ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Конечные поля

Учебное пособие
«Конечные поля»

Автор: профессор кафедры алгебры
и дискретной математики
В.В. Кабанов

Екатеринбург
2008

1. Вложения областей целостности в поля

Пусть $R, +, \cdot$ – кольцо. Кольцо R называется кольцом без делителей нуля, если для любых $r, s \in R$ из $rs = 0$ следует, что $r = 0$ или $s = 0$. Областью целостности называется ассоциативно-коммутативное кольцо с единицей не равной нулю и без делителей нуля. В области целостности выполняется *закон сокращения на ненулевые элементы*: если $a, b, c \in R,\ a \neq 0$ и $ab = ac$ то $b = c$.

Примеры областей целостности.

1) Любые поля; 2) Кольцо $\mathbb{Z}$; 3) кольцо многочленов $\mathbb{F}[x]$ над произвольным полем $\mathbb{F}$.

Теорема 1.1. *Любая область целостности изоморфно вложима в подходящее поле.*

Доказательство. Пусть R - область целостности. На множестве $R \times (R \backslash \{0\} = \{(a, b) | a, b \in R ab \neq 0\}$ определим бинарное отношение ρ, полагая, $(a, b)\rho(c, d) \Leftrightarrow ad = bc$.

Проверим является ли ρ отношением эквивалентности:

1) рефлексивность. Для любого элемента $(a, b)\rho(a, b)$, так как $ab = ba$;

2) симметричность. Для любых $(a, b)\rho(c, d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c, d)\rho(a, b)$;

3) транзитивность. Пусть $(a, b)\rho(c, d)\rho(u, v)$. Тогда $ad = bc$ и $cv = du \Rightarrow adcv = bcbu$. Если $c \neq 0$, то сокращаем на c и d, получаем $av = bu$. Если $c = 0$, то, очевидно, $a = u = 0$, снова получаем $av = bu$. Осталось заметить. что из $av = bu$ вытекает $(a, b)\rho(u, v)$.

Через $[a, b]$ обозначим класс эквивалентности ρ, содержащий (a, b). Положим

$$\mathbb{F} = \{[a, b] / a, b \in R \text{ и } \ b \neq 0\}.$$

Определим на $\mathbb{F}$ операции $+$ и $\cdot$, полагая

$$[a, b] + [c, d] = [ad + bc, bd],$$
$$[a, b] \cdot [c, d] = [ac, bd].$$

Проверим корректность этих определений. Пусть $(a,b)\rho(a_1,b_1)$, $(c,d)\rho(c_1,d_1)$, тогда $ab_1 = ba_1$, $cd_1 = dc_1$, откуда выводим, $(ad+bc)b_1d_1 = adb_1d_1 + bb_1c_1d = ba_1dd_1 + bb_1dc_1 = bd(a_1d_1 + b_1c_1)$ и $(a+c)(b_1d_1) = (bd)(a_1c_1)$, т.е. $(ad+bc,bd)\rho(a_1d_1+b_1c_1,b_1d_1)$ и $(ac,bd)\rho(a_1c_1,b_1,d_1)$.

Покажем, что $\mathbb{F},+$ – абелева группа.

1.Ассоциативность.

$$[a,b]+([c,d]+[u,v]) = [a,b]+[cv+du,dv] =$$
$$= [adv+bcv+bdu,bdv] = [ad+bc,bd]+[u,v] =$$
$$= ([a,b]+[c,d])+[u,v].$$

2. Коммутативность. $[a,b]+[c,d] = [ad+bc,bd] = [cb+ad,bd] = [c,d]+[a,b]$.

3. Существование нейтрального элемента. $[a,b]+[0,d] = [ad,bd] = [a,b]$, т. е. $0 = [0.d]$ для любого $d \in R\backslash\{0\}$.

4. Существование противоположного элемента. $-[a,b] = [-a,b]$, так как $[a,b]+[-a,b] = [0,b^2] = 0$. Очевидно, операция $(\circ)$ в $\mathbb{F}$ ассоциативна, коммутативна и $1 = [1,1]$ – единица, причем $[1,1] \neq [0,d]$, для $d \neq 0$.

Пусть $[a,b] \in \mathbb{F}$ и $[a,b] \neq 0$, тогда $a \neq 0$. Покажем, что

$$[a,b]^{-1} = [b,a].$$

Действительно, $[a,b][b,a] = [ab,ba] = [1,1] = 1$, ясно что $[d,d] = [1,1]$, для любого $d \in R\backslash\{0\}$.

Для того, чтобы доказать, что $(\mathbb{F},+,\cdot)$ – поле, осталось проверить дистрибутивность умножения относительно сложения: $[u,v]([a,b]+[c,d]) = [u,v][ad+bc,bd] = [uad+ubc,vbd]$ $[u,v]([a,b]+[c,d]) = [u,v]+[ad+bc,bd] = [uad+buc,vbd] = [uv][a,b]+[u,v][c,d] = [au,vb]+[uc,vd] = [uavd+vbuc,vbvd] = [uad+ubc,vbd][v,v] = [uad+ubc,vbd]$.

Итак, $\mathbb{F}$ – поле.

Рассмотрим отображение $\varphi(x) = [x,1]$ из R в $\mathbb{F}$. Это отображение инъективно, так как $\varphi(a) = \varphi(b) \Rightarrow [a,1] = [b,1] \Rightarrow a = b$.

Оно является гомоморфизмом, так как для любых $a, b \in R$ выполняется

$$\varphi(a+b) = [a+b,1] = [a,1] + [b,1] = \varphi(a) + \varphi(b),$$
$$\varphi(ab) = [ab,1] = [a,1][b,1] = \varphi(a)\varphi(b).$$

Таким образом, φ – изоморфизм из области целостности R в поле $\mathbb{F}$. $\square$

Заметим, что если отождествить каждое $u \in R$ с $[u,1]$, то $R \subset \mathbb{F}$ и $[a,b] = [a,1][1,b] = [a,1][b,1]^{-1} = ab^{-1} = a/b$ для любых $a, b \in R$ и $b \neq 0$, то построенное поле $\mathbb{F}$ называется полем частных области целостности R.

Примеры.

1. R – поле частных для $\mathbb{Z}$;

2. Пусть $\mathbb{F}$ – поле. Поле частных для $\mathbb{F}[x]$ обозначим $\mathbb{F}(x)$ и назовем *полем рациональных дробей над* $\mathbb{F}$.

2. Китайская теорема об остатках

Пусть $\mathbb{F}$ – поле и $f, g, h \in \mathbb{F}[x]$. Соотношение $g - h \in (f)$ часто записывают в виде $g \equiv h(\mathrm{mod}\ f)$, и по аналогии с целыми числами говорят, что g и h сравнимы по модулю f.

Теорема 2.1. *Пусть $f_1, \ldots, f_m$ – попарно взаимно простые многочлены над полем $\mathbb{F}$, а $g_1, \ldots, g_m$ – произвольные многочлены над $\mathbb{F}$. Тогда система сравнений*

$$h \equiv g_i(\mathrm{mod}\ f_i)\,(i = 1, \ldots, m)$$

имеет единственное решение $h \in \mathbb{F}[x]$ по модулю $f_1 \ldots f_m$.

Доказательство. Ясно, что для любого $i = 1, \ldots, m$ выполняется

$$HOD(f_i, \prod_{j \neq i} f_j) = 1.$$

Поэтому существуют такие $u_i, v_i \in \mathbb{F}[x]$, что

$$u_i f_i + v_i \prod_{j \neq i} f_j = 1.$$

Ясно, что $v_i \prod\limits_{j \neq i} f_j \equiv 1(\mathrm{mod}\ f_i)$, следовательно, $g_i v_i \prod\limits_{j \neq i} f_j \equiv g_i$ $(\mathrm{mod}\ f_i)$. Положим $h \rightleftharpoons \sum\limits_{k=1}^{m} (g_k v_k \prod\limits_{j \neq k} f_j)$. Тогда в силу предыдущего для любого $i = 1, \ldots, m$ имеем $h \equiv g_i(\mathrm{mod}\ f_i)$.

Предположим, что h_1 – еще одно решение нашей системы сравнений. Тогда $f_1, \ldots, f_m | h_1 - h \Rightarrow f_1 \cdot \ldots \cdot f_m | h_1 - h \Rightarrow h_1 \equiv h\ (\mathrm{mod}\ f_1 \cdot \ldots \cdot f_m)$. □

Китайскую теорему об остатках часто применяют в случае, когда $f_1, \ldots, f_m$ – это набор различных нормированных неприводимых многочленов над полем $\mathbb{F}$.

Китайская теорема об остатках была известна древним китайцам для случая целых чисел и использовалась ими для вычислений в астрономии.

3. Алгебраические расширения полей

Пусть $\mathbb{K}$ – некоторое расширение поля $\mathbb{F}$. Тогда на $\mathbb{K}$ можно смотреть как на векторное пространство над $\mathbb{F}$ относительно сложения и умножения на элементы из $\mathbb{F}$. Если $\mathbb{K}$ конечномерно над $\mathbb{F}$, то $\mathbb{K}$ называют *конечным расширением* поля $\mathbb{F}$. Размерность $\mathbb{K}$ над $\mathbb{F}$ называют *степенью поля* $\mathbb{K}$ над полем $\mathbb{F}$ и обозначают через $[\mathbb{K} : \mathbb{F}]$.

Теорема 3.1. *Пусть* $\mathbb{F}$ *– поле и* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *– башня конечных расширений. Тогда* $\mathbb{L}$ *– конечное расширение поля* $\mathbb{F}$ *и*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}] \cdot [\mathbb{L} : \mathbb{K}].$$

Доказательство. Положим $[\mathbb{K} : \mathbb{F}] = n$ и $[\mathbb{L} : \mathbb{K}] = m$. Пусть $\alpha_1, \ldots, \alpha_n$ – базис $\mathbb{K}$ над $\mathbb{F}$, и $\beta_1, \ldots, \beta_m$ – базис $\mathbb{L}$ над $\mathbb{K}$. Покажем, что

$$\{\alpha_i\beta_j | i = 1, \ldots, n;\ j = 1, \ldots, m\} \tag{1}$$

– базис $\mathbb{L}$ над $\mathbb{F}$.

Пусть $\beta \in \mathbb{L}$. Тогда $\beta = \sum\limits_{j=1}^{m} \gamma_j\beta_j$ для некоторых $\gamma_1, \ldots, \gamma_m \in \mathbb{K}$ и для любого$j = 1, \ldots, m$ существуют такие $\lambda_{j1}, \ldots, \lambda_{jn} \in \mathbb{F}$, что $\gamma_j = \sum\limits_{i=1}^{n} \lambda_{ji}\alpha_i$. Отсюда получаем $\beta = \sum\limits_{j=1}^{m} \left(\sum\limits_{i=1}^{n} \lambda_{ji}\alpha_i \right) \beta_j = \sum\limits_{j=1}^{m} \sum\limits_{i=1}^{n} \lambda_{ji}\alpha_i\beta_j$, то есть (1) – это система образующих пространства $\mathbb{L}$ над $\mathbb{F}$.

Покажем, что она линейно независима. Пусть $\sum\limits_{j=1}^{m} \sum\limits_{i=1}^{n} \lambda_{ji}\alpha_i\beta_j = 0$, для некоторых $\lambda_{ji} \in \mathbb{F}$, где, $j = 1, \ldots, m$; $i = 1, \ldots, n$. Тогда $\sum\limits_{j=1}^{m} \left(\sum\limits_{i=1}^{n} \lambda_{ji}\alpha_i \right) \beta_j = 0 \Rightarrow \sum\limits_{i=1}^{n} \lambda_{ji}\alpha_i = 0$ для любого $j = 1, \ldots, m \Rightarrow$ $\alpha_{ji} = 0$ $(j = 1, \ldots, m;\ \ i = 1, \ldots, n)$. □

Пусть $\mathbb{K}$ – расширение поля $\mathbb{F}$. Элемент $\theta \in \mathbb{K}$ называется *алгебраическим* над $\mathbb{F}$, если θ является корнем некоторого ненуле-

вого многочлена из $\mathbb{F}[x]$. Неалгебраические над полем $\mathbb{F}$ элементы называют *трансцендентными* элементами над $\mathbb{F}$.

Примеры. 1). $\sqrt{2}$ алгебраичен над $\mathbb{Q}$. Это корень многочлена $x^2 - 2 \in \mathbb{Q}[x]$.

2). π, ε – трансцендентны над $\mathbb{Q}$.

Минимальным многочленом алгебраического элемента θ над полем $\mathbb{F}$ называется ненулевой нормированный многочлен наименьшей степени из $\mathbb{F}[x]$, корнем которого является θ. Ясно, что минимальный многочлен единствен и неприводим над $\mathbb{F}$. Его степень *называется степенью элемента* θ *над полем* $\mathbb{F}$.

Лемма 3.1. *Минимальный многочлен элемента* θ *над полем* $\mathbb{F}$ *делит над* $\mathbb{F}$ *любой другой многочлен из* $\mathbb{F}[x]$ *, корнем которого является* θ*.*

Доказательство. Пусть M – минимальный многочлен элемента θ над полем $\mathbb{F}$ и $f(\theta) = 0$, для некоторого $f \in \mathbb{F}[x]$. Разделим f на M с остатком над полем $\mathbb{F}$

$$f = Mq + r,$$

где $\deg\ r < \deg\ M$. Подставляя θ, получим $r(\theta) = 0$. Отсюда, в силу минимальности M, вытекает $r = 0$, то есть $M|f$ над $\mathbb{F}$. $\square$

Расширение $\mathbb{K}$ поля $\mathbb{F}$ называется *алгебраическим*, если каждый элемент из $\mathbb{K}$ алгебраичен над $\mathbb{F}$, и – *трансцендентным*, если хотя бы один элемент из $\mathbb{K}$ трансцендентен над $\mathbb{F}$.

Например, $\mathbb{R}$ – трансцендентное расширение поля $\mathbb{Q}$.

Теорема 3.2. *Любое конечное расширение* $\mathbb{K}$ *поля* $\mathbb{F}$ *является алгебраическим.*

Доказательство. Пусть $[\mathbb{K} : \mathbb{F}] = n$ и $\theta \in \mathbb{K}$. Тогда $1, \theta, \ldots, \theta^n$ – линейно зависимая система над $\mathbb{F}$. Следовательно, существуют $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{F}$, не все равные нулю, для которых $\lambda_0 + \lambda_1\theta + \ldots + \lambda_n\theta^n = 0$. $\square$

Пусть $\mathbb{K}$ – расширение поля $\mathbb{F}$. Возьмем $S \subseteq \mathbb{K}$. Через $\mathbb{F}(S)$ обозначим пересечение всех подполей поля $\mathbb{K}$, содержащих $\mathbb{F} \cup S$. Ясно, что $\mathbb{F}(S)$ – подполе поля $\mathbb{K}$. Это наименьшее расширение поля $\mathbb{F}$ в $\mathbb{K}$, содержащее S . Говорят, что $\mathbb{F}(S)$ получено из $\mathbb{F}$ *присоединением элементов множества* S (относительно поля $\mathbb{K}$). В случае конечного $S = \{\theta_1, \ldots, \theta_m\}$ пишут $\mathbb{F}(S) = \mathbb{F}(\theta_1, \ldots, \theta_m)$. Если S состоит из одного элемента θ, то поле $\mathbb{F}(\theta)$ называется *простым расширением* поля $\mathbb{F}$, а θ – его порождающим элементом. Следующую теорему мы приводим без доказательства. Читатель монет провести доказательство самостоятельно.

Теорема 3.3. *Если элемент θ трансцендентен над полем $\mathbb{F}$, то поле $\mathbb{F}(\theta)$ изоморфно полю $\mathbb{F}(x)$ рациональных дробей над $\mathbb{F}$.*

Теорема 3.4. *Пусть $\mathbb{F}$ – поле и $f \in \mathbb{F}[x]$. Для того чтобы фактор-кольцо $\mathbb{F}[x]/(f)$ было полем, необходимо и достаточно, чтобы многочлен f был неприводим над $\mathbb{F}$.*

Доказательство. Элементами кольца $\mathbb{F}[x]/(f)$ являются смежные классы $[g] = (f) + g$, где $g \in \mathbb{F}[x]$. Очевидно $\mathbb{F}[x]/(f)$ – ассоциативно-коммутативное кольцо с единицей $1 = [1]$ и нулем $0 = [0]$.

Пусть f – неприводимый многочлен над $\mathbb{F}$ и $[g] \neq 0$, для некоторого $g \in F[x]$. Тогда $f \nmid g \Rightarrow HOD(f, g) = 1 \Rightarrow$ существуют $u, v \in \mathbb{F}[x]$ такие, что $fu + gv = 1 \Rightarrow 1 = [1] = [gv] = [g][v] \Rightarrow [g]^{-1} = [v]$. Следовательно, $\mathbb{F}[x]/(f)$ – поле.

Обратно, пусть f не является неприводимым многочленом над $\mathbb{F}$.

Рассмотрим три случая: 1) $f = 0 \Rightarrow \mathbb{F}[x]/(0) \cong \mathbb{F}[x]$ – не поле.

2) $f \in \mathbb{F}\backslash\{0\} \Rightarrow |\mathbb{F}[x]/(f)| = 1$, то есть опять имеем не поле.

3) Пусть f – неприводим над $\mathbb{F} \Rightarrow f = f_1 f_2$ для некоторых $f_1, f_2 \in \mathbb{F}[x]$ таких, что $0 < \deg\ f_1, \deg\ f_2 < \deg\ f$. Тогда получаем $[f_1][f_2] = 0$, где $[f_1] \neq 0$ и $[f_2] \neq 0$, т. е. в $\mathbb{F}[x]/(f)$ есть делители нуля, снова имеем не поле. $\square$

Теорема 3.5. *Многочлены степени 2 и 3 неприводимы над полем* $\mathbb{F}$*, тогда и только тогда, когда он не имеет корней в поле* $\mathbb{F}$*.*

Доказательство. Если многочлен f неприводим над $\mathbb{F}$, то по теореме Безу он не имеет корней в поле $\mathbb{F}$. Обратно, если f приводим над $\mathbb{F}$ и его степень 2 или 3, то он имеет линейный делитель над $\mathbb{F}$, следовательно, он имеет корень в $\mathbb{F}$. □

Пример. В силу теоремы 3.5 многочлен $f = x^2+x+1 \in \mathbb{Z}_2[x]$ неприводим над $\mathbb{Z}_2$. Возможные остатки от деления многочленов из $\mathbb{Z}_2[x]$ на f имеют вид $ax + b$, где $a, b \in \mathbb{Z}_2$. Следовательно, $\mathbb{Z}_2[x]/(f) = \{[0], [1], [x], [x + 1]\}$. Обычно квадратные скобки опускают и пишут $\mathbb{Z}_2[x]/(f) = \{0, 1, x, x + 1\}$.

$\circ$	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

$+$	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

Теорема 3.6. *Пусть* $\mathbb{K}$ *- расширение поля* $\mathbb{F}$*,* $\theta \in \mathbb{K}$ *– алгебраический элемент степени* n *над* $\mathbb{F}$ *и* M *– его минимальный многочлен над* $\mathbb{F}$*. Тогда*

1) существует изоморфизм ψ *поля* $\mathbb{F}[x]/(M)$ *на поле* $\mathbb{F}(\theta)$ *такой, что* $\psi([x]) = \theta$ *и* $\psi([a]) = a$ *для любого* $a \in \mathbb{F}$*;*

2) $1, \theta, \ldots, \theta^{n-1}$ *– базис пространства* $\mathbb{F}(\theta)$ *над* $\mathbb{F}$ *и, следовательно,* $\mathbb{F}(\theta)$ *– конечное расширение степени* n *над полем* $\mathbb{F}$*.*

Доказательство. 1. Рассмотрим отображение φ из $\mathbb{F}[x]$ в $\mathbb{F}(\theta)$, заданное условием $\varphi(f) = f(\theta)$ для любого $f \in \mathbb{F}[x]$. Очевидно, φ – гомоморфизм кольца $\mathbb{F}[x]$ в поле $\mathbb{F}(\theta)$. В силу леммы 3.1 выполняется

$$Ker\varphi = \{f \in \mathbb{F}[x] | f(\theta) = 0\} = (M).$$

По теореме 3.4 и теореме о гомоморфизме колец существует изоморфизм поля $\mathbb{F}[x]/(M)$ на $\mathrm{Im}\varphi$, для которого $\psi([x]) = \theta$ и

$\psi([a]) = a$ для любого $a \in \mathbb{F}$. Поскольку $\mathbb{F} \subseteq \mathrm{Im}\varphi \subseteq \mathbb{F}(\theta)$ и $\theta \in \mathrm{Im}\varphi$, по определению простого расширения поля имеем $\mathrm{Im}\varphi = \mathbb{F}(\theta)$, то есть ψ – искомый изоморфизм.

2. Так как $\mathrm{Im}\varphi = \mathbb{F}(\theta)$, любой элемент $\alpha \in \mathbb{F}(\theta)$ представим в виде $\alpha = f(\theta)$ для некоторого многочлена $f \in \mathbb{F}[x]$. Разделим f на M с остатком над $\mathbb{F}$. Тогда $f = Mq + r$, где $\deg\ r < \deg\ M = n \Rightarrow$ $\alpha = f(\theta) = M(\theta)q(\theta) + r(\theta) = r(\theta)$, то есть α является линейной комбинацией элементов $1, \theta, \ldots, \theta^{n-1}$ с коэффициентами из поля $\mathbb{F}$. С другой стороны, если $f \neq M$ и $f = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} = 0$ для некоторых $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$, то по определению минимального многочлена M имеем $a_0 = a_1 = \ldots = a_{n-1}$, т.е. система элементов $1, \theta, \ldots, \theta^{n-1}$ – линейно независимая система над $\mathbb{F}$. $\square$

Следствие. *Пусть $\theta_1, \ldots, \theta_m$ – элементы поля $\mathbb{K}$, алгебраические над его подполем $\mathbb{F}$. Тогда $\mathbb{F}(\theta_1, \ldots, \theta_m)$ – конечное расширение поля $\mathbb{F}$.*

Доказательство. Индукция по m. База индукции доказана в теореме 3.6. Шаг индукции справедлив в силу равенства $\mathbb{F}(\theta_1, \ldots, \theta_m) = (\mathbb{F}(\theta_1, \ldots, \theta_{m-1})(\theta_m))$ на основании теорем 3.6 и 3.1. $\square$

Следствие. *Пусть $\mathbb{K}$ – конечное расширение степени n поля $\mathbb{F}$. Тогда степень любого элемента из $\mathbb{K}$ над полем $\mathbb{F}$ делит n.*

Доказательство. В силу теоремы 3.2 поле $\mathbb{K}$ является алгебраическим расширением поля $\mathbb{F}$. Пусть θ – элемент степени m поля $\mathbb{K}$ над полем $\mathbb{F}$. Тогда, применяя теорему 3.1 к башне

$\mathbb{F} \subseteq \mathbb{F}(\theta) \subseteq \mathbb{K}$ и учитывая, что $\mathbb{K}$ – конечное расширение поля $\mathbb{F}(\theta)$, в силу теоремы 3.6 получаем $m|n$. $\square$

Простое расширение $\mathbb{F}(\theta)$ называется *простым алгебраическим расширением поля* $\mathbb{F}$, если θ является алгебраическим элементом над $\mathbb{F}$.

4. Поле разложения многочлена

Теорема 4.1. *(Кронекера). Пусть многочлен f неприводим над полем $\mathbb{F}$. Тогда существует простое алгебраическое расширение $\mathbb{F}(\theta)$ поля $\mathbb{F}$ такое, что θ – корень многочлена f.*

Доказательство. В силу теоремы 3.4 фактор-кольцо $\mathbb{L} = \mathbb{F}[x]/(f)$ является полем. Рассмотрим отображение $\varphi(a) = [a]$ ($a \in \mathbb{F}$ из $\mathbb{F}$ в $\mathbb{L}$. Ясно, что φ – изоморфное вложение поля $\mathbb{F}$ в поле $\mathbb{L}$. Отождествим каждый элемент $a \in \mathbb{F}$ с его образом $\varphi(a)$, т.е. положим $a = \varphi(a)$. Тогда $a = [a]$, для любого $a \in \mathbb{F}$. Теперь выполняется $\mathbb{F} \subseteq \mathbb{L}$.

Положим $\theta = [x]$. Пусть $f = a_0 + a_1x + \ldots + a_nx^n$. Тогда

$$f(\theta) = a_0 + a_1\theta + \ldots + a_n\theta^n = [a_0] + [a_1][x] + \ldots + [a_n][x]^n = \\ = [a_0 + a_1x + \ldots + a_nx^n] = [f] = 0,$$

т. е. θ – корень многочлена f.

Для любого $g = b_0 + b_1x + \ldots + d_mx^m \in \mathbb{F}[x]$ имеем $[g] = [b_0 + b_1x + \ldots + b_mx^m] = [b_0] + [b_1][x] + \ldots + [b_m][x]^m = b_0 + b_1\theta + \ldots + b_m\theta^m$, т. е. $\mathbb{L} = \mathbb{F}(\theta)$, и $\mathbb{L}$ – простое алгебраическое расширение поля $\mathbb{F}$ с порождающим элементом θ. $\square$

Лемма 4.1. *(о продолжении изоморфизма). Пусть φ – изоморфизм поля $\mathbb{L}$ на поле L'. Обозначим через $\bar{\varphi}$ изоморфизм кольца $\mathbb{L}[x]$ на кольцо $L'[x]$ индуцируемый φ, т. е. для любых $a_0, a_1, \ldots, a_n \in \mathbb{L}$ положим*

$$\bar{\varphi}(a_0 + a_1x + \ldots + a_nx^n) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n.$$

Пусть f – неприводимый многочлен над $\mathbb{L}$. Тогда $\bar{\varphi}(f)$ неприводим над $\mathbb{L}'$ и существует изоморфизм χ поля $\mathbb{L}[x]/(f)$ на поле $\mathbb{L}'[x]/(\bar{\varphi}(f))$, такой что $\chi([x]) = [x]$ и $\chi([a]) = [\varphi(a)]$ для любого $a \in \mathbb{L}$.

Доказательство. Очевидно, многочлен $\bar{\varphi}(f)$ неприводим над $\mathbb{L}'$. Определим χ, полагая

$$\chi([g]) = [\bar{\varphi}(g)],$$

для любого $g \in \mathbb{L}[x]$. Тривиально проверяется корректность этого определения и то, что χ – искомый изоморфизм.

Пусть многочлен $f \in \mathbb{F}[x]$ имеет положительную степень и $\mathbb{L}$ – некоторое расширение поля $\mathbb{F}$. Поле $\mathbb{L}$ называется полем разложения многочлена f над $\mathbb{F}$, если существуют $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ такие, что:

1) $f = a(x - \alpha_1) \ldots (x - \alpha_n)$;

2) $\mathbb{L} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

Иными словами, поле разложения многочлена f над полем $\mathbb{F}$ – это минимальное расширение поля $\mathbb{F}$, в котором многочлен f *вполне разложим* (т. е. разложим на линейные множители). □

Теорема 4.2. *Пусть f – многочлен положительной степени над полем $\mathbb{F}$. Тогда существует единственное с точностью до изоморфизма поле разложения многочлена f над $\mathbb{F}$.*

Доказательство. Существование. Возьмем неприводимый множитель f_1 многочлена f над $\mathbb{F}$. В силу теоремы 4.1 существует простое расширение $\mathbb{F}_1 = \mathbb{F}(\theta_1)$ поля $\mathbb{F}$ такое, что $f_1(\theta_1) = 0$. Очевидно, $f(\theta_1) = 0 \Rightarrow (x - \theta_1 | f$ над $\mathbb{F}_1$, следовательно, существует $g_1 \in \mathbb{F}_1[x]$ такой, что $f = (x - \theta_1)g_1$. Если g_1 имеет положительную степень, то аналогично предыдущему существует простое расширение $\mathbb{F}_2 = \mathbb{F}_1(\theta_2)$ поля F_1 такое, что $g_1(\theta_2) = 0$ и существует $g_2 \in \mathbb{F}_2[x]$, для которого $g_1 = (x - \theta_2)g_2$ и $f = (x - \theta_1)(x - \theta_2)g_2$. Продолжая этот процесс, мы найдем поле $\mathbb{F}_n \supseteq \mathbb{F}$, в котором f вполне разложим. Его подполе, порожденное над $\mathbb{F}$ всеми корнями многочлена f из $\mathbb{F}_n$, является полем разложения многочлена f над $\mathbb{F}$.

Единственность. Пусть $\mathbb{K}$ и $\mathbb{K}'$ – два поля разложения многочлена f над $\mathbb{F}$. Покажем, что существует изоморфизм поля $\mathbb{K}$ на поле $\mathbb{K}'$, оставляющий на месте элементы поля $\mathbb{F}$.

Будем по очереди присоединять к $\mathbb{F}$ корни многочлена f, лежащие в $\mathbb{K}$, и строить соответствующее изоморфное подполе в $\mathbb{K}'$. Предположим, что уже взята система попарно различных корней $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ многочлена f и для нее существует система $\alpha'_1, \ldots, \alpha'_m \in \mathbb{K}'$ попарно различных корней многочлена f и изоморфизм φ поля $\mathbb{L} = \mathbb{F}(\alpha_1, \ldots, \alpha_m) \subseteq \mathbb{K}$ на поле $\mathbb{L}' = \mathbb{F}(\alpha'_1, \ldots, \alpha'_m) \subseteq \mathbb{K}'$ такие, что $\varphi(a) = a$ для любого $a \in \mathbb{F}$ и $\varphi(\alpha_1) = \alpha'_1, \ldots, \varphi(\alpha_m) = \alpha'_m$. Конечно, если $m = 0$, то полагаем $\mathbb{L} = \mathbb{F} = \mathbb{L}'$.

Рассмотрим два случая.

1 случай. $\mathbb{L} = \mathbb{K}$. Тогда $\mathbb{L}$ – поле разложения многочлена f над $\mathbb{F}$. Поскольку $\mathbb{L}'$ изоморфно $\mathbb{L}$ над $\mathbb{F}, \mathbb{L}'$ также является полем разложения многочлена f над $\mathbb{F}$. Тогда из $\mathbb{L}' \subseteq \mathbb{K}'$ следует $\mathbb{L}' = \mathbb{K}'$ и нужное утверждение доказано.

2 случай. Пусть $\mathbb{L} \subset \mathbb{K}$. Возьмем корень α_{m+1} многочлена f, лежащий в $\mathbb{K}\backslash\mathbb{L}$. Пусть M – минимальный многочлен элемента α_{m+1} над $\mathbb{L}$. Тогда M неприводим над $\mathbb{L}$, $\deg\ M > 1$ и $M|f$ над $\mathbb{L}$. Следовательно, мы находимся в условии леммы 4.1 $\circ$ продолжении изоморфизма.

Рассмотрим неприводимый многочлен $\bar{\varphi}(M)$ над $\mathbb{L}'$ и изоморфизм χ поля $\mathbb{L}[x]/(M)$ на поле $\mathbb{L}'[x]/(\bar{\varphi}(M))$ такой, что $\chi([x]) = [x]$ и $\chi([a]) = [\varphi(a)]$ для любого $a \in \mathbb{L}$. Очевидно, $\bar{\varphi}(M)|f$ над $\mathbb{L}'$.

Рассмотрим расширение поля $\mathbb{K}'$, в котором $\bar{\varphi}(M)$ имеет корень α'_{m+1}. В силу делимости этот корень будет корнем и для f, т. е. он лежит в K'. Поскольку $\deg \bar{\varphi}(M) = \deg M > 1$, мы имеем $\alpha'_{m+1} \in \mathbb{K}'\backslash\mathbb{L}'$, т. е. $\alpha'_{m+1} \neq \alpha'_1, \ldots, \alpha'_m$.

В силу теоремы 3.6 из § 3 существует изоморфизм ψ_1 поля $\mathbb{L}[x]/(M)$ на поле $\mathbb{L}(\alpha_{m+1}) \subseteq \mathbb{K}$ такой, что $\psi_1([x]) = \alpha_{m+1}$ и $\psi_1([a]) = a$ для любого $a \in \mathbb{L}$.

Аналогично, существует изоморфизм ψ_2 поля $\mathbb{L}'[x]/(\bar{\varphi}(M))$ на поле $\mathbb{L}'(\alpha'_{m+1}) \subseteq \mathbb{K}'$ такой, что $\psi_2([x]) = \alpha'_{m+1}$ и $\psi_2([b]) = b$ для любого $b \in \mathbb{L}'$.

Заметим, что $\mathbb{L}(\alpha_{m+1}) = \mathbb{F}(\alpha_1, \ldots, \alpha_m)(\alpha_{m+1}) = \mathbb{F}(\alpha_1, \ldots, \alpha_{m+1})$,

$$\mathbb{L}'(\alpha'_{m+1}) = \mathbb{F}(\alpha'_1, \ldots, \alpha'_m)(\alpha'_{m+1}) = \mathbb{F}(\alpha'_1, \ldots, \alpha'_{m+1}).$$

ris.

Рассмотрим теперь изоморфизм $\psi = \psi_2 \chi \psi_1^{-1}$ поля $\mathbb{L}(\alpha_{m+1})$ на поле $L'(\alpha'_{m+1})$. Для любого $a \in \mathbb{L}$ имеем

$$\psi(a) = \psi_2 \chi \psi_1^{-1}(a) = \psi_2 \chi([a]) = \psi_2([\varphi(a)]) = \varphi(a),$$

т. е. ψ порождает φ. Кроме того,

$$\psi(\alpha_{m+1}) = \psi_2 \chi \psi_1^{-1}(\alpha_{m+1}) = \psi_2 \chi([x]) = \psi([x]) = \alpha'_{m+1}.$$

Итак, ψ – изоморфизм поля $\mathbb{F}(\alpha_1, \ldots, \alpha_{m+1}) \subseteq \mathbb{K}$ на поле $\mathbb{F}(\alpha'_1, \ldots, \alpha'_{m+1}) \subseteq \mathbb{K}'$ такой, что $\psi(a) = a$ для любого $a \in \mathbb{F}$ и $\psi(\alpha_1) = \alpha'_1, \ldots, \psi(\alpha_{m+1}) = \alpha'_{m+1}$.

Продолжая процесс присоединения корней многочлена f, лежащих в $\mathbb{K}$, после конечного числа шагов, отвечающих следствию , мы обязательно окажемся в условии следствия и требуемое утверждение будет доказано. □

5. Характеризация конечных полей

Пусть $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{F}[x]$, где $\mathbb{F}$ – поле. Положим,

$$f' \rightleftharpoons a_1 + 2a_2 x + \ldots + n a_n x^{n-1} \in \mathbb{F}[x].$$

Напомним свойства этой процедуры. Для любых $f, g, f_1, \ldots, f_m \in \mathbb{F}[x], a, b \in \mathbb{F}$ и $k \in \mathbb{N}$ выполняется:

1. $(af + bg)' = af' + bg'$,
2. $(fg)' = f'g + fg'$,
3. $(f_1 \cdot \ldots \cdot f_m)' = \sum\limits_{i=1}^{m} f_1 \ldots f_{i-1} f'_i f_{i+1} \ldots f_m$,
4. $(f^k)' = k f^{k-1} f'$.

Лемма 5.1. *Пусть f_1 – неприводимый множитель положительной степени кратности $k \geq 1$ многочлена f над полем $\mathbb{F}$. Тогда $f_1^{k-1} | f'$ над $\mathbb{F}$.*

Доказательство. Пусть $f = f_1^k g$, где $g \in \mathbb{F}[x]$. Тогда $f' = kf_1^{k-1}f_1'g + f_1^k g' = f_1^{k-1}(kf_1'g + f_1 g')$. □

Следствие. *Пусть $f \in \mathbb{F}[x]$, $\mathbb{F}$ – поле и $HOD(f, f') = 1$. Тогда многочлен f не имеет кратных неприводимых множителей положительной степени над полем $\mathbb{F}$ и не имеет кратных корней в любом расширении поля $\mathbb{F}$.*

Доказательство. Существуют $u, v \in \mathbb{F}[x]$ такие, что $fu + f'v = 1$. Осталось применить лемму 5.1. □

Лемма 5.2. *Пусть $\mathbb{F}$ – поле простой характеристики p. Тогда для любых $a, b \in \mathbb{F}$ и $n \in \mathbb{N}$ выполняется $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ и $(a-b)^{p^n} = a^{p^n} - b^{p^n}$.*

Доказательство. По формуле Ньютона имеем $(a+b)^p = \sum\limits_{k=0}^{p} c_p^k a^{p-k} b^k$. При $k = 1, \ldots, p-1$ выполняется $c_p^k = \frac{p!}{k!(p-k)!} \equiv 0 (\mathrm{mod} p)$, так как простое число p делит числитель и не делит знаменатель. Следовательно, $(a+b)^p = a^p + b^p$. Отсюда следует $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Поскольку $a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n}$, получаем второе равенство. □

Лемма 5.3. *Пусть $\mathbb{K}$ – конечное расширение степени m конечного поля $\mathbb{F}$ порядка q. Тогда $|\mathbb{K}| = q^m$.*

Доказательство. Пусть $\alpha_1, \ldots, \alpha_m$ – базис $\mathbb{K}$ над $\mathbb{F}$. Тогда любой элемент из $\mathbb{K}$ единственным образом представим в виде $a_1\alpha_1 + \ldots + a_m\alpha_m$, где $a_1, \ldots, a_m \in \mathbb{F}$, следовательно, $|\mathbb{K}| = q^m$. □

Теорема 5.1. 1) *Пусть $\mathbb{F}$ – конечное поле. Тогда $|\mathbb{F}| = p^n$ для некоторого простого числа p и $n \in \mathbb{N}$.*

2) *Для любого простого числа p и любого $n \in \mathbb{N}$ существует поле $\mathbb{F}$ порядка p^n.*

3) *Любое конечное поле порядка p^n, где p – простое число, является полем разложения многочлена $x^{p^n} - x$ над полем, изоморфным полю $\mathbb{Z}_p$.*

4) *Любые два конечных поля порядка p^n изоморфны.*

Доказательство. 1) Мы можем считать, что $\mathbb{Z}_p \subseteq \mathbb{F}$. Пусть $n = [\mathbb{F} : \mathbb{Z}_p]$. Тогда по лемме 5.3 имеем $|\mathbb{F}| = p^n$.

2) Положим $q = p^n$. Возьмем в качестве $\mathbb{F}$ поле разложения многочлена $x^q - x$ над $\mathbb{Z}_p$. Многочлен $f = x^q - x$ имеет q различных корней в поле $\mathbb{F}$, так как его производный многочлен $f' = qx^{q-1} - 1 = -1 \neq 0$ в $\mathbb{Z}_p[x]$, и поэтому в силу следствия из леммы 5.1 f не имеет кратных корней.

Положим $S = \{a \in \mathbb{F} | a^q - a = 0\}$. Легко видеть, что S является подполем поля $\mathbb{F}$. Действительно, $0, 1 \in S$; если $a, b \in S$, то в силу леммы 5.2 $a - b \in S$; если $a, b \in S$ и $b \neq 0$, то $(ab^{-1})^q = a^q(bq)^{-1} = ab^{-1}$, т. е. $ab^{-1} \in S$.

Поскольку поле S состоит из всех q корней многочлена $x^q - x$, лежащих в $\mathbb{F}$, мы имеем $|S| = q$ и $x^q - x = \prod\limits_{\alpha \in S} (x - \alpha)$. В силу минимальности $\mathbb{F}$ выполняется $S = \mathbb{F}$ и $|\mathbb{F}| = q$.

3) Пусть $\mathbb{F}$ – конечное поле порядка $q = p^n$. Порядок простого подполя делит $|\mathbb{F}|$, следовательно, $char\mathbb{F} = p$ и мы можем считать, что $\mathbb{Z}_p \subseteq \mathbb{F}$.

Покажем, что каждый элемент из $\mathbb{F}$ является корнем многочлена $x^q - x$. Для нуля $0 \in \mathbb{F}$ это очевидно. Ненулевые элементы поля $\mathbb{F}$ образуют по умножению группу $\mathbb{F}^*$ порядка $q - 1$. По теореме Лагранжа для любого $a \in \mathbb{F}^*$ имеем $a^{q-1} = 1 \Rightarrow a^q - a = 0$.

Следовательно, многочлен $x^q - x$ имеет в поле $\mathbb{F}$ точно q различных корней. Отсюда следует, что $\mathbb{F}$ является полем разложения многочлена $x^q - x$ над $\mathbb{Z}_p$.

4) вытекает из 3) в силу единственности с точностью до изоморфизма поля разложимого многочлена $x^q - x$ над $\mathbb{Z}_p$. $\square$

Следствие. *Пусть* $\mathbb{F}$ *– конечное поле порядка* q*. Тогда*

$$x^q - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha).$$

Поле порядка p^n , где p – простое число и $n \in \mathbb{N}$, называют *полем Галуа* и обозначают через $GF(p^n)$ или через $\mathbb{F}_q$, где $q = p^n$. Далее вместо $\mathbb{Z}_p$ будем писать $\mathbb{F}_p$.

Лемма 5.4. *Если* $m|n$ *над* $\mathbb{N}$*, то* $x^m - 1 | x^n - 1$ *над произвольным полем* $\mathbb{F}$ *и в* $\mathbb{F}(x)$ *выполняется*

$$\frac{x^n - 1}{x^m - 1} = 1 = x^m + x^{2m} + \ldots + x^{(k-1)m},$$

где $n = km$*.*

Доказательство. Пусть $n = km$. Тогда

$$\begin{aligned}&(x^m - 1)(1 + x^m + \ldots + x^{(k-2)m} + x^{(k-1)m}) = \\ &= x^m + x^{2m} + \ldots + x^{(k-1)m} + x^{km} - 1 - x^m - x^{2m} - \ldots - x^{(k-1)m} = \\ &= x^{km} - 1 = x^n - 1.\end{aligned}$$

□

Теорема 5.2. *Пусть* p *– простое число,* $n \in \mathbb{N}$ *и* $q = p^n$*. Тогда*

1) *любое подполе поля* $\mathbb{F}_q$ *имеет порядок* p^m*, где* $m|n$ *и* $m \in \mathbb{N}$*;*

2) *для любого* $m \in \mathbb{N}$ *такого что* $m|n$*, в поле* $\mathbb{F}_q$ *существует точно одно подполе порядка* p^m*.*

Доказательство. 1) Если $\mathbb{F}$ – подполе поля $\mathbb{F}_q$, то по теореме Лагранжа $|\mathbb{F}|$ делит q, поэтому $|F| = p^m$ для некоторого $m \in \mathbb{N}$. Пусть $[\mathbb{F}_q : \mathbb{F}] = k$. Тогда в силу леммы 5.3 имеем $(p^m)^k = p^n \Rightarrow mk = n$, т. е. $m|n$.

2) Пусть $m|n$. Тогда в силу леммы 5.4 имеем $p^m - 1 | p^n - 1 \Rightarrow x^{p^m-1} - 1 | x^{p^n-1} - 1 \Rightarrow x^{p^m} - 1 | x^{p^n} - x$ над $\mathbb{F}_p$. В поле $\mathbb{F}_q$ многочлен $x^q - x$ вполне разложим, следовательно, в поле $\mathbb{F}_q$ вполне разложим и многочлен $x^{p^m} - x$, отсюда следует, что поле $\mathbb{F}_q$ содержит

поле разложения $\mathbb{F}_{p^m}$ многочлена $x^{p^m} - x$ над $\mathbb{F}_p$, которое имеет порядок p^m. Если бы в $\mathbb{F}_q$ было два различных подполя порядка p^m, то многочлен $x^{p^m} - x$ имел бы в поле $\mathbb{F}_q$ более чем p^m корней, что невозможно. □

Пример. Решетка подполей поля $\mathbb{F}_{2^{30}}$

Поскольку $m!|n!$ для любых $m, n \in \mathbb{N}$ таких, что $m < n$, в силу теоремы 5.2 мы имеем следующую башню конечных полей:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq \ldots \subseteq \mathbb{F}_{p^{n!}} \subseteq \ldots,$$

где p – простое число. Положим $\mathbb{F}_{p^\infty} \rightleftharpoons \bigcup\limits_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$, где операции $+$ и $\cdot$ определяются естественным образом. Это поле, которое для любого $n \in \mathbb{N}$ содержит точно одно подполе из p^n элементов по теореме 5.2.

Теорема 5.3. *F_q^* – циклическая группа.*

Доказательство. Пусть α – элемент наименьшего порядка из F_q^* и его порядок $ord(\alpha) = k$. Покажем, что порядок $l = ord(\beta)$ произвольного элемента $\beta \in \mathbb{F}_q^*$ делит k, т. е. $l|k$. Возьмем разложения на простые множители $k = p_1^{s_1} \ldots p_m^{s_m}$

и $l = p_1^{t_1} \ldots p_m^{t_m}$, где $s_1, \ldots, s_m, t_1, \ldots, t_m \geq 0$. Положим $k_1 = p_2^{s_2} \ldots p_m^{s_m}$ и $l_1 = p_2^{t_2} \ldots p_m^{t_m}$. Очевидно, $(\alpha^{p_1^{s_1}}) = k_1$, $(\beta^{l_1}) = p_1^{t_1}$, $HOD(k_1, p_1^{t_1}) = 1 \Rightarrow ord(\alpha^{p_1^{s_1}} \cdot \beta^{l_1}) = ord(\alpha^{p_1^{s_1}}) \cdot ord(\beta^{l_1}) = k_1 \cdot p_1^{t_1}$.

В силу выбора α имеем

$$p_1^{t_1} k_1 \leq k = p_1^{s_1} k_1.$$

Следовательно, $p_1^{t_1} \leq p_1^{s_1}$. Аналогично, $p_i^{t_i} \leq p_i^{s_i}$ для любого $i = 2, \ldots, m$, отсюда следует, что $l|k$.

Из доказанного следует, что $\beta^k = 1$ для любого $\beta \in \mathbb{F}_q^*$, т. е. все элементы из $\mathbb{F}_q^*$ являются корнями многочлена $x^k - 1$. Следовательно, $q-1 \leq k$. С другой стороны, $k|q-1$ по теореме Лагранжа. Таким образом, $k = q-1$ и, следовательно, группа $\mathbb{F}_q^*$ порождается элементом α, т. е. $\mathbb{F}_q^* = \langle \alpha \rangle$. □

Образующий элемент циклической группы F_q^* называется *примитивным элементом* поля $\mathbb{F}_q$. Очевидно, поле $\mathbb{F}_q$ содержит $\varphi(q-1)$ примитивных элементов, где φ – функция Эйлера.

Теорема 5.4. *Пусть $\mathbb{F}_q \subseteq \mathbb{F}_r$. Тогда $\mathbb{F}_r$ является простым алгебраическим расширением поля $\mathbb{F}_q$, причем образующим элементом может служить любой примитивный элемент поля $\mathbb{F}_r$.*

Доказательство. Пусть θ – примитивный элемент поля $\mathbb{F}_r$. Тогда $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_r$. Так как в $\mathbb{F}_q(\theta)$ лежат все степени элемента θ , имеем $\mathbb{F}_r \subseteq \mathbb{F}_q(\theta)$. Следовательно, $\mathbb{F}_r = \mathbb{F}_q(\theta)$. □

Нормированный неприводимый многочлен $f \in \mathbb{F}[x]$ называется *примитивным* над полем $\mathbb{F}_q$, если f в качестве корня имеет примитивный элемент θ поля $\mathbb{F}_{q^m}$, где $m = \deg f$.Заметим, что такой f является минимальным многочленом для θ над полем $\mathbb{F}_q$.

Следствие. *Для любого конечного поля $\mathbb{F}_q$ и любого $m \in \mathbb{N}$ в кольце $\mathbb{F}_q[x]$ существует неприводимый многочлен степени m, более того, существует примитивный над полем $\mathbb{F}_q$ многочлен степени m.*

Доказательство. В силу леммы 5.3 $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$. По теореме 5.4 $\mathbb{F}_{q^m} = \mathbb{F}_q(\theta)$ для некоторого примитивного элемента θ поля $\mathbb{F}_{q^m}$. В силу теоремы 3.6 из § 3 минимальный многочлен M элемента θ неприводим и даже примитивен над $\mathbb{F}_q$, причем $\deg M = m$. □

6. Корни неприводимых многочленов

Лемма 6.1. *Пусть p – простое число, $n \in \mathbb{N}$ и $q = p^n$. Преобразование σ поля $\mathbb{F}_q$, заданное условием*

$$\sigma(\alpha) = \alpha^p \ (\alpha \in \mathbb{F}_q),$$

является автоморфизмом поля $\mathbb{F}_q$.

Доказательство. Ясно, что σ – эндоморфизм поля $\mathbb{F}_q$, поскольку

$$(\alpha \pm \beta)^p = \alpha^p \pm \beta^p \text{ и } (\alpha\beta)^p = \alpha^p\beta^p$$

для любых $\alpha, \beta \in \mathbb{F}_q$. Очевидно, σ инъективно, так как $\alpha^p = 0 \Leftrightarrow \alpha = 0$. В силу конечности $\mathbb{F}_q$ из инъективности следует сюръективность σ . □

Автоморфизм σ поля $\mathbb{F}_q$ называется *автоморфизмом Фробениуса*. Отметим, что σ оставляет на месте элементы подполя $\mathbb{F}_q$. Легко проверить, что $\sigma^k(\alpha) = \alpha^{p^k}$ для любого $\alpha \in \mathbb{F}_q, \quad k \in \mathbb{N}$.

Лемма 6.2. *Пусть f – неприводимый многочлен степени m над полем $\mathbb{F}_q$ и $k \in \mathbb{N}$. Если $f | x^{q^k} - x$ над $\mathbb{F}_q$, то $m|k$.*

Доказательство. Можно считать, что f – нормированный многочлен. Рассмотрим поля $\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$. Поскольку $f | x^{q^k} - x$ и многочлен $x^{q^k} - x$ вполне разложим над $\mathbb{F}_{q^k}$, многочлен f также вполне разложим над $\mathbb{F}_{q^k}$. Пусть α – корень многочлена f в поле $\mathbb{F}_{q^k}$. Тогда f является минимальным многочленом элемента α над полем $\mathbb{F}_{q^k}$. Следовательно, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ и поэтому $|\mathbb{F}_q(\alpha)| = q^m$. Поскольку $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^k}$, имеем $nm|nk$, где $q = p^n$, т.е. $m|k$. □

Теорема 6.1. *Пусть f – неприводимый многочлен степени m над полем $\mathbb{F}_q$. Тогда*

1) поле $\mathbb{F}_{q^m}$ является полем разложения многочлена f над $\mathbb{F}_q$;

2) все корни многочлена f , лежащие в $\mathbb{F}_{q^m}$, просты и исчерпываются следующими m различными элементами

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

где θ – произвольный корень многочлена f из поля $\mathbb{F}_{q^m}$.

Доказательство. Очевидно, теорему достаточно доказать для случая, когда f нормирован. Пусть K – поле разложения нормированного неприводимого многочлена f степени m над полем

$\mathbb{F}_q$ и θ – произвольный корень многочлена f из K. Тогда f является минимальным многочленом для θ над полем $\mathbb{F}_q$ и $|\mathbb{F}_q(\theta)| = q^m$. Поэтому будем считать, что $\mathbb{F}_q(\theta) = \mathbb{F}_{q^m} \subseteq K$.

Покажем, что если α – некоторый корень многочлена f из $\mathbb{F}_{q^m}$, то α^q – также корень многочлена f из $\mathbb{F}_{q^m}$. Действительно, если $f = a_0x^m + \ldots + a_{m-1}x + a_m$, то $f(\alpha^q) = a_0(\alpha^q)^m + \ldots + a_{m-1}(\alpha^q) + a_m = a_0^q(\alpha^m)^q + \ldots + a_{m-1}^q(\alpha)^q + a_m^q = (a_0\alpha^m + \ldots + a_{m-1}\alpha + a_m)^q = f(\alpha)^q = 0^q = 0$. В силу доказанного элементы

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

являются корнями многочлена f , лежащими в поле $\mathbb{F}_{q^m}$. Покажем, что все они различны. Пусть $\theta^{q^i} = \theta^{q^j}$ для некоторых $0 \leq i < j \leq m-1$. Возводя это равенство в степень q^{m-j} , получим

$$\theta^{q^{m-j+i}} = \theta^{q^m} = \theta.$$

Поскольку f является минимальным многочленом для θ над $\mathbb{F}_q$, многочлен f делит многочлен $x^{q^{m-j+i}} - x$ над полем $\mathbb{F}_q$. В силу леммы 6.2 имеем $m | m-j+i$, но $0 < m-j+i < m$ – противоречие.

Итак, все корни $\theta, \theta^q, \ldots, \theta^{q^{m-1}}$ многочлена f попарно различны и лежат в $\mathbb{F}_{q^m}$, следовательно, $K = \mathbb{F}_{q^m}$ – поле разложения многочлена f над $\mathbb{F}_q$. □

Следствие. *Поля разложения любых двух неприводимых многочленов одной и той же степени над полем $\mathbb{F}_q$ изоморфны.*

Следствие. *Поле $\mathbb{F}_{p^\infty}$ является алгебраическим замыканием поля $\mathbb{F}_p$.*

Доказательство. Каждый элемент поля $\mathbb{F}_{p^\infty} = \bigcup\limits_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$ алгебраичен над $\mathbb{F}_p$, так как для любого $n \in \mathbb{N}$ поля $\mathbb{F}_{p^{n!}}$ является конечным расширением поля $\mathbb{F}_p$.

Покажем, что любой многочлен положительной степени из $\mathbb{F}_{p^\infty}[x]$ вполне разложим над $\mathbb{F}_{p^\infty}$. Иными словами, над $\mathbb{F}_{p^\infty}$

неприводимы только многочлены первой степени.. Действительно, пусть f - неприводимый многочлен над $\mathbb{F}_{p^\infty}$. Тогда $f \in \mathbb{F}_{p^{n!}}[x]$ для некоторого $n \in \mathbb{N}$. В силу теоремы 6.1 многочлен f имеет корень в поле $\mathbb{F}_{(p^{n!})^m} \subseteq \mathbb{F}_{p^\infty}$, где $m = \deg f$. Следовательно, f имеет корень в $\mathbb{F}_{p^\infty}$, т.е. $\deg f = 1$. □

Пусть $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ и $\alpha \in \mathbb{F}_{q^m}$. Тогда элементы

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

называются *сопряженными с элементом* α относительно поля $\mathbb{F}_q$. Пусть M – минимальный многочлен элемента α над полем $\mathbb{F}_q$ и $d = \deg M$. Тогда $m = [\mathbb{F}_{q^m} : \mathbb{F}_q], |\mathbb{F}_q(\alpha)| = q^d$ и $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^m} \Rightarrow d|m$.

Если $d = m$, то в силу теоремы 6.1 все элементы, сопряженные с α относительно поля $\mathbb{F}_q$, попарно различны.

Если $d < m$, то в силу теоремы 6.1 попарно различны элементы

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}},$$

причем каждый из этих элементов повторяется в ряду сопряженных m/d раз. Это следует из того, что в силу равенства $\alpha^{q^m} = \alpha$ совокупность элементов

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$$

инвариантна относительно возведения ее членов в степень q (они переставляются циклически).

Пусть $q = p^n$, где p – простое число. Тогда $\sigma^n(\alpha) = \alpha^{p^n} = \alpha^q$ для любого $\alpha \in \mathbb{F}_{q^m}$, где σ – автоморфизм Фробениуса поля $\mathbb{F}_{q^m}$. Следовательно, автоморфизм σ^n циклически переставляет сопряженные элементы. Из этого вытекает, что сопряженные элементы имеют одинаковый порядок в группе $\mathbb{F}_{q^m}^*$.

Следствие. *Пусть f – примитивный многочлен степени m над полем $\mathbb{F}_q$. Тогда все его корни из $\mathbb{F}_{q^m}$ являются примитивными элементами в $\mathbb{F}_{q^m}$.*

Доказательство. Вытекает из замечания, сделанного перед следствием, и того факта, что примитивные элементы в $\mathbb{F}_{q^m}$ – это в точности элементы порядка $q^m - 1$. □

7. Группа автоморфизмов конечного поля

Автоморфизмом поля $\mathbb{F}_{q^m}$ над его подполем $\mathbb{F}_q$ называется автоморфизм поля $\mathbb{F}_{q^m}$, оставляющий на месте элементы из $\mathbb{F}_q$.

Рассмотрим преобразования $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ поля $\mathbb{F}_{q^m}$, определенные условием

$$\sigma_j(\alpha) = \alpha^{q^j},\ (j = 0, \ldots, m-1)$$

для любого $\alpha \in \mathbb{F}_{q^m}$.

Теорема 7.1. *1) Преобразования $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ и только они являются автоморфизмами поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$.*

2) Группа автоморфизмов поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$ является циклической группой порядка m и σ_1 – ее образующий элемент.

Доказательство. Пусть $q = p^n$, где $p = char\mathbb{F}_q$. Ясно, что $\sigma_j(\alpha) = \alpha^{q^j} = \alpha^{p^{nj}} = \sigma^{nj}(\alpha)$ для любого $\alpha \in \mathbb{F}_{q^m}$ и любого $j = 0, \ldots, m-1$. Следовательно, $\sigma_j = \sigma^{nj}$ – автоморфизм поля $\mathbb{F}_{q^m}$. где σ – автоморфизм Фробениуса поля $\mathbb{F}_{q^m}$. Кроме того, $\sigma_j(a) = a(a \in \mathbb{F}_q)$, так как $a^q = a$. Таким образом, $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ – автоморфизмы поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$.

Возьмем теперь в $\mathbb{F}_{q^m}$ некоторый примитивный элемент α. Для α все сопряженные с ним относительно поля $\mathbb{F}_q$ элементы попарно различны, поэтому попарно различны автоморфизмы $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$.

Предположим, что τ – произвольный автоморфизм поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$. В качестве θ возьмем некоторый примитивный элемент поля $\mathbb{F}_{q^m}$. Пусть M – его минимальный многочлен над полем $\mathbb{F}_q$. Тогда $M(\tau(\theta)) = \tau(M(\theta)) = \tau(0) = 0$, т. е. $\tau(\theta)$ является корнем многочлена M. Поскольку все корни многочлена M сопряжены, $\tau(\theta) = \theta^{q^j}$ для некоторого $j = 0, \ldots, m-1$. Пусть α –

произвольный элемент из $\mathbb{F}_{q^m}^*$. Так как θ – примитивный элемент поля F_{q^m}, существует $k \in \mathbb{N}$ такой, что $\alpha = \theta^k \Rightarrow \tau(\alpha) = \tau(\theta^k) = \tau(\theta)^k = (\theta^{q^j})^k = (\theta^k)^{q^j} = \alpha^{q^j} = \sigma_j(\alpha)$, т. е. $\tau = \sigma_j$ (отметим, что, очевидно, $\tau(0) = 0 = \sigma_j(0)$).

Итак, все автоморфизмы поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$ исчерпываются автоморфизмами $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$.

Далее, для любого $j = 0, \ldots, m-1$ выполняется $\sigma_j(\alpha) = \alpha^{q^j} = \sigma_1^j(\alpha)$ $(\alpha \in \mathbb{F}_{q^m})$, т. е. $\sigma_j = \sigma_1^j$. Следовательно, группа автоморфизмов поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$ (*группа Галуа поля* $\mathbb{F}_{q^m}$ *над полем* $\mathbb{F}_q$) порождается автоморфизмом σ_1, т. е. является циклической группой порядка m. □

Следствие. *Группа автоморфизмов поля* $\mathbb{F}_{p^n}$*, где* p *– простое число и* $n \in \mathbb{N}$*, является циклической группой порядка* n*, порождаемой автоморфизмом Фробениуса поля* $\mathbb{F}_{p^n}$*.*

Доказательство. Это частный случай теоремы 7.1 для поля $\mathbb{F}_{p^n}$ над его простым подполем $\mathbb{F}_p$, так как любой автоморфизм поля $\mathbb{F}_{p^n}$ оставляет на месте все элементы простого подполя. □

8. Формула обращения Мебиуса

Определим функцию Мебиуса μ на $\mathbb{N}$, полагая

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1; \\ (-1)^k, & \text{если } n \text{ является произведением } k \text{ различных} \\ & \text{простых чисел;} \\ 0, & \text{если } n \text{ делится на квадрат некоторого простого} \\ & \text{числа.} \end{cases}$$

(Отметим, что при $n = 1$ можно считать $k = 0$ и $(-1)^0 = 1$, т.е. первый случай такой же как второй.)

Лемма 8.1. *Для любого* $n \in \mathbb{N}$ *выполняется*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{если } n = 1; \\ 0, & \textit{если } n > 1. \end{cases}$$

Доказательство. Пусть $n > 1$. Достаточно рассмотреть лишь те натуральные делители d числа n, для которых $\mu(d) \neq 0$. Пусть $p_1, \ldots, p_m$ – множество всех попарно различных простых делителей числа n. Тогда

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{m} \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq m} \mu(p_{i_1} p_{i_2}) + \ldots =$$

$$= 1 + c_m^1(-1) + c_m^2(-1)^2 + \ldots + c_m^m(-1)^m = (1 + (-1))^m = 0.$$

□

Теорема 8.1. *1) (Аддитивный вариант.) Пусть h и H – две функции из $\mathbb{N}$ в некоторую аддитивную абелеву группу G. Условие*

$$H(n) = \sum_{d|n} h(d), \ (n \in \mathbb{N})$$

выполняется тогда и только тогда, когда выполняется условие

$$h(n) = \sum_{d|n} \mu(n/d) H(d) = \sum_{d|n} \mu(d) H(n/d) \quad (n \in \mathbb{N}).$$

(В последних равенствах фигурируют не произведения, а берутся кратные элементов в группе G!)

2) (Мультипликативный вариант.) Пусть h и H – две функции из $\mathbb{N}$ в некоторую мультипликативную абелеву группу G. Условие

$$H(n) = \prod_{d|n} h(d) \quad (n \in \mathbb{N}).$$

выполняется iff, когда выполняется условие

$$h(n) = \prod_{d|n} H(d)^{\mu(n/d)} = \prod_{d|n} H(n/d)^{\mu(d)} \quad (n \in \mathbb{N}).$$

Доказательство. 1) $\Rightarrow$. Для любого $n \in \mathbb{N}$, используя правила действия с кратными в аддитивной группе G, получаем

$$\sum_{d|n} \mu(n/d) H(d) = \sum_{d|n} \mu(d) H(n/d) =$$

$$= \sum_{d|n} \mu(d) \sum_{c|n/d} h(c) = \sum_{d|n} \sum_{c|n/d} \mu(d)h(c) =$$

$$= \sum_{cd|n} \mu(d)h(c) = \sum_{c|n} \sum_{d|n/c} \mu(d)h(c) =$$

$$= \sum_{c|n} \left(\sum_{d|n/c} \mu(d) \right) h(c) = h(n).$$

$\Leftarrow$. Обратное утверждение доказывается аналогично. Действительно, для любого $n \in \mathbb{N}$ имеем

$$\sum_{d|n} h(d) = \sum_{d|n} h(n/d) = \sum_{d|n} \sum_{c|n/d} \mu(n/cd)H(c) =$$

$$= \sum_{cd|n} \mu(n/cd)H(c) = \sum_{c|n} \sum_{d|n/c} \mu(n/cd)H(c) =$$

$$= \sum_{c|n} \left(\sum_{d|n/c} \mu(n/cd) \right) H(c) = \sum_{c|n} \left(\sum_{d|n/c} \mu(d) \right) H(c) = H(n).$$

2) представляет из себя тоже самое, что и 1), только переписанное из аддитивной формы в мультипликативную форму. $\square$

9. Корни из единицы и круговые многочлены

Поле разложения многочлена $x^n - 1$ над полем $\mathbb{F}_q$ называется n - *круговым полем* (а так же *циклотомическим полем* или *полем деления круга*)над полем $\mathbb{F}_q$ и обозначается через $\mathbb{F}_q^{(n)}$. Корни многочлена $x^n - 1$, лежащие в поле $\mathbb{F}_q^{(n)}$, называются *корнями* n-ой *степени из единицы над полем* $\mathbb{F}_q$. Множество этих корней будем обозначать через $E_q^{(n)}$.

Теорема 9.1. *Пусть $\mathbb{F}_q$ – конечное поле характеристики p, $n \in \mathbb{N}$ и $p \nmid n$. Тогда $E_q^{(n)}$ – циклическая подгруппа порядка n мультипликативной группы поля $\mathbb{F}_q^{(n)}$.*

Доказательство. Случай $n = 1$ тривиален. Пусть $n \geq 2$. Многочлен $f = x^n - 1$ и его производный многочлен $f' = nx^{n-1}$ ($\neq 0$) взаимопросты $HOD(f, f') = 1$,так как $xf' - nf = n \neq 0$. Следовательно, многочлен $x^n - 1$ не имеет кратных корней в $\mathbb{F}_q^{(n)} \Rightarrow |E_q^{(n)}| = n$. Тривиально проверяется, что $E_q^{(n)}, \cdot$ – группа, т. е. $E_q^{(n)}$ – подгруппа циклической группы $(\mathbb{F}_q^{(n)})^* \Rightarrow E_q^{(n)}$ – циклическая группа. □

Пусть $\mathbb{F}_q$ – конечное поле характеристики p, $n \in \mathbb{N}$ и $p \nmid n$. Любой образующий элемент циклической группы $E_q^{(n)}$ называется *первообразным корнем n-ой степени из единицы над полем* $\mathbb{F}_q$. Ясно, что существует точно $\varphi(n)$ различных первообразных корней n-ой степени из единицы над полем $\mathbb{F}_q$, где φ – функция Эйлера. Многочлен

$$Q_n(x) \rightleftharpoons \prod_{\substack{\varepsilon \in E_q^{(n)} \\ 0(\varepsilon) = n}} (x - \varepsilon)$$

называется n - *круговым* (или n -*циклотомическим*) *многочленом над полем* $\mathbb{F}_q$. Его корни – это все первообразные корни n-ой степени из единицы над полем $\mathbb{F}_q$ из $E_q^{(n)}$, $\deg Q_n = \varphi(n)$, а его коэффициенты принадлежат, вообще говоря, n-круговому полю $\mathbb{F}_q^{(n)}$ над $\mathbb{F}_q$. Отметим, что Q_n является нормированным многочленом.

Теорема 9.2. *Пусть $\mathbb{F}_q$ – конечное поле характеристики p, $n \in \mathbb{N}$ и $p \nmid n$. Тогда*

1) $x^n - 1 = \prod\limits_{d|n} Q_d(x)$;

2) коэффициенты n -кругового многочлена $Q_n(x)$ принадлежат простому подполю $\mathbb{F}_p$ поля $\mathbb{F}_q$.

Доказательство. 1) Если $d|n$, то $p \nmid d$ и $x^d - 1|x^n - 1$. Тогда $\mathbb{F}_q^{(d)} \subseteq \mathbb{F}_q^{(n)}$ и $E_q^{(d)} \subseteq E_q^{(n)}$. Каждый корень n -ой степени из единицы над полем $\mathbb{F}_q$ является первообразным конем d-ой степени

из единицы над полем $\mathbb{F}_q$ точно для одного делителя d числа n. Следовательно,

$$x^n - 1 = \prod_{\varepsilon \in E_q^{(n)}} (x - \varepsilon) = \prod_{d|n} \prod_{\substack{\varepsilon \in E_q^{(n)} \\ 0(\varepsilon) = d}} (x - \varepsilon) = \prod_{d|n} Q_d(x).$$

2) Индукция по n. Для $n = 1$ имеем $Q_1(x) = x - 1 \in \mathbb{F}_p[x]$. Пусть $n > 1$ и утверждение справедливо для любого Q_d, где $d|n$ и $1 \leq d < n$. Тогда в силу 1) имеем $Q_n = \dfrac{x^n - 1}{f}$, где

$$f = \prod_{\substack{1 \leq d < n \\ d|n}} Q_d.$$

По предположению индукции $f \in \mathbb{F}_p[x]$. Частное многочленов $x^n - 1$ и f также лежит в $\mathbb{F}_p[x]$, т. е. $Q_n \in \mathbb{F}_p[x]$. □

Интересно отметить, что у первых 104 многочленов все коэффициенты лежат в множестве $\{-1, 0, 1\}$. Однако у Q_{105} имеется два коэффициента, равных -2.

Теорема 9.3. *Пусть $\mathbb{F}_q$ - конечное поле характеристики p, $n \in \mathbb{N}$ и $p \nmid n$. Тогда n -круговой многочлен Q_n над $\mathbb{F}_q$ задается формулой*

$$Q_n = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}.$$

Доказательство. Применим мультипликативный вариант формулы обращения Мебиуса к мультипликативной группе $G = (\mathbb{F}_q(x))^*$ поля рациональных дробей над $\mathbb{F}_q$. Положим $h(n) = Q_n$ и $H(n) = x^n - 1$ для любого $n \in \mathbb{N}$. Используя равенство 1) из теоремы 9.2, получаем нужную формулу. □

Пример. Рассмотрим конечное поле $\mathbb{F}_q$ характеристики $p \neq 2, 3$ и 12-круговой многочлен Q_{12} над ним. Тогда

$$Q_{12} = \prod_{d|12} (x^{12/d} - 1)^{\mu(d)} = (x^{12} - 1^{\mu(1)}(x^6 - 1)^{\mu(2)}(x^4 - 1)^{\mu(3)}.$$
$$\cdot (x^3 - 1)^{\mu(4)}(x^2 - 1)^{\mu(6)}(x - 1)^{\mu(12)} =$$
$$= (x^{12} - 1)(x^6 - 1)^{-1}(x^4 - 1)^{-1}(x^2 - 1) =$$
$$= \frac{(x^{12} - 1)}{(x^6 - 1)} \cdot \frac{(x^2 - 1)}{(x^4 - 1)} = \frac{(x^6 + 1)}{(x^2 + 1)} = x^4 - x^2 + 1.$$

Теорема 9.4. *Пусть $\mathbb{F}_q$ – конечное поле характеристики p, $k \in \mathbb{N}$, r – простое число, отличное от p. Тогда над полем $\mathbb{F}_q$ выполняется $Q_{r^k} = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \ldots + x^{(r-1)r^{k-1}}$ и, в частности, $Q_r = 1 + x + x^2 + \ldots + x^{r-1}$.*

Доказательство. В силу теоремы 9.2 имеем

$$Q_{r^k} = \frac{x^{r^k} - 1}{Q_1 Q_r \ldots Q_{r^{k-1}}} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1} =$$

$$1 + x^{r^{k-1}} + x^{2r^{k-1}} + \ldots + x^{(r-1)r^{k-1}}.$$

□

Пусть $q, n \in \mathbb{N}$. *Мультипликативным порядком $ord_n(q)$ числа q по модулю n* будем называть наименьшее натуральное число d (если оно существует) такое, что $q^d \equiv 1 (\mathrm{mod}\ n)$.

Теорема 9.5. *Пусть $\mathbb{F}_q$ – конечное поле характеристики p, $n \in \mathbb{N}$ и $p \nmid n$. Тогда*

1) n – круговое поле $\mathbb{F}_q^{(n)}$ является простым алгебраическим расширением поля $\mathbb{F}_q$, порождаемым любым первообразным корнем степени n из единицы над полем $\mathbb{F}_q$;

2) степень d поля $\mathbb{F}_q^{(n)}$ над полем $\mathbb{F}_q$ равна мультипликативному порядку числа q по модулю n;

n – круговой многочлен Q_n разлагается над $\mathbb{F}_q$ в произведение $\varphi(n)/d$ различных нормированных неприводимых многочленов над $\mathbb{F}_q$ одной и той же степени d и $\mathbb{F}_q^{(n)}$ является полем разложения каждого из этих многочленов.

Доказательство. 1) Очевидно, $\mathbb{F}_q^{(n)} = \mathbb{F}_q^{(\varepsilon)}$, где ε – произвольный первообразный корень степени n из единицы над $\mathbb{F}_q$, лежащий в $\mathbb{F}_q^{(n)}$.

2) Пусть ε – произвольный первообразный корень степени n из единицы над $\mathbb{F}_q$, лежащий в $\mathbb{F}_q^{(n)} \subseteq \mathbb{F}_{p^\infty}$. Будем считать, что $\mathbb{F}_q^{(n)} \subseteq \mathbb{F}_{p^\infty}$ для любого $k \in \mathbb{N}$. Заметим, что $\mathbb{F}_q^{(n)} = \mathbb{F}_q^k$ для некоторого $k \in \mathbb{N}$.

Далее, для любого $k \in \mathbb{N}$ имеем $\varepsilon \in \mathbb{F}_{q^k} \Leftrightarrow \varepsilon^{q^k} = \varepsilon \Leftrightarrow \varepsilon^{q^k-1} = 1 \Leftrightarrow n|q^k - 1 \Leftrightarrow q^k \equiv 1(\mathrm{mod}\ n)$. Наименьшее натуральное число k, для которого выполняется это сравнение, обозначим через d. Конечно, $d = ord_n(q)$. Из определения d следует, что $\varepsilon \in \mathbb{F}_{q^d}$, но ε не лежит ни в каком собственном подполе поля $\mathbb{F}_{q^d}$ вида $\mathbb{F}_{q^k}$, где $1 \leq k < d$, т. е. $\mathbb{F}_{q^d} = \mathbb{F}_q(\varepsilon) = \mathbb{F}_q^{(n)}$ и степень минимального многочлена $M_\varepsilon(x)$ элемента ε над полем $\mathbb{F}_q$ равна d. Ясно, что $M_\varepsilon(x)|Q_n$ над $\mathbb{F}_q$. Так как ε – произвольный корень многочлена Q_n, отсюда следует заключение теоремы. □

Пример. Рассмотрим поле $\mathbb{F}_{11}$ и многочлен $Q_{12} = x^4 - x^2 + 1$ над ним, т. е. здесь $q = 11,\ n = 12$. Поскольку $11^1 \neq 1 \pmod{12}$ и $11^2 = 121 \equiv 1 \pmod{12}$, имеем $d = ord_{12}11 = 2$. Кроме того, $\varphi(12) = \deg Q_{12} = 4$. Следовательно, Q_{12} разлагается над $\mathbb{F}_{11}$ в произведение $\dfrac{\varphi(12)}{2} = 2$ нормированных неприводимых многочленов степени 2. Найдем это разложение над $\mathbb{F}_{11}$.

$$Q_{12} = x^4 - x^2 + 1 = x^4 + 2x^2 + 1 - 3x^2 = x^4 + 2x^2 + 1 - 25x^2 =$$
$$= (x^2 + 1) - (5x)^2 = (x^2 + 1 + 5x)(x^2 + 1 - 5x) =$$
$$= (x^2 + 5x + 1)(x^2 - 5x + 1).$$

Отсюда в силу теоремы 9.5 следует, что многочлены $x^2 + 5x + 1$ и $x^2 - 5x + 1$ неприводимы над $\mathbb{F}_{11}$. Кроме того, $[\mathbb{F}_{11}^{(12)} : \mathbb{F}_{11}] = d = 2$ влечет $\mathbb{F}_{11}^{(12)} = \mathbb{F}_{121}$.

Теорема 9.6. *Конечное поле $\mathbb{F}_q$ является $(q-1)$ -круговым полем над любым из своих подполей.*

Доказательство. Пусть p – характеристика поля $\mathbb{F}_q$. Ясно, что $p \nmid (q-1)$ и многочлен $x^{q-1}-1$ вполне разложим над $\mathbb{F}_q$, так как его корнями являются все ненулевые элементы поля $\mathbb{F}_q$. С другой стороны, этот многочлен нельзя разложить на линейные множители ни в каком собственном подполе поля $\mathbb{F}_q$, так как в таком подполе будет меньше чем $(q-1)$ ненулевых элементов. □

10. О представлении элементов в конечных полях

Рассмотрим три способа представления элементов конечного поля $\mathbb{F}_q$ характеристики p, где $q = p^n$ и $n \in \mathbb{N}$.

Первый способ. Возьмем произвольный неприводимый многочлен f степени n над $\mathbb{F}_p$. По теореме 6.1 из § 6 поле $\mathbb{F}_{p^n}$ является полем разложения многочлена f над $\mathbb{F}_p$. Пусть α – произвольный корень многочлена f из $\mathbb{F}_{p^n}$. Тогда $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. В силу теоремы 3.6 из § 3 $1, \alpha, \ldots, \alpha^{n-1}$ – базис поля $\mathbb{F}_{p^n}$ над полем $\mathbb{F}_p$, т. е. каждый элемент из $\mathbb{F}_p$ единственным образом представим в виде:

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1},$$

где $a_0, \ldots, a_{n-1} \in \mathbb{F}_p$.

Пример 1. Рассмотрим поле $\mathbb{F}_9$. Очевидно $[\mathbb{F}_9 : \mathbb{F}_3] = 2$. Многочлен x^2+1 неприводим над $\mathbb{F}_3$, так как он не имеет корней в поле $\mathbb{F}_3$. Поле $\mathbb{F}_9$ является полем разложения многочлена f над $\mathbb{F}_3$. Пусть α – некоторый корень многочлена f из $\mathbb{F}_9$, т. е. $\alpha^2 = -1$. Тогда любой элемент из $\mathbb{F}_9$ однозначно представим в виде $a_0 + a_1\alpha$, где $a_0, a_1 \in \mathbb{F}_3$, т. е.

$$F_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}.$$

Таблицы Кэли операций $+$ и $\cdot$ легко составить, используя равенство $\alpha^2 = -1$ и тождество $3x = 0$. Например, $(2+\alpha)(1+2\alpha) = 2 + 4\alpha + \alpha + 2\alpha^2 = 2\alpha$.

Второй способ. Усовершенствуем первый способ, используя теоремы 9.5 и 9.6 из § 9. Поле $\mathbb{F}_q$ является $(q-1)$ – круговым полем над $\mathbb{F}_p$, т. е. $F_{\text{ш}} = \mathbb{F}_p^{(q-1)}$. Рассмотрим круговой многочлен Q_{q-1}. Пусть f – неприводимый множитель многочлена Q_q над $\mathbb{F}_p$. Имеем $\deg f = ord_{q-1}(p) = d$. Возьмем корень ε многочлена f. Это первообразный корень степени $q-1$ из единицы в поле $\mathbb{F}_q^{(q)}$. Очевидно ε является примитивным элементом поля $\mathbb{F}_q$. Следовательно, $\mathbb{F}_q = \{0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{q-1} = 1\}$. С другой стороны, $1, \varepsilon, \ldots, \varepsilon^{d-1}$ – базис поля $\mathbb{F}_q$ над $\mathbb{F}_p$, т. е. мы имеем два представления элементов поля $\mathbb{F}_q$.

Пример 2. Опять рассмотрим поле $\mathbb{F}_9$. Мы имеем $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$, т. е. поле $\mathbb{F}_9$ является 8 -круговым полем над $\mathbb{F}_3$. В силу теоремы 9.4 из § 9 имеем $Q_8 = Q_{2^3} = 1 + x^{2^2} = 1 + x^4 \in \mathbb{F}_3[x]$. Мультипликативный порядок числа 3 по mod 8 равен $2 = [\mathbb{F}_3^{(8)} : \mathbb{F}_3]$ (конечно, $3^2 \equiv 1 \pmod 8$), и $4 = \deg Q_8 = \varphi(8)$. Следовательно, Q_8 разлагается над полем $\mathbb{F}_3$ в произведение двух неприводимых множителей степени 2. Так как

$$x^4 + 1 = x^4 - 2x^2 + 1 + 2x^2 = (x^2 - 1)^2 - x^2 =$$
$$= (x^2 - 1 - x)(x^2 - 1 + x) = (x^2 + 2x + 2)(x^2 + x + 2),$$

многочлены $x^2 + 2x + 2$ и $x^2 + x + 2$ — неприводимы над $\mathbb{F}_3$ и даже примитивны над $\mathbb{F}_3$.

Возьмем $f = x^2 + x + 2$, и пусть ε – корень многочлена $x^2 + x + 2$. Тогда

$$F_9 = \{0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^7, \varepsilon^8 = 1\}$$

и

$$F_9 = \{0, 1, 2, \varepsilon, 1 + \varepsilon, 2 + \varepsilon, 2\varepsilon, 1 + 2\varepsilon, 2 + 2\varepsilon\}.$$

Составим *таблицу индексов* или *дискретных логарифмов по основанию* ε.

i	ε^i	i	ε^i
1	ε	5	2ε
2	$1 + 2\varepsilon$	6	$2 + \varepsilon$
3	$2 + 2\varepsilon$	7	$1 + \varepsilon$
4	2	8	1

$$\varepsilon^2+\varepsilon+2=0\Rightarrow\varepsilon^2=2\varepsilon+1\Rightarrow$$
$$\varepsilon^3=2\varepsilon^2+\varepsilon=4\varepsilon+2+\varepsilon=2\varepsilon+2\Rightarrow$$
$$\varepsilon^4=2\varepsilon^2+2\varepsilon=4\varepsilon+2+2\varepsilon=2\Rightarrow$$
$$\varepsilon^5=2\varepsilon\Rightarrow\varepsilon^6=2\varepsilon^2=4\varepsilon+2=\varepsilon+2\Rightarrow$$
$$\varepsilon^7=\varepsilon^2+2\varepsilon=2\varepsilon+1+2\varepsilon=\varepsilon+1,\varepsilon^8=1.$$

Мы установили связь между двумя представлениями элементов. Складывать элементы складывать удобно во втором виде, а умножать – используя таблицу индексов. Например, $(2+2\varepsilon)(1+\varepsilon)=\varepsilon^3\varepsilon^7=\varepsilon^2=1+2\varepsilon$.

Установим связь этого представления с представлением из примера 1 . Заметим, что $\varepsilon-1$ является корнем многочлена x^2+1:

$$(\varepsilon-1)^2+1=\varepsilon^2-2\varepsilon+1+1=\varepsilon^2-2\varepsilon+2=\varepsilon^2+\varepsilon+2=0.$$

Положим $\alpha=\varepsilon-1$. Тогда $\alpha^2+1=0$ и $\varepsilon=1+\alpha$. Мы находимся в ситуации примера 1. Построим еще одну таблицу индексов. Ее легко получить, если в первую таблицу вместо ε подставить $1+\alpha$. Вторую таблицу можно построить, не используя первой, а используя соотношения $\alpha^2=-1$ и тождество $3x=0$.

i	1	2	3	4	5	6	7	8
ε^i	$1+\alpha$	2α	$1+2\alpha$	2	$2+2\alpha$	α	$2+\alpha$	1

Действительно, $\varepsilon=1+\alpha\Rightarrow$

$\Rightarrow\varepsilon^2=1+2\alpha+\alpha^2-2\alpha\Rightarrow\varepsilon^3=2\alpha(1+\alpha)=$
$2\alpha+2\alpha^2=1+2\alpha\Rightarrow\varepsilon^4=(1+2\alpha)(1+\alpha)=1+2\alpha+\alpha+2\alpha^2=$
$=-1=2\Rightarrow\varepsilon^5=2(1+\alpha)=2+2\alpha\Rightarrow\varepsilon^6=$
$=(2+2\alpha)(1+\alpha)=2+2\alpha+2\alpha+2\alpha^2=\alpha\Rightarrow\varepsilon^7=\alpha(1+\alpha)=$
$=\alpha+\alpha^2=2+\alpha$ и $\varepsilon^8=1$.

Теперь элементы поля $\mathbb{F}_9$ удобно складывать в виде $a+b\alpha$, а умножать в том же виде, используя таблицу индексов. Например, $(1+2\alpha)(2+\alpha)=\varepsilon^3\varepsilon^7=\varepsilon^2=2\alpha$.

Теперь видна важность знания алгоритмов разложения круговых многочленов на неприводимые множители над данным полем. Видна также особая роль примитивных многочленов над данным полем.

Пусть ε – примитивный элемент поля $\mathbb{F}_q$. Для элемента $a \in \mathbb{F}_q^*$ единственное натуральное число $i \in \{1, \ldots, q-1\}$ такое, что $a = \varepsilon^i$, называется *индексом* или *дискретным логарифмом по основанию* ε. При этом пишут $i = ind_\varepsilon(a)$. Пусть $i = ind_\varepsilon(a)$ и $j = ind_\varepsilon(b)$, где $a, b \in \mathbb{F}_q^*$. Тогда $a = \varepsilon^i$ и $b = \varepsilon^j$, отсюда следует $ab = \varepsilon^{i+j}$ и $ab^{-1} = \varepsilon^{i-j}$. Следовательно,

$$ind_\varepsilon(ab) \equiv ind_\varepsilon(a) + ind_\varepsilon(b) \pmod{(q-1)},$$

$$ind_\varepsilon(ab^{-1}) \equiv ind_\varepsilon(a) - ind_\varepsilon(b) \pmod{(q-1)}$$

в силу того, что порядок элемента ε равен $q-1$. Функция, обратная к дискретному логарифму, называется *дискретным антилогарифмом*. Она переводит i в ε^i для любого $i = 1, \ldots, q-1$.

Третий способ. Обсудим представление элементов поля $\mathbb{F}_q$ с помощью матриц над полем $\mathbb{F}_p q$. Возьмем нормированный неприводимый многочлен степени $n \geq 1$ над полем $\mathbb{F}_p$:

$$f = a_o + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n.$$

Рассмотрим его сопровождающую матрицу

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & 0 & -a_2 \\ & & & & \\ 0 & 0 & 0 & 1 & -a_{n-1} \end{pmatrix} \in M_{n \times n}(\mathbb{F}_p)$$

Тогда многочлен f является характеристическим многочленом для матрицы A. По теореме Гамильтона-Кели A аннулирует многочлен f , т. е.

$$f(A) = a_0 E_n + a_1 A + \ldots + a_{n-1} A^{n-1} + A^n = 0,$$

где E_n – единичная, а 0 – нулевая квадратная матрица порядка n над $\mathbb{F}_p$. Отметим, что f делит любой другой многочлен над $\mathbb{F}_p$, который аннулируется матрицей A (так как f – минимальный многочлен для A).

Теорема 10.1. *Поле $\mathbb{F}_{p^n}$ изоморфно подполю кольца матриц из $M_{n\times n}(\mathbb{F}_p)$, составленному из всех матриц вида*

$$b_0E_n + b_1A + \ldots + b_{n-1}A^{n-1},$$

где $b_0, b_1, \ldots, b_{n-1}$ пробегают поле $\mathbb{F}_p$.

Доказательство. Рассмотрим отображение ψ из $\mathbb{F}_p[x]$ в $M_{n\times n}(\mathbb{F}_p)$ такое, что $\psi(g) = g(A)$ для любого $g \in \mathbb{F}_p[x]$. Это отображение является кольцевым гомоморфизмом, так как для любых $g_1, g_2 \in \mathbb{F}_p[x]$ выполняется $(g_1g_2)(A) = g_1(A)g_2(A)$ и $(g_1 + g_2)(A) = g_1(A) + g_2(A)$. Очевидно, $Ker\psi$ состоит из всех многочленов над $\mathbb{F}_p$, аннулируемых матрицей A, т.е. $Ker\psi = (f)$. Тогда получаем

$$\mathbb{F}_p[x]/(f) \cong \mathrm{Im}\psi \subseteq M_{n\times n}(\mathbb{F}_p).$$

Поскольку многочлен f неприводим над $\mathbb{F}_p$, отсюда следует, что $\mathrm{Im}\psi$ является полем, изоморфным полю $\mathbb{F}_{p^n}$, причем в этом поле матрица A является корнем многочлена f и A порождает $\mathrm{Im}\psi$ как расширение поля $\mathbb{F}_p$. Таким образом, $E, A, \ldots, A^{n-1}$ – базис поля $\mathrm{Im}\psi(\cong F_{p^n})$ над полем $\mathbb{F}_p$. □

Пример 3. Как и в примере 1, рассмотрим многочлен $f = x^2 + 1 \in \mathbb{F}_3[x]$. Сопровождающая матрица для f имеет вид

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

Элементы поля $\mathbb{F}_9$ можно единственным образом представить в виде $a_0E + a_1A$, т.е. $\mathbb{F}_9 = \{0, E, 2E, A, E + A, 2E + A, 2A, E + 2A, 2E + 2A\}$. Легко показать, что $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $2E = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, $E + A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$, $2E + A = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$, $2A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$, $E + 2A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$, $2E + 2A =$

$\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$. В поле $\mathbb{F}_9$, заданном таким способом, действия производятся по обычным правилам алгебры матриц над $\mathbb{F}_3$. Например, $(2E + A)(E + 2A) = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = 2A$.

Пример 4. Как в примере 2, возьмем $f = x^2 + x + 2 \in \mathbb{F}_3[x]$. Здесь f является неприводимым множителем кругового многочлена Q_8 над $\mathbb{F}_3$. Сопровождающая матрица для f имеет вид

$$B = \begin{pmatrix} 0 & -2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

Элементы поля $\mathbb{F}_9$ можно единственным образом представить в виде $b_0E + b_1B$, где $b_0, b_1 \in \mathbb{F}_3$.

Так как $f|Q_8$ над $\mathbb{F}_3$, корни многочлена f, лежащие в поле $\mathbb{F}_3^{(8)} = \mathbb{F}_9$, являются первообразными корнями 8-й степени из единицы. Поэтому матрица B, являясь корнем многочлена f в поле $\mathbb{F}_9$, будет элементом 8-го порядка в группе $\mathbb{F}_9^*$. Следовательно,

$$\mathbb{F}_9 = \{0, B, B^2, B^3, B^4, B^5, B^6, B^7, B^8 = E\}.$$

нетрудно показать, что

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \; B = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \; B^2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$B^3 = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \; B^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \; B^5 = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$$

$$B^6 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \; B^7 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \; B^8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Вычисления в таком поле $\mathbb{F}_9$ производятся по обычным правилам алгебры матриц над $\mathbb{F}_3$, причем умножения производить очень просто, так как мы, по существу, имеем таблицу индексов по основанию B.

11. Алгоритм Берлекэмпа разложения многочленов на неприводимые множители

Пусть $\mathbb{F}_q$ – конечное поле характеристики p, $f \in \mathbb{F}_q[x]$ и $deg\ f = n \geq 1$. Наша цель – построить алгоритм разложения многочлена f на неприводимые множители над полем $\mathbb{F}_q$.

Лемма 11.1. *$f' = 0$, тогда и только тогда, когда $f = g^p$ для некоторого многочлена $g \in \mathbb{F}_q[x]$.*

Доказательство. Пусть $f' = 0$. Тогда, очевидно, $f = a_0 + +a_1x^p + \ldots + a_mx^{mp} = b_0^p + b_1^px^p + \ldots + b_m^px^{mp} = (b_0 + b_1x + \ldots + +b_mx^m)^p = g^p$. Элементы b_i такие, что $b_i^p = a_i$, существуют, поскольку возведение в степень p – это автоморфизм Фробениуса. Мы воспользуемся также тем, что возведение в степень p является эндоморфизмом поля $\mathbb{F}_q[x]$. (Отметим, что указанные рассуждения не проходят для случая произвольного поля характеристики p, так как в бесконечном поле отображение $a \to a^p$ может оказаться не автоморфизмом, а только несюръективным эндоморфизмом).

Обратно, пусть $f = g^p$. Тогда $f' = pg^{p-1}\ g' = 0$. □

Следствие. *Если многочлен f неприводим над полем $\mathbb{F}_q$, то $f' \neq 0$.*

Лемма 11.2. *Пусть $f' \neq 0$ и f_1 – неприводимый множитель кратности k многочлена f над полем $\mathbb{F}_q$. Тогда f_1 является множителем кратности k_1 многочлена f' над полем $\mathbb{F}_q$ такой, что*

1) $k_1 \geq k$, если $p \mid k$;

2) $k_1 = k - 1$, если $p \nmid k$.

Доказательство. Пусть $f' \neq 0$ и $f = f_1^k g$, где $g \in \mathbb{F}_q[x]$ и $f_1 \nmid g$. Тогда

$$f' = kf_1^{k-1}f_1'g + f_1^kg'.$$

1 случай – $p \mid k$. Тогда $f' = f_1^kg'$, где $g' \neq 0$, поскольку $f' \neq 0$. Следовательно, $k_1 \geq k$.

2 случай – $p \nmid k$. Тогда

$$f' = f_1^{k-1}(kf_1'g + f_1g'),$$

где $kf_1'g + f_1g' \neq 0$, поскольку $f' \neq 0$. Предположим, от противного, что $f_1 \mid kf_1'g + f_1g'$ над $\mathbb{F}_q$. Тогда $f_1 \mid kf_1'g$, где $kf_1'g \neq 0$ в силу следствия.

Поскольку $f_1 \nmid g$, в силу неприводимости f_1 выполняется соотношение $f_1|kf_1'$, где $f_1' \neq 0$ в силу следствия, что невозможно. □

Пусть теперь

$$f = f_1^{k_1}, \ldots, f_l^{k_l} f_{l+1}^{k_{l+1}}, \ldots, f_m^{k_m}$$

– каноническое разложение *нормированного* многочлена f на неприводимые множители над полем $\mathbb{F}_q$, где $p \mid k_1, \ldots, k_l$ и $p \nmid k_{l+1}, \ldots, k_m$. Если нет многочленов $f_i (i = 1, ..., m)$, делящихся на p, то полагаем $l = 0$.

Следствие. *Если $f' \neq 0$, то $l < m$,*

$$d \rightleftharpoons HOD(f, f') = f_1^{k_1}, \ldots, l_l^{k_l} f_{l+1}^{k_{l+1}-1}, \ldots, f_m^{k_m-1}$$

и многочлен $f/d = f_{l+1} \ldots f_m$ не имеет кратных неприводимых множителей над полем $\mathbb{F}_q$.

Доказательство. Если $l = m$, то $f = g^p$ и, следовательно, $f' = 0$, что невозможно. Далее, надо воспользоваться леммой 11.2. □

Следствие. *$d \rightleftharpoons HOD(f, f') = 1$ тогда и только тогда, когда f не имеет кратных неприводимых множителей над полем $\mathbb{F}_q$.*

Доказательство. Если $d = 1$, то в лемме 1 из §5 показано, что f не имеет кратных неприводимых множителей над полем $\mathbb{F}_q$.

Пусть $d \neq 1$. Рассмотрим два случая:

1 случай – $f' = 0$. Тогда $f = g^p$ и, очевидно, f имеет кратные неприводимые многочлены над полем $\mathbb{F}_q$.

2 случай – $f' \neq 0$. Воспользуемся следствием . Если имеется k_i такое, что $p \mid k_i$, то f имеет кратный неприводимый множитель. Пусть $p \nmid k_i$ для всех i. Тогда $d = f_1^{k_1-1}, \ldots, f_m^{k_m-1} \neq 1$ и, очевидно, опять f имеет кратный неприводимый множитель над полем $\mathbb{F}_q$. $\square$

Покажем теперь, что задачу о нахождении канонического разложения многочлена над полем $\mathbb{F}_q$ можно свести к задаче нахождения канонического разложения для случая многочлена без кратных неприводимых множителей. Иными словами, укажем алгоритм, который любой нормированный многочлен f положительной степени над полем $\mathbb{F}_q$ раскладывает в произведение многочленов, не имеющих кратных неприводимых множителей над полем $\mathbb{F}_q$.

Вычислим сначала с помощью алгоритма Евклида многочлен

$$d = HOD(f, f').$$

Если $d = 1$, то в силу следствия 3 многочлен f не имеет кратных неприводимых множителей над $\mathbb{F}_q$.

Если $d = f$, то $f' = 0$ и по лемме 11.1 имеем $f = g^p$ для некоторого многочлена $g \in \mathbb{F}_q[x]$. Далее будем применять нашу процедуру к многочлену g, степень которого строго меньше степени f.

Пусть $d \neq 1$ и $d \neq f$, т.е. $0 < deg\ d < n$ и, в частности, $f' \neq 0$. Рассмотрим для f разложение $f = f/d \cdot d$. В силу следствия 2 многочлен $f/d (\neq 1)$ не имеет кратных неприводимых множителей. Далее применяем указанную нами процедуру к многочлену d вместо многочлена f и т.д.

Через некоторое число шагов исходный многочлен будет представлен в виде произведения многочленов, не имеющих кратных неприводимых множителей над полем $\mathbb{F}_q$.

Итак, будем считать далее, что многочлен f степени $n \geq 1$ не имеет кратных неприводимых множителей над полем $\mathbb{F}_q$, т.е.

$$f = f_1, \ldots, f_m,$$

где $f_1, \ldots, f_m$ – попарно различные неприводимые множители над полем $\mathbb{F}_q$.

Наша цель – *построить алгоритм, который по f вычисляет число m и находит многочлены $f_1, \ldots, f_m$.*

Лемма 11.3. *Пусть многочлен $h \in \mathbb{F}_q[x]$ удовлетворяет условию $h^q \equiv h(\mod f)$. Тогда многочлены вида $h - c$, где $c \in \mathbb{F}_q$, попарно взаимно просты и*

$$f = \prod_{c \in \mathbb{F}_q} HOD(f, h - c). \tag{2}$$

Доказательство. Очевидно, многочлены вида $h - c$, где $c \in \mathbb{F}_q$, попарно взаимно просты, т.к. разность двух таких многочленов является ненулевым элементом из $\mathbb{F}_q$. Отсюда следует, что многочлены вида $HOD(f, h - c)$ попарно взаимно просты и правая часть из (2) делит f.

Обратно, из соотношения $x^q - x = \prod\limits_{c \in \mathbb{F}_q} (x - c)$ получаем

$$h^q - h = \prod_{c \in \mathbb{F}_q} (h - c).$$

Поскольку $f_1 \ldots f_m = f | h^q - h$ над $\mathbb{F}_q$, множитель f_i многочлена f делит точно один из многочленов $h - c$, где $c \in \mathbb{F}_q$. Отсюда следует, что f делит правую часть из (2), так как $f_1, \ldots, f_m$ попарно взаимно просты.

Итак, два нормированных многочлена делят друг друга, поэтому они равны. □

Так как многочлены $HOD(f, h - c)$ могут быть приводимы над $\mathbb{F}_q$, равенство (2), вообще говоря, еще не дает неприводимых множителей многочлена f над полем $\mathbb{F}_q$.

Если же $h \equiv c (\mod f)$ для некоторого $c \in \mathbb{F}_q$, то равенство (2) дает лишь тривиальное разложение многочлена f, и поэтому оно вообще в таком случае бесполезно для наших целей.

Если для многочлена $h \in \mathbb{F}_q[x]$ равенство (2) дает нетривиальное разложение многочлена f, то h называют *f-разлагающим*

многочленом. Заметим, что в силу леммы 11.3 любой многочлен, удовлетворяющий системе

$$\begin{cases} h^q \equiv h(\mod f) \\ 0 < deg\ h < n \end{cases},$$

является f-разлагающим.

Теперь мы перейдем к построению f-разлагающих многочленов.

Ясно, что применение равенства (2) к f-разлагающему многочлену требует вычисления q экземпляров HOD, поэтому рассмотренный нами метод имеет смысл применять для малых по числу элементов полей $\mathbb{F}_q$ (по сравнению со степенью n многочлена f).

Лемма 11.4. *Для любого набора элементов $(c_1, \ldots, c_m)$ из $\mathbb{F}_q$ существует единственный многочлен $h \in \mathbb{F}_q[x]$ такой, что $deg\ h < n$ и*

$$h \equiv c_i(\mod f_i) \quad (i = 1, \ldots, m).$$

Доказательство непосредственно следует из китайской теоремы об остатках. □

Лемма 11.5. *Система*

$$\begin{cases} h^q \equiv h(\mod f) \\ 0 < deg\ h < n \end{cases} \tag{3}$$

имеет q^m решений $h \in \mathbb{F}_q[x]$, причем решениями этой системы являются многочлены h, указанные в лемме 11.4, и только они.

Доказательство. Пусть $c_1, \ldots, c_m \in \mathbb{F}_q$ и h многочлен из леммы 11.4, отвечающий этому набору. Тогда

$$h^q \equiv c_i^q = c_i \equiv h(\mod f_i) \quad (i = 1, \ldots, m).$$

Откуда в силу взаимной простоты многочленов $f_1, \ldots, f_m$ вытекает $h^q \equiv h(\mod f)$, т.е. h удовлетворяет системе (3).

Обратно, пусть h – решение системы (3). Тогда в силу равенства

$$h^q - h = \prod_{c \in \mathbb{F}_q} (h - c)$$

каждый из многочленов $f_1, \ldots, f_m$ делит точно один из многочленов $h - c$.

Следовательно, существует единственный набор $c_1, \ldots, c_m \in \mathbb{F}_q$ такой, что

$$h \equiv c_i (\mod f_i) \quad (i = 1, \ldots, m),$$

(отметим, что некоторые из элементов c_i, вообще говоря, могут совпадать!)

Таким образом, имеется взаимно однозначное соответствие между наборами $(c_1, \ldots, c_m)$ и решениями h системы (3). Следовательно система (3) имеет q^m решений в кольце $\mathbb{F}_q[x]$. □

Научимся теперь находить все решения h системы (3) с помощью некоторой вспомогательной системы однородных линейных уравнений.

Вычислим остатки от деления многочленов $1, x^q, x^{2q}, \ldots, c^{(n-1)q}$ на многочлен f над полем $\mathbb{F}_q$, где $n = deg\ f$. Пусть

$$x^{i \cdot q} \equiv b_{i0} + b_{i1}x + \ldots + b_{i(n-1)}x^{n-1} (\mod f) \quad (i = 0, 1, \ldots, n-1).$$

Мы получим матрицу $B = (b_{ij})_{n \times n}$, где $0 \leq i,\ j \leq n-1$. Указанную систему сравнений перепишем в матричном виде, где сравнение по $\mod f$ для многочленных матриц производится покомпонентно:

$$\begin{pmatrix} 1 \\ x^q \\ \vdots \\ x^{(n-1)q} \end{pmatrix} \equiv B \begin{pmatrix} 1 \\ x^q \\ \vdots \\ x^{n-1} \end{pmatrix} (\mod f).$$

Отметим, что сравнение по $\mod f$ для многочленных матриц можно было бы заменить на равенство матриц под кольцом $\mathbb{F}_q[x]/(f)$. Используя операцию транспонирования t,последнее

сравнение матриц перепишем в виде:

$$(1, x^q, \ldots, x^{(n-1)q})^t \equiv B(1, x, \ldots, x^{n-1})^t \ (\mod f).$$

Лемма 11.6. *Многочлен $h = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]$ является решением системы (3) тогда и только тогда, когда строка его коэффициента является решением следующей однородной системы линейных уравнений:*

$$(a_0, a_1, \ldots, a_{n-1})B = (a_0, a_1, \ldots, a_{n-1}). \tag{4}$$

(В дальнейшем для удобства мы будем говорить, что "многочлен h удовлетворяет системе (4) если строка его коэффициента удовлетворяет системе (4)).

Доказательство. $\Rightarrow$. Пусть $h^q \equiv h(\mod f)$. Тогда

$$(a_0, a_1, \ldots, a_{n-1})(1, x, \ldots, x^{n-1})^t = h \equiv h(x)^q = h(x^q) =$$
$$= (a_0, a_1, \ldots, a_{n-1})(1, x^q, \ldots, x^{(n-1)q})^t \equiv$$
$$\equiv (a_0, a_1, \ldots, a_{n-1})B(1, x, \ldots, x^{n-1})^t \ (\mod f).$$

т.е. по $\mod f$ сравнимы два многочлена степени $\leq n-1$. Тогда они равны между собой, т.е.

$$(a_0, a_1, \ldots, a_{n-1})(1, x, \ldots, x^{n-1})^t =$$
$$= (a_0, a_1, \ldots, a_{n-1})B(1, x, \ldots, x^{n-1})^t.$$

Отсюда следует, что совпадают их строки коэффициентов, т.е.

$$(a_0, a_1, \ldots, a_{n-1}) = (a_0, a_1, \ldots, a_{n-1})B.$$

$\Leftarrow$. Обратно, пусть многочлен h удовлетворяет системе (4). Тогда

$$h = (a_0, a_1, \ldots, a_{n-1})(1, x, \ldots, x^{n-1})^t =$$
$$= (a_0, a_1, \ldots, a_{n-1})B(1, x, \ldots, x^{n-1})^t \equiv$$
$$\equiv (a_0, a_1, \ldots, a_{n-1})(1, x^q, \ldots, x^{(n-1)q})^t = h(x^q) = h(x)^q \ (\mod f)$$

□

Систему (4) перепишем в виде:

$$(a_0, a_1, \ldots, a_{n-1}(B - E) = 0, \tag{5}$$

где E – единичная, а 0 – нулевая $(n \times n)$-матрица и $(1 \times n)$-матрица над полем $\mathbb{F}_q$, соответственно.

Согласно леммам 11.5 и 11.6 система (5) имеет q^m решений. Поскольку в поле $\mathbb{F}_q$ имеется q элементов, система (5) имеет q^d решений, где d – дефект системы, т.е. m – дефект системы (5). Пусть $r = r(B - E)$ – ранг матрицы $B - E$. Тогда $m + r = n$, т.е. $\boxed{m = n - r}$.

Иными словами, для того чтобы найти число m различных неприводимых множителей многочлена f над полем $\mathbb{F}_q$, нужно вычислить ранг r матрицы $B - E$ и воспользоваться равенством $m = n - r$.

Для вычисления ранга матрицы $B - E$ можно эту матрицу элементарными преобразованиями по столбцам привести к ступенчатому виду. Отметим, что выгодно применять элементарные преобразования только по столбцам, так как при этом мы будем заменять систему на эквивалентную систему линейных уравнений и в случае надобности решим её.

Если $m = 1$, то $f = f_1$ – неприводимый многочлен над $\mathbb{F}_q$ и вычисление этим завершается.

Отметим, что мы попутно получили *алгоритм для проверки многочлена на неприводимость над полем* $\mathbb{F}_q$.

Пусть теперь $m \geq 2$. Очевидно, многочлен $h_1 = 1$ является решением системы (3) и, следовательно, решением системы (5). Дополним h_1 до базиса пространства решений системы(5):

$$h_1 = 1,\ h_2, \ldots, h_m.$$

Ясно, что многочлены $h_2, \ldots, h_m$ имеют положительные степени, так как они не выражаются линейно через $h_1 = 1$. Следовательно, многочлены $h_2, \ldots, h_m$ удовлетворяют системе (3) и $0 < deg\ h_2, \ldots, deg\ h_m < n$. Поэтому эти многочлены в силу леммы 11.3 являются f-разлагающими.

Возьмем h_2 и вычислим $HOD(f, h_2 - c)$ для всех $c \in \mathbb{F}_q$. В результате мы получим некоторое нетривиальное разложение многочлена f, задаваемое равенством (2). Если при этом мы не получим разложение f на m сомножителей (отметим, что важно лишь число сомножителей в разложении f), то приходим к следующему f-разлагающему многочлену h_3 и находим $HOD(g, h_3 - c)$ для всех $c \in \mathbb{F}_q$ и всех нетривиальных множителей g многочлена f, полученных на предыдущих этапах. Эту процедуру повторяем до тех пор пока не получим разложение f на m сомножителей, которые автоматически будут неприводимы над $\mathbb{F}_q$. В силу следующей леммы указанный нами процесс обязательно приведет к каноническому разложению f на m неприводимых множителей над полем $\mathbb{F}_q$.

Лемма 11.7. *Пусть f_i и f_j – два различных неприводимых множителя многочлена f, где $i,\ j \in \{1, \dots, m\}$ и $i < j$. Тогда существует базисный многочлен h_t для ... $t = 2, \dots, m$, который разделяет f_i и f_j, т.е. для которого существуют такие $c_{ti}, c_{tj} \in \mathbb{F}_q$, что $c_{ti} \neq c_{tj}$ и*

$$h_t \equiv c_{ti} \ (\mod f_i),$$
$$h_t \equiv c_{tj} \ (\mod f_j).$$

Доказательство. В силу лемм 11.5 и 11.4 для любого $t = 2, \dots, m$ существуют такие $c_{ti}, c_{tj} \in \mathbb{F}_q$, что

$$h_t \equiv c_{ti} \ (\mod f_i),$$

$$h_t \equiv c_{tj} \ (\mod f_j).$$

Пусть, от противного, $c_{ti} = c_{tj}$ для любого $t = 2, \dots, m$. Положим $c_{1i} = c_{1j}$ для $h_1 = 1$. Тогда $c_{ti} = c_{tj}$ для любого $t = 1, 2, \dots, m$.

Рассмотрим произвольное решение h системы (5). Оно является линейной комбинацией базисных решений $h_1, \dots, h_m$. Поэтому существует $c \in \mathbb{F}_q$ такое, что

$$h \equiv c(\mod f_i),$$

$$h \equiv c(\mod f_j).$$

С другой стороны, в силу лемм 11.4 и 11.5 для подходящего набора $(0,\dots,0,1,0,\dots,0)$ из m элементов поля $\mathbb{F}_q$ существует решение h системы (5) такое, что

$$h \equiv 0(\mod f_i),$$

$$h \equiv 1(\mod f_j).$$

Итак, имеется решение h системы (5), для которого верны все четыре последних сравнения при некотором c.

Если $c = 0$, то $h \equiv 0(\mod f_j)$ и $h \equiv 1(\mod f_j)$, что противоречиво.

Если $c \neq 0$, то $h \equiv c(\mod f_i)$ и $h \equiv 0(\mod f_i)$, что противоречиво. □

Мы построили и обосновали следующий

Алгоритм Берлекэмпа. Пусть $f \in \mathbb{F}_q[x]$ – нормированный многочлен положительной степени n без кратных неприводимых множителей над $\mathbb{F}_q$, т.е. $HOD(f, f') = 1$. Тогда следующая процедура приводит к построению канонического разложения многочлена f на неприводимые множители над полем $\mathbb{F}_q$.

Шаг 1. Формируем матрицу $B \in M_{n\times n}(\mathbb{F}_q)$ такую, что

$$(1, x^q, \dots, x^{(n-1)q})^t \equiv B(1, x^q, \dots, x^{(n-1)})^t \ (\mod f).$$

Шаг 2. Вычисляем ранг r матрицы $B - E$ и полагаем $m = n - r$ Если $m = 1$, то многочлен f неприводим над $\mathbb{F}_q$ и работа алгоритма завершена.

Шаг 3. При $m \geq 2$ находим m линейно независимых векторов-строк

$$u_1, u_2, \dots, u_m \in \mathbb{F}_q^n$$

таких, что $u_i(B - E) = 0$ для $i = 1$, причем $u_1 = (1, 0, \dots, 0)$.

Шаг 4. Берем многочлен $h_2 = u_2(1, x, \dots, x^{n-1})^t$ и вычисляем $HOD(f, h_2 - c)$ для всех $c \in \mathbb{F}_q$, получаем нетривиальные разложения многочлена f в произведение (не обязательно неприводимое) многочленов.

Если h_2 не дает разложения f на m нетривиальных сомножителей, то для каждого $i = 3, \ldots, m$ последовательно осуществляем следующие вычисления, пока не получим разложение f на m сомножителей. Для каждого $h_i = u_i(1, x, \ldots, x^{n-1})^t$ вычисляем $HOD(g_j, h_i - c)$ для всех $c \in \mathbb{F}_q$ и всех нетривиальных многочленов g_j, полученных на предыдущих этапах и дающих в произведении многочлен f.

На некотором шаге $i = 3, \ldots, m$ многочлен f обязательно будет представлен в виде произведения m сомножителей и алгоритм завершит свою работу (т.е. эти сомножители автоматически будут неприводимы над $\mathbb{F}_q$). $\square$

Пусть $f = g_1, \ldots, g_s$ – разложение f в произведение многочленов степени $< n$, полученное с помощью многочлена h_{i-1}.

Пример. Разложим на неприводимые множители многочлен

$$f = x^8 + x^6 + x^4 + x^3 + 1$$

над полем $\mathbb{F}_2$, применяя алгоритм Берлекэмпа.

Заметим, что $f' = x^2 \Rightarrow f + (x^6 + x^4 + x^2 + x)f' = 1 \Rightarrow$
$\Rightarrow HOD(f, f') = 1$, т.е. многочлен f не имеет кратных неприводимых множителей над $\mathbb{F}_q$.

Найдем вычеты от $x^{i \cdot q}$ по $\mod f$ для $q = 2$ и $i = 0, 1, \ldots, 7$.

	1	x	x^2	x^3	x^4	x^5	x^6	x^7
$1 = x^0 \equiv$	1							
$x^2 \equiv$			1					
$x^4 \equiv$					1			
$x^6 \equiv$							1	
$x^8 \equiv$	1			1	1		1	
$x^{10} \equiv$	1		1	1	1	1		
$x^{12} \equiv$			1		1	1	1	1
$x^{14} \equiv$	1	1		1	1	1		

$x^8 \equiv 1 + x^3 + x^4 + x^6$
$x^{10} \equiv x^2 + x^5 + x^6 + (1 + x^3 + x^4 + x^6) =$
$\quad = 1 + x^2 + x^3 + x^4 + x^5$
$x^{12} \equiv x^2 + x^4 + x^5 + x^6 + x^7$
$x^{13} \equiv x^3 + x^5 + x^6 + x^7 + (1 + x^3 + x^4 + x^6) =$
$\quad = 1 + x^4 + x^5 + x^7$
$x^{14} \equiv x^1 + x^5 + x^6 + (1 + x^3 + x^4 + x^6) =$
$\quad = 1 + x + x^3 + x^4 + x^5$

$$B-E=\begin{bmatrix}0&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0\\0&0&1&0&1&0&0&0\\0&0&0&1&0&0&1&0\\1&0&0&1&0&0&1&0\\1&0&1&1&1&0&0&0\\0&0&1&0&1&1&0&1\\1&1&0&1&1&1&0&1\end{bmatrix}\sim\begin{bmatrix}0&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&1&0\\1&0&0&1&1&0\\1&0&1&1&0&0\\0&0&1&0&0&1\\1&1&1&1&0&1\end{bmatrix}\sim$$

$$\sim\begin{bmatrix}0&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&0&1&0\\1&0&0&0&1&0\\1&0&1&1&0&0\\0&0&1&0&0&1\\1&1&1&1&0&1\end{bmatrix}\sim\begin{bmatrix}0&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&0&1&0\\1&0&0&0&0&0\\1&0&1&1&1&0\\0&0&1&0&0&1\\1&1&1&1&1&1\end{bmatrix}\sim$$

$$\begin{bmatrix}0&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&0&0&1&0&0\\0&0&1&0&0&1\\0&1&0&1&0&1\end{bmatrix}\sim\begin{bmatrix}0&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&0&0&1&0&0\\0&0&1&0&0&1\\0&1&1&1&0&1\end{bmatrix}$$

$r=6\Rightarrow m=n-r=8-6=2$, т.е. f представим в виде

произведения двух неприводимых множителей

$$\begin{cases} a_4 = 0 \\ \text{свободные переменные: } a_0\ a_7 \\ a_1 = a_7 \\ \text{1-е решение: } a_0 = 1, a_7 = 0 \\ a_2 = a_7 \\ u_1 = (1,0,0,0,0,0,0,0) \\ a_5 = a_7 \\ \text{2-е решение: } a_0 = 0, a_7 = 1 \\ a_3 = 0 \\ u_2 = (0,1,1,0,0,1,1,1) \\ a_6 = a_7 \end{cases}$$

u_1, u_2 – базис левого нуль-пространства матрицы $B - E$, $h_1 = 1,\ h_2 = x + x^2 + x^5 + x^6 + x^7$.

Далее с помощью алгоритма Евклида вычисляем $HOD(f, h_2 - c)$ для $c = 0, 1$.

12. Порядок многочлена, характеризация примитивных многочленов

Лемма 12.1. *Пусть f – многочлен степени $m \geq 1$ над полем $\mathbb{F}_q$ и $f(0) \neq 0$. Тогда существует натуральное число $l \leq q^m - 1$ такое, что $f|x^l - 1$ над $\mathbb{F}_q$.*

Доказательство. Фактор-кольцо $\mathbb{F}_q[x]/(f)$ имеет q^m элементов, так как имеется q^m многочленов степени $< m$ над полем $\mathbb{F}_q$. Все q^m классов $x^j + (f)$, где $0 \leq j \leq q^m - 1$, являются ненулевыми. Действительно, если $f|x^j$, то $j \neq 0$ и $f(0) = 0$ – противоречие. Поскольку ненулевых классов имеется точно $q^m - 1$, существуют целые числа i, j такие, что $0 \leq i < j \leq q^m - 1$ и $x^j - x^i \equiv 0(\mod f)$, т.е. $f|x^i(x^{j-i} - 1)$. Так как $HOD(x, f) = 1$, отсюда вытекает $f|x^{j-i} - 1$ над $\mathbb{F}_q$, где $0 < j - i \leq q^m - 1$. □

Пусть $f \in \mathbb{F}_q[x]$, $m = deg\ f \geq 1$ и $f(0) \neq 0$. *Порядком ord f* многочлена f над полем $\mathbb{F}_q$ называется наименьшее натуральное число l такое, что $f|x^l - 1$ над $\mathbb{F}_q$. Порядок многочлена f есть, по существу, мультипликативный порядок многочлена x по $\mod f$, так как условие $f|x^l - 1$ эквивалентно условию $x^l \equiv 1 (\mod f)$.

Заметим, что в силу леммы 12.1 $ord\ f \leq q^m - 1$. Кроме того, очевидно, $ord\ f \geq m$. Таким образом, $m \leq ord\ f \leq q^m - 1$, где $m = deg\ f$.

Теорема 12.1. *Пусть f – неприводимый многочлен степени m над $\mathbb{F}_q$ и $f(0) \neq 0$. Тогда ord f равен порядку любого корня многочлена f в группе $\mathbb{F}^*_{q^m}$.*

(Отметим, что условие $f(0) \neq 0$ здесь эквивалентно тому, что $f \neq cx$ для любого $c \in \mathbb{F}_q \backslash \{0\}$).

Доказательство. Можно считать, что f – нормированный многочлен. Поле $\mathbb{F}_{q^m}$ является полем разложения многочлена f над $\mathbb{F}_q$. Все корни многочлена f, как ранее было установлено, имеют один и тот же порядок в группе $\mathbb{F}^*_{q^m}$. Если $\alpha \in \mathbb{F}^*_{q^m}$ – корень

многочлена f, то в силу того, что f является минимальным многочленом для α над $\mathbb{F}_q$, выполняется

$$\alpha^l = 1 \Leftrightarrow f | x^l - 1 \text{ над } \mathbb{F}_q$$

для любого $l \in \mathbb{N}$. Отсюда следует. что порядок элемента α в группе $\mathbb{F}^*_{q^m}$ равен порядку многочлена. $\square$

Следствие. *Если f – неприводимый многочлен степени m над полем $\mathbb{F}_q$ и $f(0) \neq 0$, то $ord\ f | q^m - 1$.*

Доказательство. Достаточно заметить, что порядок любого корня многочлена f делит $|\mathbb{F}^*_{q^m}| = q^m - 1$. $\square$

Пусть $f \in \mathbb{F}_q[x]$, $deg\ f = m \geq 1$ и $f(0) \neq 0$. В силу леммы 12.1 $ord\ f \leq q^m - 1$. Оказывается, что эта верхняя граница достигается в точности для примитивных многочленов над $\mathbb{F}_q$. Напомним, нормированный неприводимый многочлен степени m над $\mathbb{F}_q$ называется примитивным многочленом над $\mathbb{F}_q$, если его корнем является примитивный элемент поля $\mathbb{F}_{q^m}$. Иными словами, примитивные многочлены над $\mathbb{F}_q$ – это минимальные многочлены примитивных элементов поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$.

Теорема 12.2. *Пусть f – нормированный многочлен степени $m \geq 1$ над $\mathbb{F}_q$ и $f(0) \neq 0$. Многочлен f примитивен над $\mathbb{F}_q$ тогда и только тогда, когда $ord\ f = q^m - 1$.*

Доказательство. $\Rightarrow$. Если f примитивен над $\mathbb{F}_q$, то он неприводим над $\mathbb{F}_{q^m}$, и в силу теоремы 12.1 его порядок $ord\ f$ совпадает с порядком его корня, который является примитивным элементом поля $\mathbb{F}_{q^m}$. Следовательно $ord\ f = q^m - 1$.

$\Leftarrow$. Пусть $ord\ f = q^m - 1$. Нам достаточно установить, что f неприводим над $\mathbb{F}_q$. Действительно, тогда в силу теоремы 12.1 любой корень многочлена f, лежащий в $\mathbb{F}_{q^m}$, имеет порядок $q^m - 1$, т.е. является примитивным элементом поля $\mathbb{F}_{q^m}$ и, следовательно, f – примитивный многочлен над $\mathbb{F}_q$.

Предположим от противного, что f приводим над $\mathbb{F}_q$.

1 случай. f имеет по крайней мере два различных неприводимых множителя над $\mathbb{F}_q$.

Тогда $f = g_1, g_2$, где $g_1, g_2 \in \mathbb{F}_q[x]$, $HOD(g_1, g_2) = 1$, $deg\ g_1 = m_1 \geq 1$, $deg\ g_2 = m_2 \geq 1$ и $m = m_1 + m_2$. Действительно, в качестве g_1 можно взять один из неприводимых множителей многочлена f над $\mathbb{F}_q$ в степени его кратности, а в качестве g_2 – произведение всех остальных неприводимых множителей многочлена f над $\mathbb{F}_q$.

Очевидно, $g_i(0) \neq 0$ $(i = 1, 2)$. Положим $l_i = ord\ g_i$ $(i = 1, 2)$. Очевидно, мы имеем

$$g_1 | x^{l_1} - 1; \quad g_2 | x^{l_2} - 1; \quad x^{l_1} - 1, x^{l_2} - 1 | x^{l_1 l_2} - 1.$$

Откуда следует

$$g_1, g_2 | x^{l_1 l_2} - 1 \Rightarrow f = g_1 g_2 | x^{l_1 l_2} - 1,$$

т.е. $ord\ f \leq l_1 l_2$.

Далее, в силу леммы 12.1 имеем $l_i \leq q^{m_i} - 1$ $(i = 1, 2)$ и поэтому $ord\ f \leq l_1 l_2 \leq (q^{m_1} - 1)(q^{m_2} - 1) = q^{m_1 + m_2} - q^{m_1} - q^{m_2} + 1 < q^m - 1$, что противоречиво.

2 случай. Все неприводимые множители многочлена f над $\mathbb{F}_q$ равны между собой.

Тогда $f = g^k$, где g – нормированный неприводимый многочлен над $\mathbb{F}_q$, $k \in \mathbb{N}$ и $k > 1$. Очевидно, $g(0) \neq 0$. Положим $l = ord\ g$ и $n = deg\ g$. Тогда $l \leq q^n - 1$ и $m = nk$. Пусть $p = char\ \mathbb{F}_q$. Так как $1 = p^{1-1} < k$, существует такое $t \in \mathbb{N}$, что

$$p^{t-1} < k \leq p^t.$$

Покажем, что $ord\ f \leq lp^t$. В самом деле, $g | x^l - 1$ влечет $f = g^k | (x^l - 1)^k \Rightarrow f | (x^l - 1)^{p^t} = x^{lp^t} - 1 \Rightarrow ord\ f \leq lp^t$.

Далее в силу биномиальной формулы Ньютона получаем

$$t \leq ((p - 1) + 1)^{t-1} = p^{t-1} \leq k - 1 \leq (k - 1)n$$

и, кроме того,

$$lp^t \leq (q^n - 1)p^t \leq (q^n - 1)q^t \leq q^{n+t} - q^t < q^{n+t} - 1.$$

Отсюда следует, что

$$ord\ f \leqslant lp^t < q^{n+t} - 1 \leq q^{n+(k-1)n} - 1 = q^{kn} - 1 = q^m - 1.$$

Пришли к противоречию $\square$

Ясно, что поиск примитивных многочленов – это очень важная задача. Один из подходов к ее решению основан на следующем факте.

Теорема 12.3. *Произведение всех примитивных многочленов степени m над $\mathbb{F}_q$ равно (q^m-1)-круговому многочлену Q_{q^m-1} над $\mathbb{F}_q$.*

Доказательство. Данное утверждение следует из того, что поле $\mathbb{F}_q^m$ является (q^m-1)-круговым полем над $\mathbb{F}_q$, а примитивными элементоми поля $\mathbb{F}_q^m$ являются первообразные корни степени $q^m - 1$ из 1 над $\mathbb{F}_q$. $\square$

Таким образом, все примитивные многочлены над $\mathbb{F}_q$ данной степени m можно найти, применяя к Q_{q^m-1} алгоритм Берлекэмпа разложения многочлена на неприводимые множители.

Прежде чем обсудить еще один способ построения примитивного многочлена, рассмотрим некоторый метод нахождения минимального многочлена M для заданного элемента $\beta \in \mathbb{F}_{q^m}$ над полем $\mathbb{F}_{q^m}$.

Сначала находим все сопряженные с β элементы над $\mathbb{F}_q$, т.е. вычисляем элементы

$$\beta, \beta^q, \beta^{q^2}, \dots$$

до тех пор пока не получим наименьшее натуральное число d такое, что $\beta^{q^d} = \beta$. Это число является степенью многочлена M, а сам многочлен M задается формулой

$$M = (x - \beta)(x - \beta^q) \dots (x - \beta^{q^{d-1}}).$$

Справедливость этого равенства следует из результатов §6. Отметим, что многочлен M является минимальным многочленом над $\mathbb{F}_q$ для любого из своих корней.

Пример. Найдем минимальные многочлены над $\mathbb{F}_2$ для всех элементов из $\mathbb{F}_{16}$.

Рассмотрим многочлен $f = x^4 + x + 1 \in \mathbb{F}_2[x]$. Покажем сначала, что f неприводим над $\mathbb{F}_2$. Ясно, что f не имеет над $\mathbb{F}_2$ линейных неприводимых множителей, так как он не имеет корней в поле $\mathbb{F}_2$. Пусть $f = (x^2 + b_1x + c_1)(x^2 + b_2x + c_2)$ над $\mathbb{F}_2$. Тогда, сравнивая коэффициенты при x^3, x^2, x и 1, получаем

$$0 = b_1 + b_2,\ 0 = c_2 + b_1b_2 + c_1,\ 1 = b_1c_2 + c_1b_2,\ 1 = c_1c_2.$$

Из равенства $1 = c_1c_2$ вытекает $c_1 = c_2 = 1$. Тогда $1 = b_1c_2 + c_1b_2 = b_1 + b_2 = 0$, что противоречиво.

Итак, $f = x^4 + x + 1$ неприводим над $\mathbb{F}_2$.

Покажем теперь, что f примитивен над $\mathbb{F}_2$. Для этого в силу теоремы 12.2 достаточно установить, что $ord\ f = 2^4 - 1 = 15$. В силу неприводимости f имеем $ord\ f | 15$. Кроме того, по определению порядка $ord\ f \geq deg\ f = 4$.

Пусть, от противного, $ord\ f < 15$. Тогда в силу предыдущих замечаний $ord\ f = 5$, т.е. $f | x^5 - 1$. Однако это неверно

$$x^5 - 1 = (x^4 + x + 1) \cdot x + (x^2 + x + 1).$$

Итак, $ord\ f = 15$ и многочлен $f = x^4 + x + 1$ примитивен над $\mathbb{F}_2$. Пусть $\theta \in \mathbb{F}_{16}$ – корень примитивного многочлена f над $\mathbb{F}_2$. Тогда

$$\mathbb{F}_{16} = \{\theta^i | i = 0, 1, \ldots, 14\} \cup \{0\} = \{a + b\theta + c\theta^2 + d\theta^3 | a, b, c, d \in \mathbb{F}_2\}$$

и $\theta^{15} = 1$, $\theta^4 = \theta + 1$. Строим таблицу индексов для поля $\mathbb{F}_{16}$:

i	θ^i
0	1
1	θ
2	θ^2
3	θ^3
4	$1 + \theta$

i	θ^i
5	$\theta + \theta^2$
6	$\theta^2 + \theta^3$
7	$1 + \theta + \theta^3$
8	$1 + \theta^2$
9	$\theta + \theta^3$

i	θ^i
10	$1 + \theta + \theta^2$
11	$\theta + \theta^2 + \theta^3$
12	$1 + \theta + \theta^2 + \theta^3$
13	$1 + \theta^2 + \theta^3$
14	$1 + \theta^3$

Теперь будем строить минимальный многочлен для элементов $\beta \in \mathbb{F}_{16}$ над $\mathbb{F}_2$.

1 случай $\beta = 0$. Тогда $M_1 = x$.

2 случай $\beta = 1$. Тогда $M_2 = x + 1$.

3 случай $\beta = \theta$. С ним сопряжены элементы $\theta, \theta^2, \theta^4, \theta^8$, так как $\theta^{16} = \theta$. Тогда $M_3 = (x-\theta)(x-\theta^2)(x-\theta^4)(x-\theta^6) = x^4+x+1$, поскольку θ – корень многочлена $x^4 + x + 1$.

4 случай $\beta = \theta^3$. С ним сопряжены элементы $\theta^3, \theta^6, \theta^{12}, \theta^{24} = \theta^9$, так как $\theta^{18} = \theta^3$. Тогда

$$M_4 = (x - \theta^3)(x - \theta^6)(x - \theta^{12})(x - \theta^9) =$$

$$= (x^2(\theta^3 + \theta^6)x + \theta^9)(x^2 + (\theta^9 + \theta^{12})x + \theta^{21}) =$$

$$= (x^2 + (\theta^3 + \theta^2 + \theta^3)x + \theta^9)(x^2 + (\theta + \theta^3 + 1 + \theta + \theta^2 + \theta^3)x + \theta^6) =$$

$$= (x^2 + \theta^2 x + \theta^9)(x^2 + (1 + \theta^2)x + \theta^6) = x^4 + (1 + \theta^2 + \theta^2)x^3 +$$

$$+(\theta^6 + \theta^2 + \theta^4 + \theta^9)x^2 + (\theta^8 + \theta^9 + \theta^{11})x + \theta^{15} = x^4 + x^3 +$$

$$+(\theta^2+\theta^3+\theta^2+1+\theta+\theta+\theta^3)x^2+(1+\theta^2+\theta+\theta^3+\theta+\theta^2+\theta^3)x+1 =$$

$$= x^4 + x^3 + x^2 + x + 1.$$

5 случай $\beta = \theta^5$. С ним сопряжены элементы θ^5, θ^{10}, так как $\theta^{20} = \theta^5$. Тогда

$$M_5 = (x - \theta^5)(x - \theta^{10}) = x^2 - (\theta^5 + \theta^{10})x + \theta^{15} = x^2 +$$

$$+(\theta + \theta^2 + 1 + \theta + \theta^2)x + 1 = x^2 + x + 1.$$

6 случай $\beta = \theta^7$.С ним сопряжены элементы $\theta^7, \theta^{14}, \theta^{13}, \theta^{11}$, так как $\theta^{22} = \theta^7$. Тогда

$$M_6 = (x - \theta^7)(x - \theta^{14})(x - \theta^{13})(x - \theta^{11}) =$$

$$= x^2 + (\theta^7 + \theta^{14})x + \theta^{21})(x^2 + (\theta^{13} + \theta^{11})x + \theta^{24}) =$$

$$= (x^2+(1+\theta+\theta^3+1+\theta^3)x+\theta^6)(x^2+(1+\theta^2+\theta^3+\theta+\theta^2+\theta^3)+x+\theta^9) =$$

$$= (x^2+\theta x+\theta^6)(x^2+(1+\theta)x+\theta^9) = x^4+(1+\theta+\theta)x^3+(\theta^9+\theta+\theta^2+\theta^6)x^2+$$

$$+(\theta^{10} + \theta^6 + \theta^7)x + \theta^{15} = x^4 + x^3 + (\theta + \theta^3 + \theta + \theta^2 + \theta^2 + \theta^3)x^2 +$$

$$+(1 + \theta + \theta^2 + \theta^2 + \theta^3 + 1 + \theta + \theta^3)x + 1 = x^4 + x^3 + 1.$$

Итак, зная один неприводимый многочлен степени 4 над $\mathbb{F}_2$, мы получили полный список минимальных многочленов для элементов из $\mathbb{F}_{16}$:

$$x,\ x+1,\ x^4+x+1,\ x^4+x^3+x^2+x+1,\ x^2+x+1,\ x^4+x^3+1.$$

Отметим, что для поиска минимальных многочленов элементов поля $\mathbb{F}_{q^m}$ мы можем воспользоваться любым неприводимым, не обязательно примитивным, многочленом степени m над полем $\mathbb{F}_q$.

Опишем теперь второй метод построения примитивных многочленов данной степени m над полем $\mathbb{F}_q$. Сначала ищем примитивный элемент в поле $\mathbb{F}_{q^m}$, затем указанным ранее методом строим его минимальный многочлен, который и будет примитивным многочленом степени m над $\mathbb{F}_q$.

Чтобы найти примитивный элемент в $\mathbb{F}_{q^m}$, представим его порядок в группе $\mathbb{F}_{q^m}^*$ в виде $q^m-1=t_1\dots t_s$, где числа $t_1,\dots,t_s$ попарно взаимно просты. Если для любого $i=1,\dots,s$ мы найдем элемент $\alpha_i\in\mathbb{F}_{q^m}^*$ такой, что $ord\ \alpha_i=t_i$, то элемент $\alpha_1\cdot\ldots\cdot\alpha_s$ будет иметь порядок q^m-1, т.е. будет примитивен в $\mathbb{F}_{q^m}$.

Примеры. Найдем примитивный многочлен степени 4 над $\mathbb{F}_3$. Здесь $q=3,\ m=4$ и $q^m=3^4=81$.

Мы имеем $q^m-1=80=16\cdot5$. Построим сначала в $\mathbb{F}_{81}^*$ два элемента соответственно порядка 16 и порядка 5. Элементы порядка 16 – это корни кругового многочлена $Q_{16}\in\mathbb{F}_3[x]$. Так как $16=2^4$, в силу теоремы 4 из § 9 имеем $Q_{2^4}=1+x^{2^3}$, т.е. $Q_{16}=x^8+1$. Мультипликативный порядок d числа 3 по модулю 16 равен 4, поскольку $3^4=81\equiv1(\mod 16)$ и $3^3=27\equiv11(\mod 16)$. Следовательно, многочлен Q_{16} разлагается по теореме 5 из § 9 на два нормированных неприводимых многочлена степени 4 над $\mathbb{F}_3$. Мы имеем $x^8+1=x^8-2x^4+1-x^4=(x^4-1)^2-x^4=$

$$=(x^4-1+x^2)(x^4-1-x^2)=(x^4+x^2-1)(x^4-x^2-1).$$

Здесь многочлен $f=x^4-x^2-1$ неприводим над $\mathbb{F}_3$ и $\mathbb{F}_{81}=\mathbb{F}_3(\theta)$ для его корня θ. Отсюда $\theta^4=\theta^2+1$. По построению элемент θ

имеет порядок 16 в группе $\mathbb{F}_{81}^*$. Проверим, что $\alpha = \theta + \theta^2$ имеет порядок 5. Действительно,

$$\alpha^5 = (\theta+\theta^2)^5 = \theta^5(\theta+1)^5 = \theta^5(\theta^5+2\theta^4+\theta^3+\theta^2+2\theta+1) =$$
$$= \theta^5(\underline{\theta}^3+\theta+2\theta^2+2+\underline{\theta}^3+\theta^2+2\theta+1) = \theta^5\cdot 2\theta^3 = 2(\theta^4)^2 =$$
$$= 2(\theta^2+1)^2 = 2(\theta^4+2\theta^2+1) = 2(\theta^2+1+2\theta^2+1) = 2\cdot 2 = 1.$$

Следовательно, элемент $\beta = \theta\cdot\alpha = \theta^2+\theta^3$ имеет порядок 80, т.е является примитивным элементом в $\mathbb{F}_{81}$,

Найдем элементы, сопряженные с β: $\beta, \beta^3, \beta^9, \beta^{27}$ (так как $\beta^{81} = \beta$)

$$\beta^3 = (\theta^2+\theta^3)^3 = \theta^6+\theta^9 = \theta^4+\theta^2+(\theta^4+2\theta^2+1)\theta =$$
$$= \theta^2+1+\theta^2+(\theta^2+1+2\theta^2+1)\theta = 2\theta^2+1+2\theta = 1-\theta-\theta^2;$$
$$\beta^9 = (1-\theta-\theta^2)^3 = 1-\theta^3-\theta^6 = 1-\theta^3-\theta^4-\theta^2 = 1-\theta^3-\theta^2-1-\theta^2 =$$
$$= -\theta^3-2\theta^2 = \theta^2-\theta^3;$$
$$\beta^{27} = (\theta^2-\theta^3)^3 = \theta^6-\theta^9 = \theta^4+\theta^2-\theta(\theta^4+2\theta^2+1) =$$
$$= \theta^2+1+\theta^2-\theta(\theta^2+1+2\theta^2+1) = 2\theta^2+1-2\theta = 1+\theta-\theta^2.$$

Минимальным многочленом для β служит следующий многочлен степени 4 над $\mathbb{F}_3$:

$$M = (x-\beta)(x-\beta^3)(x-\beta^9)(x-\beta^{27}) =$$
$$= (x-\theta^2-\theta^3)(x-1+\theta+\theta^2)(x-\theta^2+\theta^3)(x-1-\theta+\theta^2) =$$
$$= (x^2-2\theta^2x+(\theta^4-\theta^6))(x^2+2(-1+\theta^2)x+(\theta^2-1)^2-\theta^2) =$$
$$= (x^2+\theta^2x+\theta^4-\theta^4-\theta^2)(x^2+(1-\theta^2)x+\theta^4-2\theta^2+1-\theta^2) =$$
$$= (x^2+\theta^2x-\theta^2)(x^2+(1-\theta^2)x+\theta^2+1+1) =$$
$$= (x^2+\theta^2x-\theta^2)(x^2+(1-\theta^2)x+\theta^2-1) =$$
$$= x^4+(1-\theta^2+\theta^2)x^3+(\theta^2-1+\theta^2-\theta^4-\theta^2)x^2+$$
$$+(\theta^4-\theta^2-\theta^2+\theta^4)x-\theta^4+\theta^2 = x^4+x^3+(\theta^2-1-\theta^2-1)x^2+$$
$$+(2\theta^2+2-2\theta^2)x-\theta^2-1+\theta^2 = \underline{x^4+x^3+x^2-x-1}$$

– это примитивный многочлен степени 4 и порядка 80 над $\mathbb{F}_3$.

13. Семейство нормированных неприводимых многочленов данной степени над конечным полем

Лемма 13.1. *Пусть f – нормированный неприводимый многочлен степени m над $\mathbb{F}_q$ и $n \in \mathbb{N}$. Тогда $f|x^{q^n} - x$ над $\mathbb{F}_q$ в том и только в том случае, когда $m|n$.*

Доказательство. $\Rightarrow$. Верно в силу лемм 2 из § 6.

$\Leftarrow$ Пусть $m|n$. Тогда $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$. В § 6 мы доказали, что $\mathbb{F}_{q^m}$ – поле разложения для многочлена f над $\mathbb{F}_q$. Пусть $\alpha \in \mathbb{F}_{q^m}$ и $f(\alpha) = 0$. Тогда $\alpha \in \mathbb{F}_{q^n} \Rightarrow \alpha^{q^n} = \alpha \Rightarrow f|x^{q^n} - x$, так как f – минимальный многочлен для α. □

Теорема 13.1. *Для любого конечного поля $\mathbb{F}_q$ и любого $n \in \mathbb{N}$ многочлен $x^{q^n} - x$ равен произведению всех нормированных неприводимых многочленов над $\mathbb{F}_q$, степень которых делит n.*

Доказательство. По лемме1 каноническое разложение многочлена $g = x^{q^n} - x$ на неприводимые многочлены над $\mathbb{F}_q$ содержит те и только те нормированные неприводимые многочлены над $\mathbb{F}_q$, степень которых делит n. Так как $g' = -1$, многочлен g не имеет кратных неприводимых множителей над $\mathbb{F}_q$. □

Через $I_q(n)$ будем обозначать число нормированных неприводимых многочленов степени n над $\mathbb{F}_q$.

Следствие. *Для любого $n \in \mathbb{N}$ выполняется*

$$q^n = \sum_{d|n} d \cdot I_q(d)$$

Теорема 13.2. *Для любого $n \in \mathbb{N}$ выполняется*

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Доказательство. Применим аддитивный вариант формулы обращения Мёбиуса к группе $G = \mathbb{Z}$, $h(n) = nI_q(n)$, $H(n) = q^n$ $(n \in \mathbb{N})$ и равенству из следствия . $\square$

Пример.

1)

n	1	2	3	4	5	6
$I_3(n)$	3	3	8	18	45	116

$I_3(1) = \frac{1}{1}\mu(1)3^1 = 3;$

$I_3(2) = \frac{1}{2}(\mu(1)3^2 + \mu(2)3^1) = \frac{1}{2}(9-3) = 3;$

$I_3(3) = \frac{1}{3}(\mu(1)3^3 + \mu(3)3^1) = \frac{1}{3}(27-3) = 8;$

$I_3(4) = \frac{1}{4}(\mu(1)3^4 + \mu(2)3^2 + \mu(4)3^1) = \frac{1}{4}(3^4 - 3^2) = \frac{1}{4}3^2 \cdot 8 = 18;$

$I_3(5) = \frac{1}{5}(\mu(1)3^5 + \mu(5)3^1) = \frac{1}{5}(3^5 - 3) = \frac{1}{5}3 \cdot 80 = 48;$

$I_3(6) = \frac{1}{6}(\mu(1)3^6 + \mu(2)3^3 + \mu(3)3^2 + \mu(6)3^1) =$

$= \frac{1}{6}(3^6 - 3^3 - 3^2 + 3) = \frac{1}{2}(3^5 - 3^2 - 3 + 1) =$

$= \frac{1}{2}(3^2 \cdot 26 - 2) = 3^2 \cdot 13 - 1 = 116.$

2) Число нормированных неприводимых многочленов степени 12 над $\mathbb{F}_q$ равно:

$$I_q(12) = \frac{1}{12}(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 +$$

$$+\mu(6)q^2 + \mu(12)q^1) = \frac{1}{12}(q^{12} - q^6 - q^4 + q^2).$$

Через $I(q, n; x)$ обозначим произведение всех нормированных неприводимых многочленов степени n над полем $\mathbb{F}_q$. Теорему 13.1 можно сформулировать следующим образом: для любого $n \in \mathbb{N}$ выполняется

$$x^{q^n} - x = \prod_{d|n} I(q, d; x).$$

Теорема 13.3. *Для любого $n \in \mathbb{N}$ выполняется*

$$I(q,n;x) = \prod_{d|n}(x^{q^d} - x)^{\mu(n/d)} = \prod_{d|n}(x^{q^{n/d}} - x)^{\mu(d)}.$$

Доказательство. Применяем к указанному перед теоремой равенству мультипликативный вариант формулы обращения Мёбиуса для мультипликативной группы $G = \mathbb{F}_q(x)^*$ ненулевых рациональных дробей над полем $\mathbb{F}_q$, $h(n) = I(q,n;x)$ и $H(n) = x^{q^n} - x$ $(n \in \mathbb{N})$. □

Пример. Для $q = 2$ и $n = 4$ получаем

$$I(2,4;x) = (x^{2^4} - x)^{\mu(1)}(x^{2^2} - x)^{\mu(2)}(x^{2^1} - x)^{\mu(4)} =$$
$$= (x^{16} - x)(x^4 - x)^{-1} = \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} =$$
$$= 1 + x^3 + x^6 + x^9 + x^{12}.$$

Отметим, что $I_2(4) = \frac{12}{4} = 3$.

Все нормированные неприводимые многочлены данной степени n над полем $\mathbb{F}_q$ можно найти, раскладывая на неприводимые множители многочлен $I(q,n;x)$.

В этой связи очень полезно представить $I(q,n;x)$ хотя бы в частично разложенном виде. Такую возможность дает следующая теорема.

Напомним сначала, что через $ord_m(q)$ мы обозначаем мультипликативный порядок числа q по $\bmod m$. По определению $ord_m(q) = n$ тогда и только тогда, когда $q^n \equiv 1 (\bmod m)$ и $q^l \not\equiv 1$ для любого $l = 1, \ldots, n-1$, т.е. $m | q^n - 1$ и $m \nmid q^l - 1$ для любого $l = 1, \ldots, n-1$. Отметим, что, очевидно, $ord_{q^n-1}(q) = n$ для любого $n \in \mathbb{N}$.

Теорема 13.4. *Для любого натурального $n > 1$ выполняется*

$$I(q,n;x) = \prod_{ord_m(q)=n} Q_m,$$

где Q_m – круговые многочлены над $\mathbb{F}_q$, а произведение берется по всем натуральным делителям m числа q^n-1, для которых мультипликативный порядок числа q по модулю m равен n.

(Заметим, что в указанное произведение обязательно входит множитель θ_{q^n-1}, который равен произведению всех примитивных многочленов степени n над полем $\mathbb{F}_q$).

Доказательство. Заметим, что в силу результатов § 6 любой неприводимый многочлен степени n над полем $\mathbb{F}_q$ разложим на линейные множители над $\mathbb{F}_{q^n}$, не имеет кратных корней и все его корни в $\mathbb{F}_{q^n}$ образуют класс сопряженных элементов.

Следовательно многочлен $I(q,n;x)$ разложим на линейные множители над $\mathbb{F}_{q^n}$ и не имеет кратных корней.

Через S обозначим множество всех элементов из $\mathbb{F}_{q^n}$ степени n над полем $\mathbb{F}_q$. Каждый элемент $\alpha \in S$ имеет минимальный многочлен степени n над $\mathbb{F}_q$ и поэтому является корнем многочлена $I(q,n;x)$. Обратно, если α – корень многочлена $I(q,n;x)$ из поля $\mathbb{F}_{q^n}$, то α является корнем некоторого нормированного неприводимого многочлена степени n над $\mathbb{F}_q$ и, следовательно, $\alpha \in S$.

Таким образом,

$$I(q,n;x) = \prod_{\alpha \in S} (x-\alpha).$$

Для каждого положительного делителя m числа q^n-1 такого, что $ord_m(q) = n$ через S_m обозначим множество всех элементов порядка m из $\mathbb{F}^*_{q^n}$. Покажем, что

$$S = \bigcup_{ord_m(q)=n} S_m.$$

Пусть $\alpha \in S$. Положим $m \rightleftharpoons ord\ \alpha$ в группе $\mathbb{F}^*_{q^n}$. По теореме Лагранжа $m | q^n-1$. Если $m | q^l-1$ для некоторого $l = 1, \ldots, n-1$, то $\alpha^{q^l-1} = 1 \Rightarrow \alpha^{q^l} = \alpha \Rightarrow$ степень α над $\mathbb{F}_q$ меньше или равна $l < n$ – противоречие. Следовательно, $ord_m(q) = n$ и $\alpha \in S_m$.

Обратно, пусть $\alpha \in S_m$ и $ord_m(q) = n$. Тогда $\alpha \in \mathbb{F}_{q^n}$ и $m = ord\ \alpha$. Если $\alpha \in \mathbb{F}_{q^l} \subset \mathbb{F}_{q^n}$ для некоторого натурального

$l = 1, \ldots, n-1$, то $\alpha^{q^l} = \alpha \Rightarrow \alpha^{q^l-1} = 1 \Rightarrow m|q^l - 1$ – противоречие. Следовательно, α лежит в $\mathbb{F}_{q^n}$ и не лежит в собственных подполях этого поля, являющихся расширениями поля $\mathbb{F}_q$, т.е. $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. Поэтому степень α над $\mathbb{F}_q$ равна n и $\alpha \in S$.

В силу доказанного получаем следующее равенство

$$I(q, n; x) = \prod_{ord_m(q)=n} \prod_{\alpha \in S_m} (x - \alpha).$$

Для каждого рассматриваемого значения m множество S_m состоит из всех элементов группы $\mathbb{F}_{q^n}^*$, имеющих порядок m. Другими словами, S_m – множество первообразных корней m-й степени из единицы над $\mathbb{F}_q$. Тогда по определению кругового многочлена получаем

$$\prod_{\alpha \in S_m} (x - \alpha) = Q_m$$

и формула доказана. □

Пример. Найдем все нормированные неприводимые многочлены степени 4 над $\mathbb{F}_2$.

Покажем сначала. что в силу теоремы 13.4 выполняется

$$I(2, 4; x) = Q_5 Q_{15}$$

Действительно, $q^n - 1 = 2^4 - 1 = 15$. Найдем все натуральные делители m числа 15 такие, что $ord_m(2) = 4$. Имеем $ord_1(2) = 1$, $ord_3(2) = 2$, $ord_5(2) = 4$, так как $2^4 \equiv 1(\mod 5)$, $2^3 \equiv 3(\mod 5)$, $2^2 \equiv 4(\mod 5)$. Число $m = 15 = q^n - 1$ также подходит (так как число $m = q^n - 1$ подходит во всех случаях!), т.е. $ord_{15}(2) = 4$.

Рассмотрим многочлен Q_5 По теореме 3 § 9 имеем

$$Q_5 = (x^5 - 1)^{\mu(1)}(x - 1)^{\mu(5)} = \frac{x^5 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4.$$

Ясно, что Q_5 неприводим над $\mathbb{F}_2$, так как все неприводимые множители многочлена $I(2, 4; x)$ над $\mathbb{F}_2$ имеют степень 4.

Рассмотрим теперь Q_{15}. По теореме 3 из § 9 имеем

$$\begin{aligned} Q_{15} &= (x^{15}-1)^{\mu(1)}(x^5-1)^{\mu(3)}(x^3-1)^{\mu(5)}(x-1)^{\mu(15)} = \\ &= (x^{15}-1)(x^5-1)^{-1}(x^3-1)^{-1}(x-1) = \\ &\quad \frac{x^{15}-1}{x^5-1}\cdot\frac{x-1}{x^3-1} = \frac{1+x^5+x^{2\cdot 5}}{1+x+x^2} = \\ &\quad = x^8+x^7+x^5+x^4+x^3+x+1, \end{aligned}$$

так как $x^{10}+x^5+1 = (x^2+x+1)(x^8+x^7+x^5+x^4+x^3+x+1)$.

Все неприводимые множители многочлена Q_{15} над $\mathbb{F}_2$ имеют степень 4, так как они делят $I(2,4;x)$, поэтому Q_{15} разложим в произведение двух неприводимых над $\mathbb{F}_2$ многочленов степени 4. Найдем эти многочлены.

Очевидно, многочлен $Q_5(x+1)$ неприводим над $\mathbb{F}_2$. Действительно, если $Q_5(x+1$ приводим над $\mathbb{F}_2$, то после подстановки вместо x многочлена $x+1$ получим, что многочлен $Q_5(x)$ приводим над $\mathbb{F}_2$. Вычислим

$$Q_5(x+1) = (x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1$$

с помощью схемы Горнера: $Q_5(x+1) = x^4+x^3+1$.

Поскольку многочлен x^4+x^3+1 неприводим над $\mathbb{F}_2$ и отличен от Q_5, в силу равенства $I(2,4;x) = Q_5Q_{15}$ он делит Q_{15} над $\mathbb{F}_2$. $x^8+x^7+x^5+x^4+x^3+x+1 = (x^4+x^3+1)(x^4+x+1)$.

Таким образом, $Q_{15} = (x^4+x^3+1)(x^4+x+1)$ – разложение на неприводимые множители над полем $\mathbb{F}_2$.

Итак, все нормированные неприводимые многочлены степени 4 над $\mathbb{F}_2$ исчерпываются следующими тремя многочленами:

$$x^4+x^3+x^2+x+1,$$
$$x^4+x^3+1,$$
$$x^4+x+1.$$

Заметим, что эти многочлены мы уже находили раньше как минимальные многочлены для некоторых элементов поля $\mathbb{F}_{16}$.

14. Метод вычисления минимального многочлена

Пусть α – порождающий элемент поля $\mathbb{F}_{q^n}$ над полем $\mathbb{F}_q$, т.е $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. Тогда n – степень элемента α и $1, \alpha, \ldots, \alpha^{n-1}$ – базис поля $\mathbb{F}_{q^n}$ над полем $\mathbb{F}_q$.

Для того чтобы найти минимальный многочлен M элемента $\beta \in \mathbb{F}_{q^n}^*$ над $\mathbb{F}_q$, сначала выразим $\beta^0, \beta^1, \ldots, \beta^n$ через элементы указанного базиса:

$$\beta^i = \sum_{j=0}^{n-1} d_{ij}\alpha^j \quad (0 \le i \le n).$$

Иными словами,

$$(\beta^0, \beta^1, \ldots, \beta^n)^t = D(1, \alpha, \ldots, \alpha^{n-1})^t,$$

где $D = (d_{ij})_{(n+1)\times n}$ и $0 \le i \le n,\ 0 \le j \le n-1$.

Пусть $M = a_0 + a_1 x + \ldots + a_n x^n = (a_0, a_1, \ldots, a_n)(1, x, \ldots, x^n)^t$. Нужно, чтобы M был нормированным многочленом наименьшей степени, удовлетворяющим равенству $M(\beta) = 0$, т.е.

$$(a_0, a_1, \ldots, a_n)(1, \beta, \ldots, \beta^n)^t = 0.$$

что эквивалентно условию

$$(a_0, a_1, \ldots, a_n)D(1, \alpha, \ldots, \alpha^{n-1})^t = 0.$$

В силу линейной независимости $1, \alpha, \ldots, \alpha^{n-1}$ отсюда получаем эквивалентное равенство

$$(a_0, a_1, \ldots, a_n)D = 0.$$

Пусть $rank\ D = r$ и дефект равен $s = (n+1) - r$. Можно доказать, что в качестве s свободных неизвестных всегда можно взять s последних неизвестных (мы это доказывать не будем!).

Если $s = 1$, то положим $a_n = 1$. Остальные же коэффициенты определяются системой однозначно, и мы получим минимальный многочлен M для β.

Пусть $s > 1$. Тогда минимальный многочлен M получим при $a_n = a_{n-1} = \ldots = a_{n-s+2} = 0$ и $a_{n-s+1} = 1$. (Заметим, что другие наборы при $c_i \neq 0$ для некоторого $i \in \{n, n-1, \ldots, n-s+2\}$ дают многочлены большей степени. Следовательно, если в процессе решения мы установили, что последние s неизвестные образуют систему свободных неизвестных, то мы можем быть уверены, что построим именно минимальный минимальный многочлен M).

Пример. Пусть $\alpha \in \mathbb{F}_{64}$ – корень неприводимого многочлена $x^6 + x + 1$ над $\mathbb{F}_2$. Найдем минимальный многочлен M для $\beta = \alpha^3 + \alpha^4$.

Сначала ищем матрицу D, учитывая, что $\alpha^6 = \alpha + 1 = 1 + \alpha$.

$$\beta^0 = 1$$
$$\beta^1 = \alpha^3 + \alpha^4$$
$$\beta^2 = \alpha^6 + \alpha^8 = 1 + \alpha + \alpha^2 + \alpha^3$$
$$\beta^3 = (1 + \alpha + \alpha^2 + \alpha^3)(\alpha^3 + \alpha^4) =$$
$$= \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 =$$
$$= \alpha^3 + \alpha^7 = \alpha^3 + \alpha + \alpha^2 = \alpha + \alpha^2 + \alpha^3$$
$$\beta^4 = (\alpha + \alpha^2 + \alpha^3)(\alpha^3 + \alpha^4) = \alpha^4 + \alpha^5 + \alpha^6 + \alpha^5 + \alpha^6 + \alpha^7 =$$
$$= \alpha^4 + \alpha^7 = \alpha + \alpha^2 + \alpha^4$$
$$\beta^5 = (\alpha + \alpha^2 + \alpha^4)(\alpha^3 + \alpha^4) = \alpha^4 + \alpha^5 + \alpha^7 + \alpha^5 + \alpha^6 + \alpha^8 =$$
$$= \alpha^4 + \alpha^6 + \alpha + \alpha^2 + \alpha^2 + \alpha^3 = \alpha^4 + 1 + \alpha + \alpha + \alpha^3 = 1 + \alpha^3 + \alpha^4$$
$$\beta^6 = (1 + \alpha^3 + \alpha^4)(\alpha^3 + \alpha^4) = \alpha^2 + \alpha^4 + \alpha^6 = 1 + \alpha + \alpha^2 + \alpha^4$$

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$rank\ D = 3$

$$s = n + 1 - r = 7 - 3 = 4$$

$$\begin{array}{cccccc} (a_0, a_1, a_2, & a_3, & a_4, & a_5, & a_6) & \begin{cases} a_0 = a_3 + a_4 + a_5 \\ a_1 = a_4 + a_5 + a_6 \\ a_2 = a_3 + a_4 + a_6 \end{cases} \\ & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \\ & 1 & 0 & 0 & 0 & \end{array}$$

$$\begin{cases} a_0 = a_3 = 1 \\ a_1 = 0 \\ a_2 = a_3 = 1 \end{cases}$$

т.е. $M = 1+x^2+x^3$ – минимальный многочлен элемента $\beta = \alpha^3+\alpha^4$ над полем $\mathbb{F}_2$

Литература

1. **Александров П.С.** Введение в теорию множеств и общую топологию. М.: Наука, 1977.
2. **Баранский В.А.** Введение в общую алгебру: Учеб. пособие. Свердловск: УрГУ, 1991.
3. **Биркгоф Г., Барти Т.** Современная прикладная алгебра. М.: Мир, 1976.
4. **Важенин Ю.М., Замятин А.П.** Введение в математическую логику: Учеб. пособие. Свердловск: УрГУ, 1984.
5. **Ван-дер-Варден Б.Л.** Алгебра. М.: Наука, 1976.
6. **Горбатов В.А.** Основы дискретной математики. М.: Высш. шк., 1986.
7. **Калужнин Л.А.** Введение в общую алгебру. М.: Наука, 1973.
8. **Кон П.** Универсальная алгебра. М.: Мир, 1968.
9. **Кострикин А.И.** Введение в алгебру. М.: Наука, 1977.
10. **Кузнецов О.П., Адельсон-Вельский Г.М.** Дискретная математика для инженера. М.: Энергия, 1980.
11. **Курош А.Г.** Лекции по общей алгебре. М.: Физматгиз, 1962.
12. **Ленг С.** Алгебра. М.: Мир, 1968.

13. **Лидл Р., Нидеррайтер Г.** Конечные поля Том 1, 2 : Мир, 1988.

14. **Мальцев А.И.** Алгебраические системы. М.: Наука, 1970.

15. **Саломаа А.** Жемчужины теории формальных языков. М.: Мир, 1986.

16. **Скорняков Л.А.** Элементы теории структур. М.: Наука, 1982.

17. **Скорняков Л.А.** Элементы общей алгебры. М.: Наука, 1983.

18. **Яблонский С.В.** Введение в дискретную математику. М.: Наука, 1986.