tr}_{F/K}(a) + \mathrm{Tr}_{F/K}(b)$ для всех $a, b \in F$;

(4) $\mathrm{Tr}_{F/K}(\alpha a) = \alpha\,\mathrm{Tr}_{F/K}(a)$ для всех $\alpha \in K$, $a \in F$;

(5) $\mathrm{Tr}_{F/K}$ является сюръективным отображением $F \to K$ (отображением “на”).

Лемма 5.3. Для всех $\alpha \in K$ выполняется: $\alpha^q = \alpha$. Если для $\alpha \in F$ выполняется $\alpha^q = \alpha$, то $\alpha \in K$.

Доказательство. Равенство $\alpha^q = \alpha$ очевидно выполняется для $\alpha = 0$. Для ненулевого α по теореме Лагранжа $\operatorname{ord}\alpha$ делит порядок $q-1$ мультипликативной группы K^*. Следовательно $\alpha^{q-1} = 1$ или $\alpha^q = \alpha$.

Все элементы K являются корнями многочлена $f(x) = x^q - x \in F[x]$. Если $f(\alpha) = 0$ для некоторого $\alpha \notin K$, то многочлен f степени q имеет $> q$ корней, что невозможно. □

Доказательство. **1.** Будем учитывать лемму о степени суммы ($(a+b)^q = a^q + b^q$) и тот факт, что $a^{q^m} = a$. Имеем

$$\mathrm{Tr}_{F/K}(a^q) = a^q + a^{q^2} + \ldots + a^{q^{m-1}} + a^{q^m} = \begin{cases} a^q + a^{q^2} + \ldots + a^{q^{m-1}} + a = \mathrm{Tr}_{F/K}(a), \\ (a + a^q + \ldots + a^{q^{m-1}})^q = \mathrm{Tr}_{F/K}(a)^q. \end{cases}$$

2. Согласно (1) $\mathrm{Tr}_{F/K}(a)^q - \mathrm{Tr}_{F/K}(a) = 0$. Следовательно, элемент $\mathrm{Tr}_{F/K}(a)$ лежит в подполе из q элементов, т. е. в K.

3. Следует из леммы о степени суммы.

4. Проверяется непосредственно с учетом того, что $\alpha^q = \alpha$.

5. С учетом (4) достаточно показать, что имеется элемент $a \in F$ такой, что $\mathrm{Tr}_{F/K}(a) \neq 0$. Ясно, что $\mathrm{Tr}_{F/K}(a) = 0$ только если a является корнем многочлена $x + x^q + x^{q^2} + \ldots + x^{q^{m-1}} \in K[x]$. Данный многочлен может иметь не более q^{m-1} корней в F. Но $|F| = q^m$ и нужный нам элемент a существует. □

Пусть F и K рассматриваются как векторные пространства над полем K (размерности m и 1 соответственно). Доказанная теорема означает, что отображение $\mathrm{Tr}_{F/K}$ является линейным отображением F на K. Более того,

Теорема 5.11. Линейными отображениями $F \to K$ являются отображения вида

$$L_b\colon a \mapsto \mathrm{Tr}_{F/K}(ab), \quad b \in F,$$

и только они.

Доказательство. Всего имеется q^m различных линейных отображений $F \to K$ (действие линейного отображения $L\colon F \to K$ однозначно задается выбором элементов $L(a_1), \ldots, L(a_m)$, где $a_1, \ldots, a_m$ — базис F над K.

Отображения L_b и L_c различны для $b \neq c$ (если $L_b(a(b-c)^{-1}) = L_c(a(b-c)^{-1})$ для всех $a \in F$, то $Tr_{F/K}(a) = 0$ для всех a, противоречие с п. (5) теоремы), следовательно, только такими отображениями исчерпываются линейные. □