О.В. Маркова

Алгебраические основы теории кодов и линейных рекуррентных последовательностей

Версия от *27 апреля 2023г.*

Содержание

Лекция 1. Основные параметры кодов: размерность, расстояние Хэмминга, исправление ошибок. Линейные коды. Граница Синглтона. МДР-коды, их свойства. Граница Хэмминга (граница сферической упаковки). Совершенные коды. Двоичный код Хэмминга. Граница Плоткина. Эквидистантные коды. Симплексный код.

Под *кольцом* в нашем курсе будет пониматься конечное ассоциативное, коммутативное кольцо с единицей, т.е. конечное множество $(\mathcal{R}, +, \cdot)$ с двумя бинарными операциями (для удобства их называют сложением и умножением), удовлетворяющими следующим аксиомам:
1) $(\mathcal{R}, +)$ — абелева группа с нейтральным элементом 0 (аддитивная группа кольца);
2) выполнены тождества *дистрибутивности*:

$$\forall a, b, c \in \mathcal{R}, \quad a(b + c) = ab + ac, \quad (a + b)c = ac + bc;$$

3) $(\mathcal{R}, \cdot)$ — полугруппа, т.е. операция $\cdot$ ассоциативна;
4) в $\mathcal{R}$ имеется нейтральный относительно умножения элемент 1 (или e, или 1_R, когда приходится говорить одновременно о разных кольцах);
5) $\forall a, b, c \in \mathcal{R}, \quad ab = ba$, т.е. операция $\cdot$ коммутативна.

Определение 1.1. *Правым модулем* над кольцом $\mathcal{R}$, или правым $\mathcal{R}$-модулем, называется абелева группа $(M, +)$ с определёнными на ней операциями умножения справа на элементы кольца $\mathcal{R}$, которые удовлетворяют тождествам

$$a(rs) = (ar)s, \ (a + b)r = ar + br, \ a(r + s) = ar + as, a \cdot 1 = a$$

для всех $a, b \in M, \ r, s \in \mathcal{R}$.

Аналогично можно определить левый $\mathcal{R}$-модуль.

Определение 1.2. *Подмодуль* произвольного модуля M — это его подмножество, содержащее 0 и замкнутое относительно операций сложения, взятия противоположного элемента и умножения на элементы кольца.

Определение 1.3. Внешняя *прямая сумма* $M_1 \oplus \ldots \oplus M_n$ $\mathcal{R}$-модулей $M_1, \ldots, M_n$ — множество всех строк $(m_1, \ldots, m_n)$, где $m_i \in$

M_i $\forall i \in \{1, \ldots, n\}$, с покомпонентными сложением и умножением на элементы кольца $\mathcal{R}$.
В частности, если $M_1 = \ldots = M_n = M$ мы будем рассматривать $\mathcal{R}$ модуль M^n строк длины n.

Определение 1.4. Отображение $f : M \to N$ правых модулей над кольцом $\mathcal{R}$ называется *гомоморфизмом*, если

$$\forall a, b \in M,\ r \in \mathcal{R},\ f(a+b) = f(a) + f(b),\ f(ar) = f(a)r.$$

Гомоморфизм модулей называется *изоморфизмом*, если он является биективным отображением. Изоморфизм модуля в себя называется *автоморфзмом*.

1°. Основные параметры кодов: размерность, расстояние Хэмминга, исправление ошибок. Линейные коды.

Определение 1.5. Пусть Ω — некоторое конечное множество, $|\Omega| > 1$, — *алфавит*. Пусть n — натуральное число, Ω^n — декартова степень множества Ω. Элементы множества Ω^n будем называть *словами длины* n в алфавите Ω.

Определение 1.6. *Расстоянием Хэмминга* между словами $\mathbf{a} = (a_1, \ldots, a_n)$ и $\mathbf{b} = (b_1, \ldots, b_n)$ из Ω^n назовём число

$$d(\mathbf{a}, \mathbf{b}) = |\{i : 1 \le i \le n \ \&\ a_i \ne b_i\}|.$$

Нетрудно проверить, что (Ω, d) — метрическое пространство, которое и называется *пространством Хэмминга*.

Определение 1.7. Произвольное непустое подмножество $\mathcal{C}$ пространства Ω^n называется *кодом длины* n над алфавитом Ω.

Определение 1.8. *Размерностью* (более точно, *комбинаторной размерностью*) кода $\mathcal{C}$ называется действительное число $\dim(\mathcal{C}) = \log_q |\mathcal{C}|$, где $q = |\Omega|$.

Определение 1.9. *Расстоянием* (точнее, *минимальным расстоянием*) кода $\mathcal{C}$ при $|\mathcal{C}| > 1$ называется число

$$d(\mathcal{C}) = \min\{d(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathcal{C}\ \&\ \mathbf{a} \ne \mathbf{b}\},$$

расстояние кода из одного слова можно считать равным 0.

Если код $\mathcal{C}$ над алфавитом мощности q имеет длину n, размерность k и расстояние d, говорят, что $\mathcal{C}$ есть $[n, k, d]_q$-код. Некоторые из этих параметров можем опускать, если они неизвестны или несущественны.

Передачу информации по каналу связи можно описать следующим образом:

$$\text{слово } w \xrightarrow{\text{канал связи}} \text{слово } w' .$$

Если $w' \neq w$, говорят, что при передаче данных произошла ошибка. В простейшем случае можно считать, что искажения любых двух символов — равновероятные независимые события. Желательно, чтобы приёмник мог обнаруживать и, по возможности, исправлять слово w', получая исходное слово w.

Для этого применяют процесс кодирования/декодирования, который можно описать так.

Пусть M — известное множество входных слов (как правило, $M = \Omega^k$ для некоторого натурального числа k). Выбирается некоторое инъективное отображение (кодирование) $\varphi : M \to \Omega^n$, где $\mathcal{C} = \varphi(M)$ — некоторый известный код. Допустим, надо передать слово m. Вместо него по каналу связи передаётся слово $w = \varphi(m)$ и полученное слово w' проверяется на принадлежность коду $\mathcal{C}$. Если $w' \in \mathcal{C}$, считается, что передано (однозначно определённое) слово $\varphi^{-1}(w')$. Если же $w' \notin \mathcal{C}$, выбирается ближайшее (в смысле Хэмминга) к w' слово $w'' \in \mathcal{C}$. Если такое слово определено однозначно, предполагается, что передано слово $\varphi^{-1}(w'')$ (*принцип максимального правдоподобия*). Если же на минимальном расстоянии от слова w' находится несколько слов, принадлежащих коду $\mathcal{C}$, то фиксируется ошибка, которую невозможно исправить.

Теорема 1.10. Пусть d — расстояние Хэмминга кода $\mathcal{C}$, $2r < d$ и $s < d$. Тогда код $\mathcal{C}$ обнаруживает s ошибок и исправляет r ошибок.

◀ Очевидно, что если $m \in M$, $d(w', \varphi(m)) = s < d(\mathcal{C})$ и $w' \in \mathcal{C}$, то $w' = \varphi(m)$. Заметим, что для любого слова $a \in \Omega^n$ существует не более одного слова $c \in \mathcal{C}$, для которого выполнено неравенство $d(a, c) \leq r$. Действительно, пусть $c_1, c_2 \in C$, $d(a, c_1) \leq r$ и $d(a, c_2) \leq r$. Тогда $d(c_1, c_2) \leq d(c_1, a) + d(a, c_2) \leq 2r < d$, откуда $c_1 = c_2$. Поскольку, по предположению, $d(w', \varphi(m)) = r$ и $\varphi(m) \in \mathcal{C}$, получаем, что $w'' = \varphi(m)$ и $\varphi^{-1}(w'') = m$. ▶

Примеры.
1. Повторение слова. Если любое слово $w = (w_1, \ldots, w_k)$ кодировать словом $(w|w) = (w_1, \ldots, w_k, w_1, \ldots, w_k)$, то получается $[2k, k, 2]$-код. Видно, что он обнаруживает одну ошибку и ни одной не исправляет, а объём передаваемой информации увеличивается вдвое.
2. Код проверки на чётность. Пусть на множестве Ω задана групповая операция "+" (не обязательно коммутативная). Тогда слово $w = (w_1, \ldots, w_k)$ можно кодировать словом $(w_1, \ldots, w_k, -(w_k + \ldots + w_1))$. Тогда получится $[k+1, k, 2]$-код, но скорость передачи информации (т.е. отношение k/n) у кода проверки на чётность выше, чем у кода удвоения.

Определение 1.11. Пусть M — конечный правый или левый модуль над кольцом $\mathcal{R}$, $|M| \geq 2$. *Линейным кодом длины* n над модулем M называется произвольный подмодуль $\mathcal{R}$-модуля M^n.

Основные частные случаи:
$M = \mathcal{R}_{\mathcal{R}}$ или $M = {}_{\mathcal{R}}\mathcal{R}$ — говорят о коде над кольцом $\mathcal{R}$.
$M = \mathcal{R}$, где $\mathcal{R} = \mathbb{F}$, $\mathbb{F}$ — конечное поле. В этом случае говорят о линейных кодах над полем $\mathbb{F}$.

Примеры. Почти все коды, которые мы построим в данной лекции — линейные коды над полем (двоичный код Хэмминга, обобщённый код Рида–Соломона, симплексный код).

Определение 1.12. Пусть M — конечный модуль. Назовём *весом* слова $\mathbf{a} = (a_1, \ldots, a_n) \in M^n$ число

$$||\mathbf{a}|| = |\{i : 1 \leq i \leq n \ \&\ a_i \neq 0\}|.$$

Очевидны следующие соотношения:
1) $\forall \mathbf{a}, \mathbf{b} \in M^n : d(\mathbf{a}, \mathbf{b}) = ||\mathbf{a} - \mathbf{b}||$;
2) $\forall \mathcal{C} \leq M^n : d(\mathcal{C}) = \min\{||\mathbf{a}|| : \mathbf{a} \in \mathcal{C} \setminus \{0\}\}$.

2°. Граница Синглтона. МДР-коды, их свойства.

Теорема 1.13 (Граница Синглтона)**.** Если $\mathcal{C}$ есть $[n, k, d]$-код, то

$$d \leq n - k + 1. \tag{1.1}$$

◀ Пусть $m = |\mathcal{C}|$. Перенумеруем все слова кода $\mathcal{C}$: $\mathbf{a}_i = (a_{i1}, \ldots, a_{in})$, $1 \leq i \leq m$. Составим из них матрицу, в которой выделим первые $d-1$ столбцов:

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} = \left(\begin{array}{ccc|ccc} a_{11} & \ldots & a_{1,d-1} & a_{1d} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{m,d-1} & a_{md} & \ldots & a_{mn} \end{array}\right)$$

Поскольку $d(\mathcal{C}) = d$, то в выделенной группе последних $n - d + 1$ столбцов этой матрицы любые две строки различны. Следовательно, количество кодовых слов не превосходит количества различных строк длины $n - d + 1$ в алфавите Ω, т.е. $m \leq q^{n-d+1}$, где $q = |\Omega|$. Логарифмируя по основанию q, получаем требуемую оценку.►

Определение 1.14. Код $\mathcal{C}$ называется *кодом с максимально достижимым расстоянием*, или *МДР-кодом*, если $\mathcal{C}$ есть $[n, k, n - k + 1]$-код, т.е. неравенство (1.1) обращается в равенство.

Тривиальными примерами МДР-кодов являются:
— $[n, n, 1]$-код Ω^n;
— $[n, 1, n]$-код констант $\mathcal{C} = \{(a, \ldots, a) \in \Omega^n\}$;
— $[n, n-1, 2]$-код проверки на чётность.

Пример. Пусть $\mathbb{F}$ — конечное поле, $q = |\mathbb{F}|$, $M = \mathbb{F}[x|k] = \{f(x) \in \mathbb{F}[x] : \deg f(x) < k\}$, $x_1, \ldots, x_n$ — различные элементы поля $\mathbb{F}$, где $n \geq k$. $u_1, \ldots, u_n$ — обратимые элементы $\mathbb{F}$, отображение $\varphi : \mathbb{F}[x|k] \to \mathbb{F}^n$ задано правилом

$$\varphi(f(x)) = (u_1 f(x_1), \ldots, u_n f(x_n)).$$

Образ $\varphi(\mathbb{F}[x|k])$ называется *обобщённым* $[n, k]$-*кодом Рида–Соломона* над полем $\mathbb{F}$ и даёт менее тривиальный пример МДР-кода.

Предложение 1.15. Обобщённый $[n, k]$-код Рида–Соломона является МДР-кодом.

◄ Если $f(x) \in \mathbb{F}[x|k]$ и $f(x) \neq 0$, то по теореме Безу число корней многочлена $f(x)$ среди $x_1, \ldots, x_n$, равное $n - d(\varphi(f(x)), 0)$, удовлетворяет также неравенству $n - d(\varphi(f(x)), 0) \leq \deg(f(x)) < k$, откуда $d(\varphi(f(x)), 0) > n - k$. Во-первых, отсюда видно, что $\ker \varphi = 0$, поэтому $\dim\ \varphi(\mathbb{F}[x|k]) = \dim\ \mathbb{F}[x|k] = k$. Во-вторых, беря в качестве $f(x)$ разность любых различных многочленов из $\mathbb{F}[x|k]$, убеждаемся, что расстояние d данного кода также удовлетворяет неравенству $d > n - k$, что, в силу границы Синглтона, возможно лишь при $d = n - k + 1$. ►

3°. Граница Хэмминга (граница сферической упаковки). Совершенные коды. Двоичный код Хэмминга.

Теорема 1.16 (Граница Хэмминга, или граница сферической упаковки)**.** Пусть $\mathcal{C}$ есть $[n,k,d]_q$-код над алфавитом Ω и $d > 2r$. Тогда

$$q^k \le \frac{q^n}{s_q(n,r)}, \text{ где } s_q(n,r) = \sum_{i=0}^{r} (q-1)^i \binom{n}{i}. \tag{1.2}$$

◀ Нетрудно видеть, что i-е слагаемое в $s_q(n,r)$ — число точек пространства Ω^n, лежащих на расстоянии i от произвольной фиксированной точки $\mathbf{a}$ этого пространства, поэтому $s_q(n,r) = |O_r(\mathbf{a})|$, где

$$O_r(\mathbf{a}) = \{\mathbf{b} \in \Omega^n : d(\mathbf{a},\mathbf{b}) \le r\}.$$

В силу неравенства треугольника $O_r(\mathbf{a}) \cap O_r(\mathbf{a}') = \varnothing$ при $\mathbf{a}, \mathbf{a}' \in \mathcal{C}$ и $\mathbf{a} \ne \mathbf{a}'$, следовательно,

$$q^k s_q(n,r) = |\mathcal{C}| s_q(n,r) = \left| \bigcup_{\mathbf{a}\in\mathcal{C}} O_r(\mathbf{a}) \right| \le |\Omega^n| = q^n.$$

▶

Определение 1.17. Код $\mathcal{C}$ называется *совершенным*, если неравенство в (1.2) обращается в равенство (при этом обязательно $d = 2r+1$).

Пример. Двоичный код Хэмминга $\mathcal{H}_2(l)$ длины $n = 2^l - 1$ — множество слов $a \in \mathbb{Z}_2^n$, удовлетворяющих условию $Ha^T = 0$, где H — матрица, столбцы которой — все ненулевые столбцы длины l над $\mathbb{Z}_2$.

Предложение 1.18. Двоичный код Хэмминга $\mathcal{H}_2(l)$ является линейным $[n, n-l, 3]_2$ совершенным кодом.

◀ Линейность очевидна по построению. Поскольку матрица H содержит все ненулевые столбцы высоты l, то $\mathrm{rk} H = l$, откуда $\dim \mathcal{H}_2(l) = n - l$.

Так как матрица H не содержит нулевого столбца и любые два её столбца различны, то никакое ненулевое слово веса ≤ 2 не удовлетворяет условию $Ha^T = 0$, значит, $d(\mathcal{H}_2(l)) \ge 3$. С другой стороны, матрица H содержит столбцы $\mathbf{e}_1^T$, $\mathbf{e}_2^T$, $\mathbf{e}_1^T + \mathbf{e}_2^T$ (здесь $\mathbf{e}_s^T = (0,\dots,0,1,0,\dots,0)^T$ — столбец с единицей на s-ом месте), поэтому код $\mathcal{H}_2(l)$ содержит слово веса 3 и $d(\mathcal{H}_2(l)) = 3$.

В равенстве (1.2) для $d = 3$ имеем $r = 1$, $k = n - l$, $s_2(n,1) = \sum\limits_{i=0}^{1} (2-1)^i \binom{n}{i} = 1 + n = 1 + (2^l - 1) = 2^l$, поэтому $2^{n-l} = \dfrac{2^n}{s_2(n,1)}$ и

код $\mathcal{H}_2(l)$ является совершенным. ►

4°. Граница Плоткина. Эквидистантные коды. Симплексный код.

Теорема 1.19 (Граница Плоткина)**.** Пусть $\mathcal{C}$ есть $[n,k,d]_q$-код. Тогда

$$d \le \frac{nq^{k-1}(q-1)}{q^k-1} = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n \tag{1.3}$$

◄ Пусть $\mathcal{C} \subseteq \Omega^n$, где $|\Omega| = \{\omega_1,\dots,\omega_q\}$, $M = |\mathcal{C}|$. Обозначим через π_i проекцию Ω^n на i-ю координату (т.е. $\pi_i((a_1,\dots,a_n)) = a_i$ при $i = 1,\dots,n$) и положим

$$m_{ij} = |\{\mathbf{a} \in \mathcal{C} : \pi_i(\mathbf{a}) = \omega_j\}| = \sum_{\mathbf{a}\in M} \delta_{\pi_i(a),\omega_j}.$$

По определению, для любой пары $\mathbf{a},\mathbf{b} \in \mathcal{C}$ при $\mathbf{a} \ne \mathbf{b}$ имеем $d \le d(\mathbf{a},\mathbf{b})$. Суммируя по всем парам, получим

$$M(M-1)d \le \sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}} d(\mathbf{a},\mathbf{b}). \tag{1.4}$$

С другой стороны, $d(\mathbf{a},\mathbf{b}) = \sum_{i=1}^n \big(1 - \delta_{\pi_i(\mathbf{a}),\pi_i(\mathbf{b})}\big)$. Таким образом, правую часть неравенства (1.4) можно переписать в виде

$$\sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}}\sum_{i=1}^n (1-\delta_{\pi_i(\mathbf{a}),\pi_i(\mathbf{b})}) = nM^2 - \sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}}\sum_{i=1}^n \delta_{\pi_i(\mathbf{a}),\pi_i(\mathbf{b})} =$$

$$= nM^2 - \sum_{i=1}^n \sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}} \sum_{\omega\in\Omega} \delta_{\pi_i(\mathbf{a}),\omega}\delta_{\pi_i(\mathbf{b}),\omega} = nM^2 - \sum_{i=1}^n\sum_{j=1}^q m_{ij}^2.$$

Теперь применим неравенство Коши–Буняковского к векторам $(1,1,\dots,1)$ и $(m_{i1},m_{i2},\dots,m_{iq})$:

$$\left(\sum_{j=1}^q m_{ij}\right)^2 \le q\sum_{j=1}^q m_{ij}^2.$$

При каждом $i = 1,\dots,n$, $\sum_{j=1}^q m_{ij} = M$, поэтому

$$M(M-1)d \le nM^2 - n/qM^2 = nM^2\frac{q-1}{q}.$$

►
Если неравенство (1.3) обращается в равенство, говорят, что код лежит на границе Плоткина. Как видно из доказательства теоремы 1.19, необходимым (но не достаточным!) условием этого является эквидистантность кода в смысле следующего определения.

Определение 1.20. Код $\mathcal{C}$ называется *эквидистантным*, если все расстояния между различными словами кода $\mathcal{C}$ одинаковы.

Очевидным примером эквидистантного кода является уже упомянутый код констант. Более сложно устроен следующий

Пример. Пусть $\mathbb{F}$ — конечное поле, $|\mathbb{F}| = q$, V — линейное пространство над $\mathbb{F}$, $k = \dim_{\mathbb{F}} V$. Положим $n = q^k - 1$ и как-нибудь занумеруем ненулевые векторы пространства V:

$$V \setminus \{0\} = \{v_1, \ldots, v_n\}.$$

Рассмотрим далее сопряжённое пространство V^*, состоящее из линейных функций $V \to \mathbb{F}$ и составим код

$$\mathcal{C} = S_P(k) = \{(f(v_1), \ldots, f(v_n)) : f \in V^*\}.$$

Ясно, что $|\mathcal{C}| = |V^*| = |V| = q^k$, а $d(\mathcal{C}) = n - (q^{k-1} - 1) = q^k - q^{k-1}$, так как ядро любой ненулевой линейной функции — подпространство размерности $k-1$ пространства V. Таким образом, вычисляя правую часть (1.3), имеем

$$\frac{nq^{k-1}(q-1)}{q^k - 1} = q^{k-1}(q-1) = d(\mathcal{C}).$$

Лекция 2. Изометрические преобразования пространства Хэмминга. Теорема А.А. Маркова.

1°. Общий случай.

Определение 2.1. Пусть Ω — алфавит, $n \in \mathbb{N}$. Биективное отображение $\varphi : \Omega^n \to \Omega^n$ называется *изометрией*, если

$$d(\varphi(\mathbf{a}), \varphi(\mathbf{b})) = d(\mathbf{a}, \mathbf{b})$$

для любых слов $\mathbf{a}, \mathbf{b} \in \Omega^n$ (иначе говоря, если φ сохраняет расстояние Хэмминга).

Определение 2.2. Если $\Omega = M$ — модуль над кольцом $\mathcal{R}$, то изометрия $\varphi : \Omega^n \to \Omega^n$ называется *линейной изометрией*, если $\varphi : \Omega^n \to \Omega^n$ — гомоморфизм $\mathcal{R}$-модулей.

Заметим, что изометрии $\mathfrak{S}(\Omega^n)$ составляют подгруппу группы S_{Ω^n} всех биективных преобразований множества Ω^n в себя.

Изометрии пространства Хэмминга устроены очень просто, как показывает следующая

Теорема 2.3 (А.А. Марков, 1956 г.)**.** Биекция $\varphi : \Omega^n \to \Omega^n$ является изометрией тогда и только тогда, когда φ задаётся следующим правилом:

$$\forall \mathbf{a} = (a_1, \ldots, a_n) \in \Omega^n, \quad \varphi(\mathbf{a}) = (\pi_1(a_{\sigma(1)}), \ldots, \pi_n(a_{\sigma(n)})), \qquad (2.1)$$

где $\sigma \in S_n$, $\pi_i \in S_\Omega$, $i = 1, \ldots, n$, а S_Ω обозначает группу всех биективных отображений множества Ω в себя.

◀ Преобразования, заданные правилом (2.1), называются *мономиальными*. Очевидно, что мономиальное преобразование является изометрией.

1. Отметим, что мономиальные преобразования $\mathcal{M}(\Omega^n)$ образуют подгруппу группы $\mathfrak{S}(\Omega^n)$. Действительно, очевидно, что тождественное отображение мономиально. Если $\phi, \psi \in \mathcal{M}(\Omega^n)$ и $\phi(\mathbf{a}) = (\pi_1(a_{\sigma(1)}), \ldots, \pi_n(a_{\sigma(n)}))$, $\psi(\mathbf{a}) = (\rho_1(a_{\tau(1)}), \ldots, \rho_n(a_{\tau(n)}))$, то

$$\psi\phi(\mathbf{a}) = \psi(\pi_1(a_{\sigma(1)}), \ldots, \pi_n(a_{\sigma(n)})) = \\ = (\rho_1(\pi_{\tau(1)}(a_{\sigma\tau(1)})), \ldots, \rho_n(\pi_{\tau(n)}(a_{\sigma\tau(n)}))),$$

также является мономиальным преобразованием. Отсюда также следует мономиальность обратного к мономиальному отображению: $\phi^{-1}(\mathbf{a}) = (\pi^{-1}_{\sigma^{-1}(1)}(a_{\sigma^{-1}(1)}), \ldots, \pi^{-1}_{\sigma^{-1}(n)}(a_{\sigma^{-1}(n)}))$.

2. Пусть $\varphi \in \mathfrak{S}(\Omega^n)$ — произвольная изометрия. В силу сказанного выше для того, чтобы доказать мономиальность φ, достаточно доказать мономиальность преобразования вида $\eta_1\varphi\eta_2$, где $\eta_1, \eta_2 \in \mathcal{M}(\Omega^n)$. Это позволит нам далее, не ограничивая общности считать, что φ обладает каким-то требуемым свойством, добившись того, чтобы $\eta_1\varphi\eta_2$ им обладало.

3. Переобозначив буквы алфавита, будем считать, что $\Omega = \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. Положим $\mathbf{0} = (0, \ldots, 0)$.

Можно считать, что $\varphi(\mathbf{0}) = \mathbf{0}$. Действительно, если $\varphi(\mathbf{0}) = (c_1, \ldots, c_n)$ для тех $i = 1, \ldots, n$, что $c_i \neq 0$ возьмём в качестве $\nu_i \in S_\Omega$ транспозицию $(0, c_i)$, для оставшихся i положим $\nu_i = id$. Взяв мономиальное преобразование η_1, соответствующие подстановкам $\nu_i \in S_\Omega$ и тождественной $\sigma \in S_n$, получаем, что $\eta_1\varphi(\mathbf{0}) = \mathbf{0}$.

4. Как и в линейном случае, обозначим за $||\mathbf{a}||$ число ненулевых координат слова $\mathbf{a} \in \Omega^n$. Имеем

$$||\varphi(\mathbf{a})|| = d(\varphi(\mathbf{a}), \mathbf{0}) = d(\varphi(\mathbf{a}), \varphi(\mathbf{0})) = d(\mathbf{a}, \mathbf{0}) = ||\mathbf{a}||.$$

5. В частности, для $\mathbf{e}_s = (0, \ldots, 0, 1, 0, \ldots, 0)$ с единицей на s-ом месте, $s = 1, \ldots, n$, из $||\mathbf{e}_s|| = 1$ получаем, что $||\varphi(\mathbf{e}_s)|| = 1$, откуда

$$\varphi(\mathbf{e}_s) = u_s\mathbf{e}_{\omega(s)},$$

где $u\mathbf{e}_i$ обозначает слово с u на i-ом месте и нулями на остальных, $u_s \in \Omega \setminus \{0\}$, $\omega : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Покажем, что $\omega \in S_n$. Пусть $p, q \in \{1, \ldots, n\}, p \neq q$. Тогда $d(\mathbf{e}_p, \mathbf{e}_q) = 2$, откуда $d(u_p\mathbf{e}_{\omega(p)}, u_q\mathbf{e}_{\omega(q)}) = 2$. Следовательно, $\omega(p) \neq \omega(q)$, т.е. ω — инъективное отображение, поэтому $\omega \in S_n$. Для $u_s \neq 1$ взяв транспозиции $\tau_s = (1, u_s) \in S_\Omega$, для оставшихся s положив $\tau_s = id$ и определяя мономиальное преобразование η_2, соответствующее подстановкам $\tau_s \in S_\Omega$ и тождественной $\sigma \in S_n$, и домножив φ на η_2, получаем, что

$$\varphi(\mathbf{e}_s) = \mathbf{e}_{\omega(s)},\ \omega \in S_n.$$

6. Для любого $s \in \{1, \ldots, n\}$ и любого $u \in \Omega \setminus \{0\}$ имеем

$$||\varphi(u\mathbf{e}_s)|| = ||u\mathbf{e}_s|| = 1,$$

$$d(\varphi(u\mathbf{e}_s), \mathbf{e}_{\omega(s)}) = d(u\mathbf{e}_s, \mathbf{e}_s) = 1.$$

Отсюда получаем, что

$$\varphi(u\mathbf{e}_s) = \pi_s(u)\mathbf{e}_{\omega(s)},\ \pi_s : \Omega \to \Omega, \pi_s(0) = 0, \pi_s(1) = 1.$$

При этом $\pi_s \in S_\Omega$ для каждого $s \in \{1, \ldots, n\}$. Действительно, если $u, v \in \Omega, u \neq v$, то

$$d(u\mathbf{e}_s, v\mathbf{e}_s) = 1 = d(\varphi(u\mathbf{e}_s), \varphi(v\mathbf{e}_s)) = d(\pi_s(u)\mathbf{e}_{\omega(s)}, \pi_s(v)\mathbf{e}_{\omega(s)}),$$

значит, $\pi_s(u) \neq \pi_s(v)$, т.е. π_s — инъективное отображение, поэтому $\pi_s \in S_\Omega$.

Взяв мономиальное отображение η_3, с подстановками, обратными к $\pi_{\omega^{-1}(1)}, \ldots, \pi_{\omega^{-1}(n)}$ и ω, и умножив его на φ, будем считать, что

$$\varphi(u\mathbf{e}_s) = u\mathbf{e}_s,\ \forall u \in \Omega,\ s \in \{1, \ldots, n\}.$$

7. Докажем, что $\varphi = id$ — тождественное преобразование на Ω^n. Предположим противное: пусть $\varphi(\mathbf{a}) = \mathbf{b}$, $\mathbf{b} \neq \mathbf{a}$ для некоторых $\mathbf{a}, \mathbf{b} \in \Omega^n$. При этом по доказанному в пункте 4, $||\mathbf{b}|| = ||\mathbf{a}||$. По построению $a_i \neq b_i$ для некоторого $i \in \{1, \ldots, n\}$. Имеем две возможности.

Случай $a_i = 0$. Тогда $b_i \neq 0$, откуда

$$d(\mathbf{a}, b_i\mathbf{e}_i) = ||a|| + 1 = ||b|| + 1,$$

с другой стороны,

$$d(\varphi(\mathbf{a}), \varphi(b_i\mathbf{e}_i)) = d(\mathbf{b}, b_i\mathbf{e}_i) = ||b|| - 1.$$

Противоречие с тем, что φ — изометрия.

Случай $a_i \neq 0$. Тогда

$$d(\mathbf{a}, a_i\mathbf{e}_i) = ||a|| - 1 = ||b|| - 1,$$

с другой стороны,

$$d(\varphi(\mathbf{a}), \varphi(a_i\mathbf{e}_i)) = d(\mathbf{b}, a_i\mathbf{e}_i) \geq ||b||.$$

Противоречие с тем, что φ — изометрия.

Полученные противоречия доказывают, что $\varphi = id$, поэтому мономиально.▶

2°. Линейный случай. Пусть $\Omega = M$ — модуль над кольцом $\mathcal{R}$. Линейное мономиальное преобразование — преобразование вида (2.1), для которого $\pi_s \in \mathrm{Aut}(M),\ s \in \{1, \ldots, n\}$.

Докажем линейную версию теоремы А.А.Маркова.

Теорема 2.4 (А.А.Марков)**.** Биекция $\varphi : M^n \to M^n$, где M — модуль над кольцом $\mathcal{R}$, является линейной изометрией тогда и только тогда, когда она является линейным мономиальным преобразованием.

◀ Пусть φ — линейное мономиальное преобразование вида (2.1). Тогда

$$\varphi(\mathbf{a}+\mathbf{b}) = (\pi_1(a_{\sigma(1)}+b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)}+b_{\sigma(n)})) = \\ = (\pi_1(a_{\sigma(1)})+\pi_1(b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)})+\pi_n(b_{\sigma(n)})) = \varphi(\mathbf{a})+\varphi(\mathbf{b})$$

$$\varphi(\mathbf{a}r) = (\pi_1(a_{\sigma(1)}r),\dots,\pi_n(a_{\sigma(n)}r) = \\ = (\pi_1(a_{\sigma(1)})r,\dots,\pi_n(a_{\sigma(n)})r) = \varphi(\mathbf{a})r$$

для любых $r \in \mathcal{R}, \mathbf{a}, \mathbf{b} \in M^n$. Следовательно, φ является линейной изометрией.

Обратно, пусть φ — линейная изометрия. По теореме 2.3 φ является мономиальным преобразованием.

По линейности φ для любых $r \in \mathcal{R}, \mathbf{a}, \mathbf{b} \in M^n$ имеем

$$(\pi_1(a_{\sigma(1)}+b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)}+b_{\sigma(n)})) = \varphi(\mathbf{a}+\mathbf{b}) = \\ = \varphi(\mathbf{a})+\varphi(\mathbf{b}) = (\pi_1(a_{\sigma(1)})+\pi_1(b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)})+\pi_n(b_{\sigma(n)}))$$

откуда получаем, что $\pi_i(a+b) = \pi_i(a)+\pi_i(b)$ для любых $a, b \in M$ и $i \in \{1,\dots,n\}$.

Аналогично,

$$(\pi_1(a_{\sigma(1)}r),\dots,\pi_n(a_{\sigma(n)}r)) = \varphi(\mathbf{a}r) = \\ = \varphi(\mathbf{a})r = (\pi_1(a_{\sigma(1)})r,\dots,\pi_n(a_{\sigma(n)})r),$$

откуда получаем, что $\pi_i(ar) = \pi_i(a)r$ для любых $a \in M$, $r \in \mathcal{R}$ и $i \in \{1,\dots,n\}$.

Следовательно, $\pi_i \in \mathrm{Aut}(M)$ для всех $i \in \{1,\dots,n\}$, поэтому φ является линейным мономиальным преобразованием. ▶

Рассмотрим важный частный случай, когда $M = \mathcal{R}$, т.е. линейные коды над кольцом $\mathcal{R}$. Любой эндоморфизм π (гомоморфизм в себя) кольца $\mathcal{R}$ определяется элементом $\pi(1)$, поскольку $\pi(r) = \pi(1)r$. При этом $\pi \in \mathrm{Aut}(\mathcal{R}_{\mathcal{R}})$ тогда и только тогда, когда $\pi(1) \in \mathcal{R}^*$ — обратимый элемент кольца $\mathcal{R}$.

Следовательно, для любой линейной изометрии φ модуля $\mathcal{R}^n$ существуют элементы $u_1, \ldots, u_n \in \mathcal{R}^*$ и $\sigma \in S_n$ такие, что φ задается правилом

$$\forall \mathbf{a} \in \mathcal{R}^n : \ \varphi(\mathbf{a}) = (u_1 a_{\sigma(1)}, \ldots, u_n a_{\sigma(n)}).$$

Определение 2.5. Два (линейных) кода $\mathcal{C}_1$ и $\mathcal{C}_2$ длины n над алфавитом Ω называются (*линейно*) *эквивалентными*, если существует (линейная) изометрия $\varphi : \Omega^n \to \Omega^n$, такая, что $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

Сразу заметим, что все параметры эквивалентных кодов одинаковы.

Определение 2.6. Подгруппа $\mathrm{Aut}(\mathcal{C}) = \{\sigma \in \mathfrak{S}(\Omega^n) : \sigma(\mathcal{C}) = \mathcal{C}\}$ называется *группой автоморфизмов* кода $\mathcal{C}$.

Определение 2.7. Подгруппа $\mathcal{L}\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}) \cap \mathrm{Aut}(M^n)$ называется *группой линейных автоморфизмов* линейного кода $\mathcal{C}$.

Используя теорему Лагранжа и связь орбит и стабилизаторов действия, можно получить

Теорема 2.8. Число кодов $\mathcal{C}' \in \Omega^n$, эквивалентных коду $\mathcal{C} \in \Omega^n$ равно индексу $[\mathfrak{S}(\Omega^n) : \mathrm{Aut}(\mathcal{C})]$ подгруппы $\mathrm{Aut}(\mathcal{C})$ в группе $\mathfrak{S}(\Omega^n)$. Если $\mathcal{C}' = \sigma(\mathcal{C})$, $\sigma \in \mathfrak{S}(\Omega^n)$, то $\mathrm{Aut}(\mathcal{C}') = \sigma^{-1}\mathrm{Aut}(\mathcal{C})\sigma$.

Лекция 3. Реальная длина кода. Теорема Мак-Вилльямс о продолжении изометрий линейных кодов.

Определение 3.1. Пусть $\mathbb{F}$ — произвольное конечное поле. Линейные коды $\mathcal{C}, \mathcal{L} \leqslant {}_{\mathbb{F}}\mathbb{F}^n$ *линейно изометричны*, если существует изоморфизм линейных пространств

$$\tau : {}_{\mathbb{F}}\mathcal{C} \to {}_{\mathbb{F}}\mathcal{L} \tag{3.1}$$

такой, что

$$d(\mathbf{a}, \mathbf{b}) = d(\tau(\mathbf{a}), \tau(\mathbf{b})) \ \forall \ \mathbf{a}, \mathbf{b} \in \mathcal{C}. \tag{3.2}$$

Определение 3.2. *Реальной длиной кода* $\mathcal{C}$ называется число

$$l(\mathcal{C}) = |\{i \in \{1, \ldots, n\} : \ \exists \mathbf{a} = (a_1, \ldots, a_n) \in \mathcal{C} \ a_i \neq 0\}|.$$

Сначала докажем вспомогательную лемму.

Код $\mathcal{C}$ в этом случае можно рассматривать как код длины $l(\mathcal{C})$, при этом $l(\mathcal{C})$ минимальное такое число.

Реальная длина кода также связана и с другими кодовыми параметрами. Докажем два утверждения о её связи с весами кодовых слов в линейном случае.

Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный код над полем $\mathbb{F}$.

Очевидно, что $d(\mathcal{C}) \leq ||\mathbf{a}|| \leq l(\mathcal{C})$ для любого слова $\mathbf{a} \in \mathcal{C} \setminus \{0\}$, т.е. минимальное кодовое расстояние и реальная длина кода служат границами весов кодовых слов. По определению минимального расстояния слово веса $d(\mathcal{C})$ в коде $\mathcal{C}$ всегда содержится. Следующее предложение показывает, когда в коде $\mathcal{C}$ есть слово веса $l(\mathcal{C})$.

Предложение 3.3. Пусть $\mathbb{F}$ — конечное поле мощности q. Тогда
1.любой линейный код $\mathcal{C} \leq \mathbb{F}^n$, имеющий реальную длину $l(\mathcal{C}) \leq q$, содержит слово веса $l(\mathcal{C})$;
2. для любого такого l, что $n \geq l > q$, среди кодов длины n и реальной длины l существуют коды, не содержащие слов веса l.

◀ Положим $l = l(\mathcal{C})$. Для простоты обозначений пусть ненулевые координаты слов из $\mathcal{C}$ расположены в позициях $1, \ldots, l$.

1. Пусть $l \leq q$. Обозначим $\mathbf{a}(i) = (a(i)_1, \ldots, a(i)_n) \in \mathcal{C}$, так что $a(i)_i \neq 0$, $i = 1, \ldots, l$.

Доказательство проведем индукцией по l.

База индукции. При $l \leq 1$ утверждение верно.

Шаг индукции. Допустим, что $l > 1$ и для $l-1$ утверждение доказано.

Это означает, что существует слово $\mathbf{a} \in \langle \mathbf{a}(i) |\ i = 1, \ldots, l-1 \rangle$ такое, что $a_k \neq 0,\ k = 1, \ldots, l-1$. Действительно, предположение индукции применимо к коду $\mathcal{C}' = \langle \tilde{\mathbf{a}}(i) |\ i = 1, \ldots, l-1 \rangle$, где $\tilde{a}(i)_m = a(i)_m$, при $m \neq l$, и $\tilde{a}(i)_l = 0$. При этом в $\mathcal{C}'$ слово $\tilde{\mathbf{a}}$ веса $l-1$ выражается как линейная комбинация $\tilde{\mathbf{a}} = \sum\limits_{j=1}^{l-1} \alpha_j \tilde{\mathbf{a}}(j)$. Тогда можно взять $\mathbf{a} = \sum\limits_{j=1}^{l-1} \alpha_j \mathbf{a}(j)$ и $a_k = \tilde{a}_k \neq 0$ при $k = 1, \ldots, l-1$.

Добавляем к рассмотрению слово $\mathbf{b} = \mathbf{a}(l)$.

Если $a_l \neq 0$, то $||\mathbf{a}|| = l$ и это требуемое слово; если $b_i \neq 0$ для всех $i = 1, \ldots, l$, то $||\mathbf{b}|| = l$ и это требуемое слово. В противном случае рассмотрим слова $\mathbf{a} + \alpha\mathbf{b},\ \alpha \in \mathbb{F},\ \alpha \neq 0$. Пусть $y_i(x) = b_i x + a_i,\ i = 1, \ldots, l-1$. При каждом i по построению $a_i \neq 0$, значит уравнение $y_i(x) = 0$ имеет в $\mathbb{F}$ не более одного решения. При этом слово $\mathbf{b}$ имеет нулевую координату в позициях $[1, l]$, значит по крайней мере одно из уравнений $y_i(x) = 0$ несовместно. Следовательно, если $X = \{x \in \mathbb{F} |\ \exists i \in \{1, \ldots, l-1\}\ y_i(x) = 0\}$, то $|X| \leq l-2$. Из условия на число элементов поля следует, что найдётся $\alpha \in \mathbb{F},\ \alpha \neq 0$, что $\alpha \notin X$, т.е. $a_i + \alpha b_i \neq 0,\ i = 1, \ldots, l$. Слово $\mathbf{a} + \alpha\mathbf{b} \in \langle \mathbf{a}(i) |\ i = 1, \ldots, l \rangle$ и есть искомое.

2. Пусть $n \geq l > q$. Рассмотрим $\mathcal{C} = \langle \mathbf{a}, \mathbf{b} \rangle \leq \mathbb{F}^n$, где $a_2 = \ldots = a_l = 1$, $a_1 = a_{l+1} = \ldots = a_n = 0$, $b_1 = 1$, $b_2 = b_{q+2} = \ldots = b_n = 0$, $b_3, \ldots, b_{q+1}$ — все различные ненулевые элементы поля $\mathbb{F}$. Тогда для любого $\alpha \in \mathbb{F}^*$ имеем номер $t = 3, \ldots, q+1$, что $\alpha = -b_t$. Поэтому в слове $\mathbf{b} + \alpha\mathbf{a}$ на месте t стоит 0 и значит, его вес меньше l. Все слова в коде $\mathcal{C}$ кратны $\mathbf{a}, \mathbf{b}$, либо $\mathbf{b} + \alpha\mathbf{a}$, поэтому содержат 0 на позициях $[1, l]$. Таким образом, в коде $\mathcal{C}$ реальной длины l нет слов веса l. ►

Для доказательствва теоремы Мак-Вилльямс сначала докажем вспомогательную лемму.

Лемма 3.4. Пусть $\mathbb{F}$ — конечное поле мощности q. Тогда для любого линейного кода $\mathcal{C} \leq \mathbb{F}^n$ справедливо равенство

$$\sum_{\mathbf{a} \in \mathcal{C}} ||\mathbf{a}|| = \frac{q-1}{q} |\mathcal{C}| l(\mathcal{C}).$$

◄ Для каждого $i \in \{1, \ldots, n\}$ рассмотрим проекцию

$$\pi_i : \mathbb{F}^n \to \mathbb{F},\ \pi_i(\mathbf{a}) = a_i.$$

Поскольку π_i — гомоморфизм пространств, то $\pi_i(\mathcal{C})$ является подпространством $\mathbb{F}$, соответственно, $\pi_i(\mathcal{C}) \in \{0, \mathbb{F}\}$ и

$$l(\mathcal{C}) = |\{i \in \{1, \ldots, n\} : \ \pi_i(\mathcal{C}) = \mathbb{F}\}|.$$

Кроме того, если рассмотреть ядро ограничения гомоморфизма π_i на пространство $\mathcal{C}$: $\mathcal{K}_i = \mathrm{Ker}(\pi_i|_{\mathcal{C}})$, то по теореме о гомоморфизме

$$|\mathcal{K}_i| = \frac{|\mathcal{C}|}{|\pi_i(\mathcal{C})|} = \begin{cases} \frac{|\mathcal{C}|}{q}, \text{ если } \pi_i(\mathcal{C}) = \mathbb{F}, \\ |\mathcal{C}| \text{ если } \pi_i(\mathcal{C}) = 0. \end{cases}$$

Справедливы равенства

$$\sum_{\mathbf{a} \in \mathcal{C}} ||\mathbf{a}|| = \sum_{\mathbf{a} \in \mathcal{C}} \sum_{i=1}^{n} ||a_i|| = \sum_{i=1}^{n} \sum_{\mathbf{a} \in \mathcal{C}} ||a_i||.$$

При условии $\pi_i(\mathcal{C}) = \mathbb{F}$ прообраз в $\mathcal{C}$ каждого элемента $a \in \mathbb{F}$ при гомоморфизме $\pi_i|_{\mathcal{C}}$ имеет мощность $|\mathcal{K}_i|$, поэтому

$$\sum_{\mathbf{a} \in \mathcal{C}} ||a_i|| = \sum_{\mathbf{a} \in \mathcal{C}} ||\pi_i(\mathbf{a})|| = |\mathcal{K}_i| \sum_{a \in \mathbb{F}} ||a|| = |\mathcal{K}_i|(q-1) = \frac{q-1}{q}|\mathcal{C}|.$$

При условии $\pi_i(\mathcal{C}) = 0$ имеем $\sum\limits_{\mathbf{a} \in \mathcal{C}} ||a_i|| = 0$.

В итоге,

$$\sum_{i=1}^{n} \sum_{\mathbf{a} \in \mathcal{C}} ||a_i|| = \frac{q-1}{q}|\mathcal{C}|l(\mathcal{C}).$$

►

Следствие 3.5. Пусть $\mathbb{F}$ — конечное поле. Если эквидистантный линейный код $\mathcal{C} \leq \mathbb{F}^n$ лежит на границе Плоткина, то $l(\mathcal{C}) = n$.

◄ Вспомним, что код лежит на границе Плоткина, если $d = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n$.

Для экиквидистантного линейного кода имеем $||\mathbf{a}|| = d$ для любого $\mathbf{a} \in \mathcal{C} \setminus \{0\}$, откуда по лемме о сумме весов получаем $\sum\limits_{\mathbf{a} \in \mathcal{C}} ||\mathbf{a}|| = (|\mathcal{C}| - 1)d = \frac{q-1}{q}|\mathcal{C}|l(\mathcal{C})$ и $d = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}l(\mathcal{C})$.

Приравнивая эти два выражения для d получаем требуемое равенство $l(\mathcal{C}) = n$.►

Перейдём к основной теореме данной лекции.

Теорема 3.6 (Теорема Мак-Вилльямс, 1962)**.** Пусть $\mathbb{F}$ — произвольное конечное поле. Тогда любая линейная изометрия (3.1) линейных кодов над $\mathbb{F}$ продолжается до линейного над $\mathbb{F}$ мономиального преобразования (2.1).

◀ Как было показано в теореме 2.3, мономиальные преобразования $\mathcal{M}(\mathbb{F}^n)$ образуют группу. Поэтому для доказательства существования продолжения τ, достаточно доказать результат для произведения τ и некоторых мономиальных преобразований.

Проведём доказательство индукцией по $l(\mathcal{C}) \geq 0$.

База индукции. Если $l(\mathcal{C}) = 0$, то $\mathcal{C} = 0$. В этом случае утверждение очевидно: в качестве продолжения τ можно взять произвольное мономиальное преобразование из $\mathcal{M}(\mathbb{F}^n)$.

Шаг индукции. Пусть теорема верна для всех кодов $\mathcal{C}, \mathcal{L} \leq \mathbb{F}^n$ произвольной длины $n \in \mathbb{N}$ таких, что $0 \leq l(\mathcal{C}) < l$ для некоторого $l \in \mathbb{N}$. Докажем её для $l(\mathcal{C}) = l$. Ввиду линейности отображения τ на пространстве $\mathcal{C}$ условие (3.2) эквивалентно

$$||\tau(\mathbf{a})|| = ||\mathbf{a}|| \ \forall \mathbf{a} \in \mathcal{C}.$$

По лемме 3.4 отсюда следует, что $l(\mathcal{L}) = l(\mathcal{C})$.

Поскольку $l(\mathcal{C}) = l > 0$, то $\pi_i(\mathcal{C}) = \mathbb{F}$ для некоторого $i \in \{1, \ldots, n\}$. Умножив при необходимости τ справа на мономиальное преобразование, меняющее местами i-ую и первую координаты, без ограничения общности можем считать, что $i = 1$. Тогда код $\mathcal{C}$ содержит слово $\mathbf{a}_1 = (1, *, \ldots, *)$. Вспомним, что для $\mathcal{K}_1 = \mathrm{Ker}(\pi_1|_{\mathcal{C}})$ справедливо $\dim \mathcal{K}_1 = \dim \mathcal{C} - 1$, $|\mathcal{K}_1| = \frac{|\mathcal{C}|}{q}$, $q = |\mathbb{F}|$. Более того,

$$\mathcal{C} = \mathbb{F}\mathbf{a}_1 \oplus \mathcal{K}_1,$$

т.к. $\mathbf{a}_1 \notin \mathcal{K}_1$ по построению. Поскольку по определению первые координаты всех слов в $\mathcal{K}_1$ равны нулю и $\mathcal{K}_1 \subset \mathcal{C}$, то

$$l(\mathcal{K}_1) \leq l - 1 < l.$$

Рассмотрим линейный код $\tau(\mathcal{K}_1) \subset \tau(\mathcal{C}) = \mathcal{L}$. По лемме 3.4 отсюда следует, что $l(\tau(\mathcal{K}_1)) = l(\mathcal{K}_1) < l$. Следовательно, существует индекс $j \in \{1, \ldots, n\}$ такой, что $\pi_j(\mathcal{L}) = \mathbb{F}$, но $\pi_j(\tau(\mathcal{K}_1)) = 0$. Умножив при необходимости τ слева на мономиальное преобразование, меняющее местами j-ую и первую координаты, без ограничения общности можем считать, что $j = 1$. Рассмотрим подпространство $\mathcal{L}_1 = \mathrm{Ker}(\pi_1) \cap \mathcal{L}$. Имеем $\tau(\mathcal{K}_1) \subseteq \mathcal{L}_1$. Поскольку $\pi_1(\mathcal{L}) = \mathbb{F}$, то $|\mathcal{L}_1| = \frac{|\mathcal{L}|}{q} = \frac{|\mathcal{C}|}{q} = |\mathcal{K}_1|$. Следовательно, $\tau(\mathcal{K}_1) = \mathcal{L}_1$.

Поскольку τ — биекция из $\mathcal{C}$ в $\mathcal{L}$, $\tau(\mathcal{K}_1) = \mathcal{L}_1$ и $\mathbf{a}_1 \notin \mathcal{K}_1$, то $\tau(\mathbf{a}_1) \notin \mathcal{L}_1$. Значит, $\tau(\mathbf{a}_1) = \mathbf{b}_1 = (\beta, *, \ldots, *)$, $\beta \in \mathbb{F}^*$. Откуда имеем разложение

$$\mathcal{L} = \mathbb{F}\mathbf{b}_1 \oplus \mathcal{L}_1.$$

Для произвольного числа $c \in \mathbb{F}$ из линейности τ следует, что

$$\tau(c\mathbf{a}_1) = c\tau(\mathbf{a}_1) = c\mathbf{b}_1 = (c\beta, *, \ldots, *).$$

Тогда для произвольного слова $\mathbf{a} \in \mathcal{C}$ получаем

$$\mathbf{a} = a_1\mathbf{a}_1 + (0, a'_2, \ldots, a'_n),\ \tau(\mathbf{a}) = a_1\tau(\mathbf{a}_1) + \tau((0, a'_2, \ldots, a'_n)),$$

причём $\tau((0, a'_2, \ldots, a'_n)) \in \mathcal{L}_1$, откуда

$$\tau(\mathbf{a}) = (a_1\beta, \tau_2(\mathbf{a}), \ldots, \tau_n(\mathbf{a})),$$

где $\tau_i : \mathcal{C} \to \mathbb{F}$, $i \in \{2, \ldots, n\}$ — линейные функции.

Покажем, что линейные функции $\tau_2, \ldots, \tau_n$ не зависят от первой координаты вектора $\mathbf{a} \in \mathcal{C}$, т.е. для любых $\mathbf{a}, \mathbf{b} \in \mathcal{C}$, если $a_2 = b_2, \ldots, a_n = b_n$, то $\tau_i(\mathbf{a}) = \tau_i(\mathbf{b})$, $i \in \{2, \ldots, n\}$. Если $a_1 \neq b_1$, то $||\mathbf{a}-\mathbf{b}|| = 1$. Поскольку τ — линейная изометрия, то $||\tau(\mathbf{a})-\tau(\mathbf{b})|| = 1$. При этом $(\tau(\mathbf{a}))_1 = a_1\beta \neq b_1\beta = (\tau(\mathbf{b}))_1$, следовательно, все остальные координаты этих векторов обязательно равны.

Введём обозначения

$$\mathcal{C}' = \left\{(a_2, \ldots, a_n) \in \mathbb{F}^{n-1} :\ \exists a_1 \in \mathbb{F}(a_1, a_2, \ldots, a_n) \in \mathcal{C}\right\},$$

$$\mathcal{L}' = \left\{(b_2, \ldots, b_n) \in \mathbb{F}^{n-1} :\ \exists b_1 \in \mathbb{F}(b_1, b_2, \ldots, b_n) \in \mathcal{L}\right\},$$

и зададим отображение $\tau' : \mathcal{C}' \to \mathbb{F}^{n-1}$ условием

$$\tau'((a_2, \ldots, a_n)) = (\tau_2(\mathbf{a}), \ldots, \tau_n(\mathbf{a}))\ \forall (a_2, \ldots, a_n),$$

где $a_1 \in \mathbb{F}$ произвольная константа, для которой $(a_1, a_2, \ldots, a_n) \in \mathcal{C}$. По доказанному выше отображение τ' определено корректно (не зависит от выбора a_1). Поскольку $\tau : \mathcal{C} \to \mathcal{L}$ — биекция, то из равенства $\tau(\mathbf{a}) = (a_1\beta, \tau_2(\mathbf{a}), \ldots, \tau_n(\mathbf{a}))$ заключаем, что $\tau'(\mathcal{C}') = \mathcal{L}'$, т.е. τ' — изоморфизм линейных пространств $\mathcal{C}'$ и $\mathcal{L}'$. Поскольку

$$\forall \mathbf{a} \in \mathcal{C} :\ ||\tau(\mathbf{a})|| = ||\mathbf{a}|| = ||a_1|| + ||(a_2, \ldots, a_n)||$$

и

$$||\tau(\mathbf{a})|| = ||a_1\beta|| + ||\tau'(a_2, \ldots, a_n)||,$$

то

$$\forall \mathbf{a}' \in \mathcal{C}' : \ ||\tau'(\mathbf{a}')|| = ||\mathbf{a}'||.$$

Таким образом, $\tau' : \mathcal{C}' \to \mathcal{L}'$ — линейная изометрия. Из определения пространства $\mathcal{C}'$ также следует, что $l(\mathcal{C}') = l - 1 < l$. Соответственно, можно применить предположение индукции: линейная изометрия τ' продолжается до линейного мономиального преобразования $\sigma' : \mathbb{F}^{n-1} \to \mathbb{F}^{n-1}$, с подстановкой $\rho' \in S_{n-1}$ на множестве $\{2, \ldots, n\}$ и обратимыми константами $u_2, \ldots, u_n \in \mathbb{F}^*$. Тогда продолжением τ будет мономиальное преобразование $\sigma : \mathbb{F}^n \to \mathbb{F}^n$, с подстановкой $\rho \in S_n$, $\rho(1) = 1$, $\rho(j) = \rho'(j)$, $j \in \{2, \ldots, n\}$, и обратимыми константами $\beta, u_2, \ldots, u_n \in \mathbb{F}^*$.▶

Лекция 4. Проверочная и порождающая матрицы, гарантируемый ранг и расстояние линейного кода над полем. Проверочная и порождающая матрицы в стандартной форме. Двойственный код, его проверочная и порождающая матрицы. Коды, двойственные к двоичному коду Хэмминга и к обобщённому коду Рида–Соломона.

1°. Проверочная и порождающая матрицы, гарантируемый ранг и расстояние линейного кода над полем. Проверочная и порождающая матрицы в стандартной форме.

Определение 4.1. Пусть S — произвольное множество элементов правого модуля M над кольцом $\mathcal{R}$. Наименьший (по включению) подмодуль $\langle S\rangle_{\mathcal{R}}$ модуля M, содержащий множество S, называется *подмодулем, порождённым множеством* S.

Если $N = \langle S\rangle_{\mathcal{R}}$, говорят также, что S — *система образующих подмодуля* N.

Предложение 4.2. Пусть S — произвольное множество элементов правого модуля M над кольцом $\mathcal{R}$. Тогда

$$\langle S\rangle_{\mathcal{R}} = S\mathcal{R} = \{x_1r_1 + \ldots + x_nr_n : x_i \in S, r_i \in \mathcal{R}, i = 1,\ldots,n,\ n \geq 0\}.$$

Определение 4.3. Если слова $g_i = (g_{i1},\ldots,g_{in})$, $i = 1,\ldots,m$ порождают код $\mathcal{C}$ длины n над модулем M, то матрица

$$G = \begin{pmatrix} g_{11} & \ldots & g_{1n} \\ \ldots\ldots\ldots\ldots\ldots \\ g_{m1} & \ldots & g_{mn} \end{pmatrix}$$

называется *порождающей матрицей* кода $\mathcal{C}$.

Определение 4.4. Пусть M — левый $\mathcal{R}$-модуль и $\mathcal{C}$ — код над M длины n. Матрица $H = (h_{ij})$ размера $r\times n$ над кольцом $\mathcal{R}$ называется *проверочной матрицей* кода $\mathcal{C}$ длины n над M, если

$$\mathcal{C} = \left\{\mathbf{a} \in M^n :\ H\mathbf{a}^T = 0\right\}. \tag{4.1}$$

Можно заметить, что для кодов над модулями и даже над кольцами проверочная матрица существует далеко не всегда. Однако, из курса линейной алгебры следует, что в случае линейных кодов над

полем $\mathbb{F}$ ($M = \mathcal{R} = \mathbb{F}$) любой код (т.е. подпространство в $\mathbb{F}^n$) задаётся некоторой однородной системой линейных уравнений вида (4.1), которой заведомо удовлетворяют строки порождающей матрицы кода и не удовлетворяют никакие другие векторы. Поэтому получаем следующий критерий.

Теорема 4.5. Пусть G и H — матрицы над полем $\mathbb{F}$ размеров $r \times n$ и $m \times n$, соответственно. Тогда следующие условия эквивалентны:

1. G и H — порождающая и проверочная матрицы некоторого кода $\mathcal{C}$ длины n над $\mathbb{F}$;
2. $HG^T = 0$ и $\mathrm{rk}(G) + \mathrm{rk}(H) = n$.

При этом размерность кода $\mathcal{C}$ равна $\mathrm{rk}(G)$.

Из (4.1) и теоремы 4.5 легко следует, что если умножить проверочную матрицу H (соответственно, порождающую матрицу G) кода $\mathcal{C}$ слева на обратимую матрицу A, (соответственно, B) допустимых размеров, то определяемый каждой из них код не изменится (т.к. $AH(BG)^T = AHG^TB = 0$). В частности, элементарные преобразования строк матриц H и G, т.е. прибавление к строке другой строки, умноженной на элемент поля, перестановка строк и умножение строки на ненулевой элемент поля, не меняют множества решений системы (4.1) (соответственно, линейной оболочки системы строк матрицы G), поэтому можно считать, что каждая из них содержит набор столбцов единичной матрицы порядков $n - \mathrm{rk}(\mathcal{C})$ и $\mathrm{rk}(\mathcal{C})$, соответственно, и число строк каждой из них равно её рангу.

Пример. Код проверки на чётность над полем задаётся матрицами

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix} \text{ и } G = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & -1 \\ 0 & 1 & 0 & \dots & 0 & 0 & -1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & & \dots & 1 & 0 & -1 \\ 0 & 0 & & \dots & 0 & 1 & -1 \end{pmatrix}.$$

Перестановка столбцов порождающей матрицы линейного кода соответствует переходу к некоторому линейно эквивалентному коду. При этом проверочную матрицу нового кода можно получить той же перестановкой столбцов. Следовательно, любой линейный код над полем линейно эквивалентен коду с проверочной матрицей *стандартного вида*: $H = (H' | -E)$, где E — единичная матрица порядка $n - k$, а H' — некоторая матрица размера $n - k \times k$.

Смысл этой записи в том, что первые k символов любого кодового слова $(a_1, \ldots, a_n)$ являются определяющими, а остальные вычисляются как $(a_{k+1}, \ldots, a_n) = (a_1, \ldots, a_k)(H')^T$.

Если код $\mathcal{C}$ имеет проверочную матрицу H в стандартной форме, то условиям $HG^T = 0$, $\mathrm{rk}H + \mathrm{rk}G = n$ удовлетворяет матрица $G = (E|(H')^T)$ размера $k \times n$, где E — единичная матрица порядка k. Она называется порождающей матрицей *стандартного вида*. Соответственно, любой линейный код над полем линейно эквивалентен коду с порождающей матрицей стандартного вида.

Определение 4.6. *Гарантируемым рангом* прямоугольной матрицы A над полем $\mathbb{F}$ называется число $\varkappa(A)$, равное максимальному числу s такому, что любые s столбцов матрицы линейно независимы (если A содержит нулевой столбец, считаем, что $\varkappa(A) = 0$).

Очевидно, что $\mathrm{rk}(A) \geq \varkappa(A)$.

Предложение 4.7. Если H — проверочная матрица ненулевого линейного кода $\mathcal{C}$ над полем, то $d(\mathcal{C}) = \varkappa(H) + 1$. Код $\mathcal{C}$ является МДР-кодом в точности тогда, когда $\varkappa(H) = \mathrm{rk}H$.

◀ Наличие в коде $\mathcal{C}$ слова веса d равносильно тому, что некоторые d столбцов матрицы H линейно зависимы, откуда $d(\mathcal{C}) > \varkappa(H)$. С другой стороны, по определению гарантируемого ранга, существует линейно зависимая система из $\varkappa(H)+1$ столбцов матрицы H, откуда $d \leq \varkappa(H) + 1$.

Действительно, $d(\mathcal{C}) = \varkappa(H) + 1$ и $n - k + 1 = \mathrm{rk}H + 1$. Поэтому $d(\mathcal{C}) = n - k + 1$ в точности при совпадении $\varkappa(H) = \mathrm{rk}H$. ▶

Предложение 4.8. Линейный код $\mathcal{C}$ над полем с проверочной матрицей $H = (H'|-E)$ стандартного вида является МДР-кодом тогда и только тогда, когда в матрице H' все квадратные подматрицы невырождены.

◀ Согласно предыдущему предложению, $\mathcal{C}$ есть МДР-код тогда и только тогда, когда любая система из $n-k$ столбцов матрицы H линейно независима. Пусть $H'[i_1, \ldots, i_s|j_1, \ldots, j_s]$ подматрица размера $s \times s$ матрицы H', составленная из элементов, стоящих на пересечении строк с номерами $i_1, \ldots, i_s$ и столбцов с номерами $j_1, \ldots, j_s$. Рассмотрим систему столбцов матрицы H с номерами $j_1, \ldots, j_s, k + i_{s+1}, \ldots, k + i_{n-k}$, где $i_{s+1}, \ldots, i_{n-k} \in \{1, \ldots, n-k\} \setminus \{i_1, \ldots, i_s\}$. Т.е.

это столбцы с номерами $j_1, \ldots, j_s$ из матрицы H' и столбцы с номерами $i_{s+1}, \ldots, i_{n-k}$ из матрицы $-E$. По формуле разложения определителя по столбцу определитель матрицы $(n-k)\times(n-k)$, построенный на этих столбцах, равен $\pm \det H'[i_1, \ldots, i_s | j_1, \ldots, j_s]$. Следовательно, линейная независимость этих столбцов равносильна невырожденности подматрицы $H'[i_1, \ldots, i_s | j_1, \ldots, j_s]$. ►

2°. Двойственный код, его проверочная и порождающая матрицы. Пусть $\mathbb{F}$ — конечное поле. Определим скалярное умножение векторов $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ правилом $\mathbf{ab} = a_1 b_1 + \cdots + a_n b_n \in \mathbb{F}$.

Определение 4.9. *Кодом, двойственным к линейному коду* $\mathcal{C} < \mathbb{F}^n$ называется код

$$\mathcal{C}^\circ = \{\mathbf{b} \in \mathbb{F}^n : \mathbf{b}\mathcal{C} = 0\},$$

(под $\mathbf{b}\mathcal{C} = 0$ понимается, что $\mathbf{ba} = 0$ для любого $\mathbf{a} \in \mathcal{C}$).

Теорема 4.10. Пусть $\mathcal{C}$ — линейный $[n, k]$-код над полем $\mathbb{F}$ с порождающей матрицей G и проверочной матрицей H. Тогда
1) $\mathcal{C}^\circ$ есть линейный $[n, n-k]$-код над $\mathbb{F}$ с порождающей матрицей H и проверочной матрицей G;
2) $\mathcal{C}^{\circ\circ} = \mathcal{C}$;
3) для любого линейного кода $\mathcal{L} \leq \mathbb{F}^n$ справедливы равенства

$$(\mathcal{C} + \mathcal{L})^\circ = \mathcal{C}^\circ \cap \mathcal{L}^\circ, \ (\mathcal{C} \cap \mathcal{L})^\circ = \mathcal{C}^\circ + \mathcal{L}^\circ.$$

◄ 1) Условие $\mathbf{b}\mathcal{C} = 0$ эквивалентно системе линейных уравнений $G\mathbf{b}^T = 0$. Поэтому матрица G будет проверочной для кода $\mathcal{C}^\circ$. Соответственно, из теоремы 4.5 получаем, что H — его порождающая матрица и $\dim \mathcal{C}^\circ = n - k$.

2) Получается из 1) повторным применением теоремы 4.5.

3)$(\mathcal{C} + \mathcal{L})^\circ = \{\mathbf{b} \in \mathbb{F}^n : \mathbf{b}(\mathcal{C} + \mathcal{L}) = 0\}$. В частности, $\mathcal{C}, \mathcal{L} \subseteq \mathcal{C} + \mathcal{L}$, $\mathbf{b}\mathcal{C} = 0$ и $\mathbf{b}\mathcal{L} = 0$, поэтому $(\mathcal{C}+\mathcal{L})^\circ \subseteq \mathcal{C}^\circ \cap \mathcal{L}^\circ$. Обратно, если $\mathbf{b} \in \mathcal{C}^\circ \cap \mathcal{L}^\circ$, то $\mathbf{b}\mathcal{C} = 0$ и $\mathbf{b}\mathcal{L} = 0$, значит, $\mathbf{b}(\mathcal{C} + \mathcal{L}) = 0$ и $(\mathcal{C} + \mathcal{L})^\circ \supseteq \mathcal{C}^\circ \cap \mathcal{L}^\circ$. Второе утверждение доказывается аналогично.►

Утверждение (1) теоремы 4.10 является эквивалентным определением двойственного кода.

Предложение 4.11. Пусть $\mathcal{C}$ — линейный $[n, k, n-k+1]$ МДР код над полем $\mathbb{F}$. Тогда $\mathcal{C}^\circ$ есть линейный $[n, n-k, k+1]$ МДР код над $\mathbb{F}$.

◄ Можно считать, что $\mathcal{C}$ имеет проверочную матрицу стандартного вида. Тогда по предложению 4.8 в матрице H' все квадратные подматрицы невырождены. По теореме 4.10 матрица $G = (E|(H')^T)$ является проверочной для кода $\mathcal{C}^\circ$. В матрице $(H')^T$ все квадратные подматрицы тоже невырождены, значит по предложению 4.8 код $\mathcal{C}^\circ$ также является МДР кодом.►

3°. Код, двойственный к обобщённому коду Рида–Соломона. Пусть $\mathbb{F}$ — конечное поле, $q = |\mathbb{F}|$, $M = \mathbb{F}[x|k] = \{f(x) \in \mathbb{F}[x] : \deg f(x) < k\}$, $x_1, \ldots, x_n$ — различные элементы поля $\mathbb{F}$, где $n \geq k$. $u_1, \ldots, u_n$ — обратимые элементы $\mathbb{F}$, отображение $\varphi : \mathbb{F}[x|k] \to \mathbb{F}^n$ задано правилом

$$\varphi(f(x)) = (u_1 f(x_1), \ldots, u_n f(x_n)).$$

Напомним, что образ $\varphi(\mathbb{F}[x|k])$ называется *обобщённым* $[n, k]$*-кодом Рида–Соломона* над полем $\mathbb{F}$. Обозначим его $GRS_q(n, k)$. Его порождающая матрица имеет вид

$$G = \begin{pmatrix} u_1 & u_2 & \ldots & u_n \\ u_1 x_1 & u_2 x_2 & \ldots & u_n x_n \\ \vdots & \vdots & & \vdots \\ u_1 x_1^{k-1} & u_2 x_2^{k-1} & \ldots & u_n x_n^{k-1} \end{pmatrix}.$$

Предложение 4.12. $GRS_q(n, k)^\circ = GRS_q(n, n-k)$.

◄ Рассмотрим элементы

$$y_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} (x_i - x_j)^{-1}, \; v_i = y_i u_i^{-1} \in \mathbb{F}^*, \; i = 1, \ldots, n,$$

и матрицу

$$H = \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1 x_1 & v_2 x_2 & \ldots & v_n x_n \\ \vdots & \vdots & & \vdots \\ v_1 x_1^{n-k-1} & v_2 x_2^{n-k-1} & \ldots & v_n x_n^{n-k-1} \end{pmatrix}.$$

Код с порождающей матрицей H является кодом $GRS_q(n, n-k)$. Достаточно показать, что H — проверочная для кода $GRS_q(n, k)$,

поскольку по теореме 4.10 это доказывает, что она порождающая для двойственного кода. По построению очевидно, что $\mathrm{rk}H = n - k$, следовательно, достаточно доказать равенство $HG^T = 0$.

Элемент на позиции (s,t) матрицы HG^T равен

$$\sum_{i=1}^{n} v_i x_i^{s-1} u_i x_i^{t-1} = \sum_{i=1}^{n} y_i x_i^{s+t-2}.$$

Возьмём матрицу Вандермонда

$$V = V(x_1, \ldots, x_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{pmatrix}.$$

Имеем $|V| = \prod\limits_{1 \le s < t \le n} (x_t - x_s)$, алгебраические дополнения элементов последней строки этой матрицы имеют вид

$$V_{n,j} = (-1)^{n+j} \prod_{\substack{1 \le s < t \le n \\ s,t \ne j}} (x_t - x_s).$$

Отметим, что

$$\frac{V_{n,i}}{|V|} = \prod_{\substack{s=1 \\ s \ne i}}^{n} (x_i - x_s)^{-1} = y_i.$$

Откуда

$$\sum_{i=1}^{n} y_i x_i^{s+t-2} = |V|^{-1} \sum_{i=1}^{n} x_i^{s+t-2} V_{n,i} = 0 \ \ -$$

фальшивое разложение определителя Вандермонда (элементы взяты из строки с номером $s+t-1 \le n-1$, а алгебраические дополнения для n-ой строки.) ►

4°. Код, двойственный к двоичному коду Хэмминга.

Определение 4.13. Код $\mathcal{M}_2(l)$, двойственный к двоичному коду Хэмминга $\mathcal{H}_2(l)$, называется *кодом Макдональда.*

Предложение 4.14. Код Макдональда $\mathcal{M}_2(l)$, двойственный к двоичному коду Хэмминга $\mathcal{H}_2(l)$, является линейным эквидистантным $[n, l, 2^{l-1}]_2$-кодом, лежащим на границе Плоткина.

◄ Линейность очевида по построению. Поскольку матрица H, проверочная для кода Хэмминга, содержит все ненулевые столбцы высоты l, то $\dim \mathcal{M}_2(l) = \mathrm{rk}H = l$.

Вычислим расстояние кода $\mathcal{M}_2(l)$ и докажем его эквидистантность. Поскольку матрица H содержит все столбцы высоты l, кроме нулевого, то любая её строка содержит в точности $\frac{2^l}{2} = 2^{l-1}$ единиц. Проведем дальнейшее доказательство индукцией по l.

База индукции. При $l = 1$ имеем $n = 1$, $H = (1)$ и слово (1) веса 1 является единственным ненулевым словом в коде $\mathcal{M}_2(1)$.

Шаг индукции. Пусть $l > 1$ и для всех $m < l$ утверждение верно. Пусть H' — порождающая матрица кода $\mathcal{M}_2(l-1)$, составленная из всех ненулевых столбцов высоты $l-1$. Обозначим $\mathbf{0} = (0, \ldots, 0)$, $\mathbf{1} = (1, \ldots, 1)$. Тогда $H = \begin{pmatrix} H' & \mathbf{0}^T & H' \\ \mathbf{0} & 1 & \mathbf{1} \end{pmatrix}$ (ненулевой столбец высоты l можно получить либо из ненулевого столбца высоты $l-1$ приписыванием 0 или 1, либо единицу можно также приписать к нулевому столбцу).

Любое ненулевое слово $\mathbf{a} \in \mathcal{M}_2(l)$ — сумма некоторых строк матрицы H. Если в сумме не участвует последняя строка, то $\mathbf{a} = (\mathbf{a}', 0, \mathbf{a}')$, где $\mathbf{a}' \in \mathcal{M}_2(l-1) \setminus \{0\}$. По предположению индукции $||\mathbf{a}'|| = 2^{l-2}$, соответственно, $||\mathbf{a}|| = 2||\mathbf{a}'|| = 2^{l-1}$. В противном случае, $\mathbf{a} = (\mathbf{a}', 0, \mathbf{a}') + (\mathbf{0}, 1, \mathbf{1})$. Заметим, что $||\mathbf{a}' + \mathbf{1}|| = 2^{l-1} - 1 - ||\mathbf{a}'||$. Откуда, $||\mathbf{a}|| = ||\mathbf{a}'|| + 1 + 2^{l-1} - 1 - ||\mathbf{a}'|| = 2^{l-1}$. Следовательно, веса всех ненулевых слов линейного кода $\mathcal{M}_2(l)$ одинаковы, поэтому он является эквидистантным кодом с минимальным расстоянием $d = 2^{l-1}$.

Вспомним, что код лежит на границе Плоткина, если $d = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n$. В данном случае $q = 2$, $n = 2^l - 1$, $|\mathcal{M}_2(l)| = 2^l$, откуда

$$\frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n = \frac{2^l}{2(2^l-1)} \cdot (2^1 - 1) = 2^{l-1} = d(\mathcal{M}_2(l)).$$

►

Заметим, что $|\mathcal{M}_2(l)| = 2^l = n + 1$. Оказывается, что мощность кода Макдональда является максимально возможной среди любых эквидистантных линейных n-кодов.

Теорема 4.15. Пусть $\mathcal{C}$ — эквидистантный линейный код в $\mathbb{F}_2^n$, тогда $|\mathcal{C}| \leq n + 1$.

◄ Пусть $\mathcal{C} = \{\mathbf{c_1}, \ldots, \mathbf{c_s}\}$, и при этом $d(\mathbf{c_i}, \mathbf{c_j}) = d$, для всех $i \neq j$.

Для любых различных $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$ имеем

$$d(\mathbf{a},\mathbf{b}) = \sum_{i=1}^{n} |a_i - b_i| = \sum_{i=1}^{n} (a_i - b_i)^2 = ||\mathbf{a}|| + ||\mathbf{b}|| - 2\mathbf{ab}$$

(все вычисления, в частности, модуля и скалярного произведения выполняются над $\mathbb{R}$). Откуда для $\mathbf{a}, \mathbf{b} \in \mathcal{C} \setminus \{0\}$ получаем, что $d = 2d - 2\mathbf{ab}$ и $\mathbf{ab} = \frac{d}{2}$. Без ограничения общности можно считать, что $\mathbf{c_1} = 0$.

Вычислим определитель Грама для векторов $\mathbf{c_2}, \ldots, \mathbf{c_s}$ как векторов в $\mathbb{R}^n$ (для $(0,1)$-векторов вес Хэмминга совпадает со скалярным квадратом):

$$\begin{vmatrix} d & \frac{d}{2} & \ldots & \frac{d}{2} \\ \frac{d}{2} & d & \ldots & \frac{d}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d}{2} & \frac{d}{2} & \ldots & d \end{vmatrix} = \frac{d^{s-1}}{2^{s-1}} \begin{vmatrix} 2 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 2 \end{vmatrix} = \frac{d^{s-1}}{2^{s-1}} s \neq 0,$$

т.е. $\mathbf{c_2}, \ldots, \mathbf{c_s}$ линейно независимы над $\mathbb{R}$.

Итак, имеем $s-1$ линейно независимых векторов. В пространстве $\mathbb{R}^n$ может быть не более n линейно независимых векторов, значит, $s - 1 \leq n$ и $s \leq n + 1$. ▶

Лекция 5. Построение новых кодов из заданных. Граница Грайсмера.

1°. Добавление констант

Определение 5.1. Код $\mathcal{C} \subseteq \mathbb{F}^n$ *содержит константы*, если он содержит все слова вида $(a, \ldots, a)$, $a \in \mathbb{F}$. Для линейного кода это условие равносильно включению $\mathbf{1} = (1, \ldots, 1) \in \mathcal{C}$.

Определение 5.2. Для произвольных $\alpha \in \mathbb{F}$ и $\mathbf{a} \in \mathbb{F}^n$ обозначим через $s_\alpha(\mathbf{a})$ количество координат в слове $\mathbf{a}$, равных α. Также положим $s_{\max} = \max\{s_\alpha(\mathbf{a}) : \ \mathbf{a} \in \mathcal{C} \setminus \{0\}\,, \ \alpha \in \mathbb{F}\}$.

Определение 5.3. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный код, не содержащий констант. Тогда говорят, что код $\mathcal{C}^c = \mathcal{C} + \mathbb{F}\mathbf{1}$ *получен из кода* $\mathcal{C}$ *добавлением констант.* Заметим, что добавление констант к коду равносильно приписыванию строки $\mathbf{1}$ к его порождающей матрице.

Предложение 5.4. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n, k, d]_q$-код, не содержащий констант. Тогда код $\mathcal{C}^c = \mathcal{C} + \mathbb{F}\mathbf{1}$ есть линейный $[n, k+1, d']_q$-код с расстоянием $d' = n - s_{\max} \leq d$.

◀ По построению код $\mathcal{C}^c$ есть линейный $[n, k+1]_q$-код. Вычислим его расстояние.

Произвольное слово $\mathbf{b} \in \mathcal{C}^c$ представляется в виде $\mathbf{b} = \mathbf{a} - \alpha\mathbf{1}$, где $\mathbf{a} \in \mathcal{C}, \alpha \in \mathbb{F}$. По построению $||b|| = n - s_\alpha(\mathbf{a}) \geq n - s_{\max}$. Выражение $n - s_{\max} \geq 1$ в силу того, что код $\mathcal{C}$ не содержит констант. Откуда видно, что $d' \geq n - s_{\max}$. Выбирая такие $\mathbf{a} \in \mathcal{C} \setminus \{0\}$ и $\alpha \in \mathbb{F}$, что $s_{\max} = s_\alpha(\mathbf{a})$, получаем, что $||b|| = n - s_{\max}$ и $d' = n - s_{\max}$.

Неравенство $d' \leq d$ следует из включения $\mathcal{C} \leq \mathcal{C}^c$. ▶

2°. Добавление проверки на чётность

Определение 5.5. Код $\mathcal{C} \subseteq \mathbb{F}^n$ *содержит проверку на чётность*, если его двойственный код $\mathcal{C}^\circ$ содержит слово $\mathbf{1}$.

Определение 5.6. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n, k, d]_q$-код с проверочной матрицей H размера $l \times n$. Тогда говорят, что код $\widehat{\mathcal{C}} \leq \mathbb{F}^{n+1}$ с проверочной матрицей

$$\widehat{H} = \begin{pmatrix} \mathbf{1} & 1 \\ H & \mathbf{0}^T \end{pmatrix}$$

получен из кода $\mathcal{C}$ добавлением проверки на чётность.

Предложение 5.7. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n,k,d]_q$-код с проверочной матрицей H размера $l \times n$. Тогда линейный код $\widehat{\mathcal{C}} \leq \mathbb{F}^{n+1}$, полученный из кода $\mathcal{C}$ добавлением проверки на чётность, есть линейный $[n+1,k,\widehat{d}]_q$-код с расстоянием $\widehat{d} \in \{d, d+1\}$. Если код $\mathcal{C}$ содержит проверку на чётность, то $\widehat{d} = d$.

◀ По построению $\mathrm{rk}\widehat{H} = \mathrm{rk}H + 1$, поэтому $\dim\widehat{\mathcal{C}} = n + 1 - \mathrm{rk}\widehat{H} = n - \mathrm{rk}H = k$.

Вычислим расстояние кода $\widehat{\mathcal{C}}$. Вспомним, что $d(\widehat{\mathcal{C}}) = \varkappa(\widehat{H})+1$. Заметим, что любые $\varkappa(H)$ столбцов матрицы $\widehat{H}$ линейно независимы, поскольку любые $\widehat{H}$ из первых n столбцов получены приписыванием 1 к линейно независимым столбцам матрицы H, а последний столбец не выражается через остальные, если они также линйено независимы.

С другой стороны, если мы возьмём в матрице $\widehat{H}$ $\varkappa(H)+1$ столбцов из первых n так, что сооответсвующие столбцы линейно зависимы в H, то их линейная комбинация с теми же коэффициентами даст столбец, пропорциональный последнему. Следовательно, в матрице $\widehat{H}$ есть $\varkappa(H)+2$ линейно зависимых столбца, и $\varkappa(\widehat{H}) \leq \varkappa(H)+1$. Таким образом, $d \leq \widehat{d} \leq d+1$. ▶

Следствие 5.8. Если $q = 2$ и d нечётно, то $\widehat{d} = d + 1$.

◀ Если $q = 2$, то все слова кода $\widehat{\mathcal{C}}$ имеют чётный вес, поэтому $\widehat{d}$ чётно, значит не равно d в данном случае.▶

3°. Расширение кода

Определение 5.9. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n,k,d]_q$-код. Тогда про код $\mathcal{C}^{ext}$, полученный из кода $\mathcal{C}$ добавлением констант и проверки на чётность, говорят, что он есть *расширение кода $\mathcal{C}$* или *расширенный код $\mathcal{C}$*.

Следствие 5.10. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n,k,d]_q$-код, не содержащий констант. Тогда код $\mathcal{C}^{ext}$ есть линейный $[n+1,k+1,d^{ext}]_q$-код, где $d^{ext} = n - s_{\max} + \delta$, $\delta \in \{0,1\}$.

4°. Декартово произведение кодов

Определение 5.11. Пусть $\mathcal{C}_i$ — линейные $[n_i, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, \ldots, m$. Тогда о коде

$$\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_m \leq \mathbb{F}^{n_1 + \cdots + m_m},$$

состоящем из всех слов вида $(\mathbf{a}_1, \ldots, \mathbf{a}_m)$, $\mathbf{a}_i \in \mathcal{C}_i$, $i = 1, \ldots, m$, говорят как о *декартовом произведении кодов* $\mathcal{C}_1, \ldots, \mathcal{C}_m$. При этом коды $\mathcal{C}_i$ называют *компонентами* кода $\mathcal{C}$.

Предложение 5.12. Код $\mathcal{C}$ есть $[n_1 + \cdots + n_m, k_1 + \cdots + k_m, d]_q$-код для $d = \min\{d_1, \ldots, d_m\}$. $\mathcal{C}$ — линейный код тогда и только тогда, когда все его компоненты линейны. При этом проверочная матрица кода $\mathcal{C}$ задаётся равенством

$$H = \begin{pmatrix} H_1 & 0 & \ldots & 0 \\ 0 & H_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & H_m \end{pmatrix},$$

где H_i — проверочная матрица кода $\mathcal{C}_i$, $i = 1, \ldots, m$.

5°. Тензорное произведение кодов

Определение 5.13. *Тензорным произведением матриц* $A \in M_{m,n}(\mathbb{F})$ *и* $B \in M_{k,l}(\mathbb{F})$ называется матрица

$$A \otimes B = \begin{pmatrix} a_{11}B & \ldots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \ldots & a_{mn}B \end{pmatrix} \in M_{mk,nl}(\mathbb{F}).$$

Определение 5.14. Пусть $\mathcal{C}_i$ — линейные $[n_i, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, 2$. *Тензорным произведением кодов* $\mathcal{C}_1$ *и* $\mathcal{C}_2$ называется код $\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2 \in \mathbb{F}^{n_1 n_2}$, порождённый всеми словами вида

$$\mathbf{a} \otimes \mathbf{b},\ \mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2$$

(под тензорным произведением кодовых слов понимается их произведение как $1 \times n_i$ матриц).

Предложение 5.15. Пусть $\mathcal{C}_i$ — линейные $[n_i, k_i, d_i]_q$-коды над полем $\mathbb{F}$, с порождающими матрицами $G^{(i)} \in M_{k_i, n_i}$ и проверочными матрицами $H^{(i)} \in M_{n_i - k_i, n_i}$, $i = 1, 2$. Тогда код $\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2$

есть линейный $[n_1n_2, k_1k_2, d_1d_2]_q$-код с порождающей матрицей $G = G^{(1)} \otimes G^{(2)}$ и проверочной матрицей $H = \begin{pmatrix} H^{(1)} \otimes E_{n_2} \\ E_{n_1} \otimes H^{(2)} \end{pmatrix}$.

◀ Пусть $G^{(i)} = \begin{pmatrix} \mathbf{a}_1^{(i)} \\ \vdots \\ \mathbf{a}_{k_i}^{(i)} \end{pmatrix}$, $i = 1, 2$. Любое слово кода $\mathcal{C}$ линейно выражается через множество слов $\mathbf{a}_r^{(1)} \otimes \mathbf{a}_s^{(2)}$, $r = 1, \ldots, k_1$, $s = 1, \ldots, k_2$. Эти слова составлют множество строк матрицы G, следовательно она является порождающей матрицей кода $\mathcal{C}$.▶

По свойству тензорного произведения $\dim\mathcal{C} = \mathrm{rk}G = \mathrm{rk}G^{(1)} \cdot \mathrm{rk}G^{(2)} = k_1k_2$.

Вычислим расстояние кода $\mathcal{C}$. Для этого рассмотрим изоморфизм $\varphi : \mathbb{F}^{n_1n_2} \to M_{n_1,n_2}(\mathbb{F})$ линейных пространств, сопоставляющий любому слову $\mathbf{c} = (c_1, \ldots, c_{n_1n_2})$ матрицу

$$\varphi(\mathbf{c}) = \begin{pmatrix} c_1 & \ldots & c_{n_2} \\ \vdots & & \vdots \\ c_{(n_1-1)n_2+1} & \ldots & c_{n_1n_2} \end{pmatrix}.$$

Тогда для любых $\mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2$ слову

$$\mathbf{a} \otimes \mathbf{b} = (a_1b_1, \ldots, a_1b_{n_2}, a_2b_1, \ldots, a_2b_{n_2}, \ldots, a_{n_1}b_1, \ldots, a_{n_1}b_{n_2}) \in \mathcal{C}$$

соответствует матрица

$$\varphi(\mathbf{a} \otimes \mathbf{b}) = \begin{pmatrix} a_1b_1 & a_1b_2 & \ldots & a_1b_{n_2} \\ a_2b_1 & a_2b_2 & \ldots & a_2b_{n_2} \\ \vdots & \vdots & & \vdots \\ a_{n_1}b_1 & a_{n_1}b_2 & \ldots & a_{n_1}b_{n_2} \end{pmatrix},$$

столбцы которой принадлежат коду $\mathcal{C}_1$, а строки — $\mathcal{C}_2$. По линейности это верно для любой матрицы из пространства $\varphi(\mathcal{C})$. Следовательно, если $M \in \varphi(\mathcal{C}) \setminus \{0\}$, то в M есть столбец с весом не менее d_1, а значит есть не менее d_1 ненулевой строки. Вес каждой из этих строк не менее d_2, поэтому в матрице M не менее d_1d_2 ненулевых элементов. Значит, столько же ненулевых элементов содержит кодовое слово $\mathbf{c} = \varphi^{-1}(M) \in \mathcal{C} \setminus \{0\}$ и $||\mathbf{c}|| \geq d_1d_2$. Таким образом, $d(\mathcal{C}) \geq d_1d_2$. Выбирая $\mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2$ так, что $||\mathbf{a}|| = d_1$, $||\mathbf{b}|| = d_2$ получаем, что $||\mathbf{a} \otimes \mathbf{b}|| = d_1d_2$. Следовательно, $d(\mathcal{C}) = d_1d_2$. Осталось найти проверочную матрицу кода $\mathcal{C}$.

Условие $HG^T = 0$ выполнено по определению матриц G и H. Пусть для слова $\mathbf{c} \in \mathbb{F}^{n_1 n_2}$ выполнено равенство $H\mathbf{c}^T = 0$. Тогда для матрицы $M = \varphi(\mathbf{c})$ это означает, что выполнены равенства $H^{(1)}M = 0, H^{(2)}M^T = 0$. Из условия $H^{(2)}M^T = 0$ следует, что строки матрицы M являются линейными комбинациями строк матрицы $G^{(2)}$, поэтому $M = UG^{(2)}$ для некоторой матрицы $U \in M_{n_1,k_2}(\mathbb{F})$. Тогда $H^{(1)}M = H^{(1)}UG^{(2)} = 0$. Поскольку строки матрицы $G^{(2)}$ линейно независимы отсюда следует, что $H^{(1)}U = 0$. Это означает, что столбцы матрицы U принадлежат коду $\mathcal{C}_1$ и линейно выражаются через столбцы матрицы $G^{(1)}$. Тогда из равенства $M = UG^{(2)}$ заключаем, что матрица M является линейной комбинацией матриц $(\mathbf{a}_r^{(1)})^T \cdot \mathbf{a}_s^{(2)}$, а её прообраз слово $\mathbf{c}$ — линейной комбинацией слов $\mathbf{a}_r^{(1)} \otimes \mathbf{a}_s^{(2)}$, $r = 1, \ldots, k_1$, $s = 1, \ldots, k_2$, базисных для кода $\mathcal{C}$. Таким образом, $\mathbf{c} \in \mathcal{C}$. Значит, однородной системе с матрицей H удовлетворяют слова кода $\mathcal{C}$ и только они, поэтому H — проверочная матрица этого кода.

6°. Гибридный код

Определение 5.16. Пусть $\mathcal{C}_i$ — линейные $[n, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, 2$. *Гибридом кодов кодов* $\mathcal{C}_1$ *и* $\mathcal{C}_2$ называется код $\mathcal{C} = \mathcal{C}_1 \dashv \mathcal{C}_2 \in \mathbb{F}^{2n}$, состоящий из всех слов вида

$$(\mathbf{a}, \mathbf{a} + \mathbf{b}),\ \mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2.$$

Предложение 5.17. Пусть $\mathcal{C}_i$ — линейные $[n, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, 2$. Тогда код $\mathcal{C} = \mathcal{C}_1 \dashv \mathcal{C}_2$ есть линейный $[2n, k_1 + k_2, d]_q$-код с $d = \min\{2d_1, d_2\}$.

◀ По построению очевидно, что $\mathcal{C}$ есть линейный $[2n, k_1 + k_2]_q$-код. Вычислим его расстояние. Сразу видно, что $d \leq \min\{2d_1, d_2\}$, поскольку в $\mathcal{C}$ есть слова $(\mathbf{a}, \mathbf{a})$ и $(0, \mathbf{b})$ с $||\mathbf{a}|| = d_1$ и $||\mathbf{b}|| = d_2$.

С другой стороны по неравенству треугольника получаем, что

$$||(\mathbf{a}, \mathbf{a} + \mathbf{b})|| = ||\mathbf{a}|| + ||\mathbf{a} + \mathbf{b}|| \geq ||\mathbf{a}|| + |||\mathbf{a}|| - ||\mathbf{b}|||\,.$$

Если $\mathbf{a} = 0$, то вес такого слова не меньше d_2.

Пусть $\mathbf{a} \neq 0$. Если $||\mathbf{b}|| \geq ||\mathbf{a}|| (> 0)$, то $||\mathbf{a}|| + |||\mathbf{a}|| - ||\mathbf{b}||| = ||\mathbf{b}|| \geq d_2$. Пусть $0 < ||\mathbf{b}|| < ||\mathbf{a}||$. Имеем $||(\mathbf{a}, \mathbf{a} + \mathbf{b})|| \geq ||\mathbf{a}|| > ||\mathbf{b}|| \geq d_2$, иначе $\mathbf{b} = 0$ и $||(\mathbf{a}, \mathbf{a})|| \geq 2d_1$. ▶

7°. Увеличение размерности с сохранением расстояния

Предложение 5.18. Пусть $\mathcal{C}$ — линейный $[n,k,d]_q$-код над полем $\mathbb{F}$ и $\mathbf{b} \in \mathbb{F}^n \setminus \mathcal{C}$ – слово, расстояние от которого до любого слова из кода $\mathcal{C}$ не меньше, чем $d-1$. Тогда код $\mathcal{C}'$, состоящий из всех слов вида

$$(\mathbf{a} + \alpha\mathbf{b}, \alpha),\ \mathbf{a} \in \mathcal{C}, \alpha \in \mathbb{F},$$

есть линейный $[n+1, k+1, d]$-код. Если G — порождающая матрица кода $\mathcal{C}$, то порождающей для $\mathcal{C}'$ будет, например, матрица $G' = \begin{pmatrix} G & \mathbf{0}^T \\ \mathbf{b} & 1 \end{pmatrix}$.

8°. Граница Грайсмера.

Далее будем использовать обозначение $\lceil x \rceil = \min\{i \in \mathbb{Z} : i \geq x\}$. Легко проверить, что если $a, b \in \mathbb{R}$ и $c \in \mathbb{N}$, то

$$\left\lceil \frac{a}{bc} \right\rceil = \left\lceil \frac{\left\lceil \frac{a}{b} \right\rceil}{c} \right\rceil. \tag{5.1}$$

Действительно, для любого $i \in \mathbb{Z}$ имеем

$$i \geq \frac{a}{bc} \Leftrightarrow ic \geq \frac{a}{b} \Leftrightarrow ic \geq \left\lceil \frac{a}{b} \right\rceil \Leftrightarrow i \geq \frac{\left\lceil \frac{a}{b} \right\rceil}{c}.$$

Теорема 5.19 (Граница Грайсмера)**.** Пусть $\mathcal{C}$ — линейный $[n,k,d]_q$-код над полем $\mathbb{F}$. Тогда

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil. \tag{5.2}$$

◀ 1. Обозначим через $N_q(k,d)$ наименьшее число N, для которого существует линейный код над $\mathbb{F}$ длины N размерности k, расстояние которого не меньше d. Заметим, что это определение корректно: достаточно рассмотреть код длины kd, состоящий из всех слов вида

$$(\underbrace{\alpha_1, \ldots, \alpha_1}_{d \text{ раз}}, \underbrace{\alpha_2, \ldots, \alpha_2}_{d \text{ раз}}, \ldots, \underbrace{\alpha_k, \ldots, \alpha_k}_{d \text{ раз}}), \quad \alpha_1, \ldots, \alpha_k \in \mathbb{F}.$$

Еще заметим, что функция $N_q(k,d)$ монотонна по второму аргументу: $N_q(k,d) \leq N_q(k,\tilde{d})$ при $d \leq \tilde{d}$.

2. Докажем следующее неравенство:

$$N_q(k,d) \geq d + N_q\left(k-1, \left\lceil \frac{d}{q} \right\rceil\right). \tag{5.3}$$

Пусть некоторый $[n,k,\tilde{d}]_q$-код с $n = N_q(n,d)$ и $\tilde{d} \geq d$ задаётся порождающей матрицей G ранга k, первая строка которой имеет вес $\tilde{d}$. Переходя к линейно эквивалентному коду, можем считать, что матрица G состоит из k строк и имеет вид

$$\left(\begin{array}{c|c} \overbrace{0\ldots0}^{n-\tilde{d}} & \overbrace{1\ldots1}^{\tilde{d}} \\ \hline G' & G'' \end{array}\right).$$

Заметим, что $\mathrm{rk}G' = k-1$. Действительно, запишем строки матрицы G в виде $a_i = (a_i'|a_i'')$, $i = 1,\ldots,k$, где a_i' и a_i'' — строки матриц G' и G'', причём $a_1' = 0$. Допустим, что $\sum_{i=2}^k \lambda_i a_i' = 0$ для некоторых $\lambda_2,\ldots,\lambda_k \in P$. Положим $b = \sum_{i=2}^k \lambda_i a_i''$. Ясно, что для некоторого $\lambda \in \mathbb{F}$ имеем $||b - \lambda a_1''|| < \tilde{d}$. Следовательно,

$$||-\lambda a_1 + \sum_{i=2}^k \lambda_i a_i|| = ||-\lambda(a_1'|a_1'') + \sum_{i=2}^k \lambda_i(a_i'|a_i'')|| = ||(0|b-\lambda a_1'')|| < \tilde{d},$$

откуда $-\lambda a_1 + \sum_{i=2}^k \lambda_i a_i = 0$ и $\lambda_2 = \ldots = \lambda_k = 0$.

Пусть теперь d' — минимальное расстояние кода $\mathcal{C}'$, порождённого строками матрицы G'. Тогда в коде $\mathcal{C}$ содержится слово вида $(a|b)$, где $||a|| = d'$. Но в слове b длины $\tilde{d}$ над $\mathbb{F}$ хотя бы один символ, скажем, λ, встречается не менее чем $\left\lceil \frac{\tilde{d}}{q} \right\rceil$ раз (иначе число вхождений каждого символа меньше $\tilde{d}/q$, а сумма этих q чисел равна $\tilde{d}$). Значит, $||b - \lambda a_1''|| \leq \tilde{d} - \left\lceil \frac{\tilde{d}}{q} \right\rceil$. Имеем $\tilde{d} \leq ||(a|b) - \lambda a_1|| = d' + ||b - \lambda a_1''|| \leq d' + \tilde{d} - \left\lceil \frac{\tilde{d}}{q} \right\rceil$. Таким образом, $d' \geq \left\lceil \frac{\tilde{d}}{q} \right\rceil \geq \left\lceil \frac{d}{q} \right\rceil$, поэтому $n - d \geq n - \tilde{d} \geq N_q(k-1,d') \geq N_q\left(k-1, \left\lceil \frac{d}{q} \right\rceil\right)$, откуда сразу следует (5.3).

3. Теперь применим доказанное неравенство к $[n,k,d]_q$-коду

несколько раз. Имеем

$$n \geq N_q(k,d) \geq d + N_q\left(k-1, \left\lceil \frac{d}{q} \right\rceil\right) \geq$$
$$\geq d + \left\lceil \frac{d}{q} \right\rceil + N_q\left(k-2, \left\lceil \frac{\left\lceil \frac{d}{q} \right\rceil}{q} \right\rceil\right) \overset{(5.1)}{=}$$
$$= d + \left\lceil \frac{d}{q} \right\rceil + N_q\left(k-2, \left\lceil \frac{d}{q^2} \right\rceil\right) \geq \ldots \geq$$
$$\geq d + \left\lceil \frac{d}{q} \right\rceil + \ldots + \left\lceil \frac{d}{q^{k-2}} \right\rceil + N_q\left(1, \left\lceil \frac{d}{q^{k-1}} \right\rceil\right),$$

откуда
следует утверждение теоремы, поскольку, очевидно, $N_q(1,m) = m$ для любого натурального числа m.►

9°. Уменьшение длины кода

Предложение 5.20. Пусть $\mathcal{C}$ — линейный $[n,k,d]_q$-код над полем $\mathbb{F}$ и $\in \mathcal{C}$ – слово веса d с ненулевыми координатами в позициях $i_1,\ldots,i_d$. Тогда код $\overline{\mathcal{C}}$, получающийся из кода $\mathcal{C}$ вычеркиванием всех слов, пропорциональных $\mathbf{c}$, и вычёркиванием в остальных словах координат с номерами $i_1,\ldots,i_d$ есть линейный $[n-d,k-1,d_1]$-код, где $d_1 \geq \left\lceil \frac{d}{q} \right\rceil$. Если $\mathcal{C}$ — не МДР-код (т.е. $d \leq n-k$), то двойственный к коду $\overline{\mathcal{C}}$ код $\overline{\mathcal{C}}^\circ$ есть $[n-d, n-d-(k-1), d_0]$-код, где $d_0 \geq d(\mathcal{C}^\circ)$.

◄ Первое утверждение сразу следует из доказательства пункта 2 теоремы о границе Грайсмера.

Введённая в этом утверждении матрица G' будет проверочной для кода $\overline{\mathcal{C}}^\circ$, поэтому это линейный код длины $n-d$ и размерности $(n-d) - \mathrm{rk}G' = (n-d) - (k-1) \geq 1$, т.к. $d \leq n-k$.

Пусть G — порождающая матрица кода $\mathcal{C}$, она же будет проверочной матрицей для кода $\mathcal{C}^\circ$. Тогда по предложению о связи расстояния кода и гарантируемого ранга имеем $\varkappa(G) = d(\mathcal{C}^\circ) - 1$. И поскольку код и двойственный к нему являются МДР-кодами одновременно, то $\varkappa(G) < \mathrm{rk}G = k$. Таким образом, число $\varkappa(G)$ не превосходит числа $k-1$ столбцов матрицы G'. С учётом этого, из строения матрицы G видно, что в матрице G' любые $\varkappa(G)$ столбцов линейно независимы. Следовательно, $\varkappa(G') \geq \varkappa(G)$. В итоге получаем, что $d_0 \geq d(\mathcal{C}^\circ)$. ►

Следствие 5.21. Пусть $\mathcal{C}$ — линейный МДР-код $[n,k,d]_q$-код над полем $\mathbb{F}$ мощности q размерности $k \geq 2$. Тогда $d \leq q$ и $n \leq q+k-1$.

◀ Поскольку $\mathcal{C}$ — МДР-код, то $d = n-(k-1)$ и $n = d+k-1$. Поэтому в обозначениях предыдущего доказательства имеем, что матрица G' размера $(k-1)\times(k-1)$ имеет $\mathrm{rk}G' = k-1$. Следовательно, $\overline{\mathcal{C}} = \mathbb{F}^{k-1}$ и $d_1 = 1$. Откуда $\left\lceil \frac{d}{q} \right\rceil \leq 1$, $d \leq q$ и $n \leq q+k-1$. ▶

Лекция 6. Основные понятия теории колец. Локальные кольца, эквивалентные определения. Разложение конечного коммутативного кольца в прямую сумму локальных колец.

Пусть $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$.

1°. Основные понятия теории колец.

Определение 6.1. Пусть $\mathcal{R}, \mathcal{S}$ — кольца. Отображение $f : \mathcal{R} \to \mathcal{S}$ называется *гомоморфизмом* кольца $\mathcal{R}$ в кольцо $\mathcal{S}$, если оно сохраняет операции:

$$\forall a, b \in \mathcal{R}, \quad f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b).$$

Мы будем рассматривать только унитарные гомоморфизмы колец, т.е. такие гомоморфизмы, которые отображают единицу кольца $\mathcal{R}$ в единицу кольца $\mathcal{S}$. Гомоморфизм называется *изоморфизмом*, если он является биективным отбражением. Кольца, между которыми имеется изоморфизм, называются *изоморфными* (обозначение $\mathcal{R} \cong \mathcal{S}$). С каждым гомоморфизмом колец $f : \mathcal{R} \to \mathcal{S}$ связаны его *образ* $\mathrm{Im}(f) = f(\mathcal{R})$ и *ядро* $\ker(f) = \{x \in R : f(x) = 0\}$.

Определение 6.2. Подмножество I кольца $\mathcal{R}$ называется *правым (левым) идеалом* этого кольца, если I — подмодуль правого модуля $\mathcal{R}_{\mathcal{R}}$ (левого модуля ${}_{\mathcal{R}}\mathcal{R}$). Подмножество кольца $\mathcal{R}$, которое является и правым и левым идеалом кольца $\mathcal{R}$, называется *идеалом* (иногда уточняется: двусторонним идеалом) кольца $\mathcal{R}$, что обозначается так: $I \lhd \mathcal{R}$. В случае коммутативного кольца все идеалы — двусторонние.

Определение 6.3. Пусть I — идеал кольца $\mathcal{R}$. Рассмотрим множество всех смежных классов $\{x + I : x \in \mathcal{R}\}$ аддитивной группы кольца $\mathcal{R}$ по подгруппе I и зададим на этом множестве операции

$$(x+I) + (y+I) = (x+y) + I, \ (x+I)(y+I) = xy + I$$

для любых $x, y \in \mathcal{R}$. Полученное кольцо называется *фактор-кольцом* кольца $\mathcal{R}$ по идеалу I и обозначается $\mathcal{R}/I$. Отображение $\pi : \mathcal{R} \to \mathcal{R}/I$, заданное равенством $\pi(x) = x+I$ для любого $x \in \mathcal{R}$, называется *каноническим гомоморфизмом* кольца на фактор-кольцо.

Определение 6.4. Конечная (внешняя) *прямая сумма* колец $\mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$ это множество $\mathcal{R}_1 \times \ldots \times \mathcal{R}_n$ (т.е. декартово произведение множеств $\mathcal{R}_1, \ldots, \mathcal{R}_n$) с покоординатными операциями сложения и умножения.

Определение 6.5. Элемент $e \in \mathcal{R}$ называется *идемпотентом*, если $e^2 = e$ (заметим, что при этом $(1-e)^2 = 1 - 2e + e = 1 - e$ — также идемпотент).

Лемма 6.6. Для любого $r \in \mathcal{R}$ существует $k = k(r) \in \mathbb{N}$, для которого r^k — идемпотент.

◀ Выберем $m, n \in \mathbb{N}$, для которых $r^{m+n} = r^n$. Умножая на r^m и r^n несколько раз, имеем $r^{pn+qm} = r^{pn}$ для любых $p, q \in \mathbb{N}$. Осталось взять $p = m, q = n$ и $k = mn$.▶

Определение 6.7. *Полное ортогональное множество идемпотентов* (сокращённо, *ПОМИ*) — это такая система элементов $e_1, \ldots, e_n \in \mathcal{R} \setminus \{0\}$, что
1) $e_i e_j = \delta_{ij} e_i$, $1 \leq i, j \leq n$, в частности, $e_i^2 = e_i$, $i = 1, \ldots, n$;
2) $\sum\limits_{i=1}^{n} e_i = 1$.

Теорема 6.8. $\mathcal{R} \cong \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$ тогда и только тогда, когда существует ПОМИ $e_1, \ldots, e_n \in \mathcal{R}$ такое, что $\mathcal{R}_i \cong \mathcal{R}e_i$, $i = 1, \ldots, n$.

◀ "$\Rightarrow$" Положим $e_i = (0, \ldots, 0, 1_{\mathcal{R}_i}, 0, \ldots, 0)$. По определению операций в прямой сумме колец множество $e_1, \ldots, e_n$ является ПОМИ и $\mathcal{R}e_i \cong \mathcal{R}_i$.

"$\Leftarrow$" Пусть $e_1, \ldots, e_n \in \mathcal{R}$ — ПОМИ. Зададим отображение $\varphi : \mathcal{R} \to \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$ так, что $\varphi(r) = (re_1, \ldots, re_n)$.

Проверим, что φ — гомоморфизм колец. Действительно, для произвольных $r, s \in \mathcal{R}$ имеем

$$\varphi(r) = (re_1, \ldots, re_n),\ \varphi(s) = (se_1, \ldots, se_n).$$

Откуда сразу получаем, что

$$\varphi(r+s) = ((r+s)e_1, \ldots, (r+s)e_n) = \\ = (re_1, \ldots, re_n) + (se_1, \ldots, se_n) = \varphi(r) + \varphi(s).$$

Кроме того

$$rse_j = rse_j^2 = re_j se_j \ \forall j = 1, \ldots, n,$$

поэтому

$$\varphi(rs) = (rse_1, \ldots, rse_n) = (re_1 se_1, \ldots, re_n se_n) = \varphi(r)\varphi(s).$$

Проверим, что φ — биекция. Условие, что $r \in \ker(\varphi)$ означает, что $(re_1, \ldots, re_n) = (0, \ldots, 0)$, т.е. $re_i = 0$ для всех $i = 1, \ldots, n$. Следовательно, $r = r \cdot 1 = \sum\limits_{i=1}^{n} re_i = 0$, значит, $ker(\varphi) = \{0\}$. Инъективность отображения φ доказана. Для $r = r_1e_1 + \cdots + r_ne_n$ имеем $re_i = r_ie_i$ по ортогональности, поэтому $\varphi(r) = (re_1, \ldots, re_n) = (r_1e_1, \ldots, r_ne_n)$ — произвольный элемент кольца $\mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$, т.е. φ — сюръективно.▶

Определение 6.9. Элемент $r \in \mathcal{R}$ называется *нильпотентным*, если существует $n \in \mathbb{N}$, что $r^n = 0$.

Определение 6.10. Определим произведение идеала I кольца $\mathcal{R}$ на правый $\mathcal{R}$-модуль M:

$$MI = \left\{ \sum_{i=1}^{n} x_i a_i : n \in \mathbb{N}, x_i \in M, a_i \in I \right\}.$$

В частности, таким образом определены степени идеала: $I,\ I^2, \ldots$.

Определение 6.11. Идеал $I \lhd \mathcal{R}$ называется *нильпотентным*, если $I^n = 0$ для некоторого $n \in \mathbb{N}$.

Определение 6.12. *Радикал* $J(\mathcal{R})$ конечного коммутативного кольца $\mathcal{R}$ — множество всех его нильпотентных элементов.

Лемма 6.13. $J(\mathcal{R})$ — нильпотентный идеал в $\mathcal{R}$.

◀ $J(\mathcal{R})$ — идеал в $\mathcal{R}$, поскольку если $r^n = 0, s^k = 0$, то

$$(r+s)^{n+k} =$$
$$= \sum_{i=0}^{n+k} C_{n+k}^i r^i s^{n+k-i} = \sum_{i=0}^{n} C_{n+k}^i r^i s^{n-i} s^k + \sum_{i=n+1}^{n+k} C_{n+k}^i r^n r^{i-n} s^{n+k-i} =$$
$$= 0 + 0 = 0,$$

и для любого $u \in \mathcal{R}$: $(ur)^n = u^n r^n = u^n 0 = 0$, т.е. $r + s, ur \in J(\mathcal{R})$.

В силу конечности $\mathcal{R}$ множество $J(\mathcal{R})$ тоже конечно. Поэтому существует $t \in \mathbb{N}$, что $a^t = 0$ для всех $a \in J(\mathcal{R})$ (берём максимум таких степеней по всем элементам радикала). Пусть $m = |J(\mathcal{R})|$. Тогда по принципу Дирихле в произведении любых $N = m(t-1) + 1$ элементов $x_1, \ldots, x_N \in J(\mathcal{R})$ хотя бы один элемент x_s повторяется по крайней мере t раз, что в силу коммутативности кольца означает,

что произведение $x_1 \cdots x_N = (x_s)^t \cdot a = 0a = 0$, где a — произведение оставшихся элементов. Откуда $J(\mathcal{R})^N = 0$. ▶

2°. Локальные кольца, эквивалентные определения.

Определение 6.14. Кольцо $\mathcal{R}$ называется *локальным*, если фактор-кольцо $\mathcal{R}/J(\mathcal{R})$ — поле.

Следующая теорема даёт четыре эквивалентных определения локального кольца.

Теорема 6.15. Следующие утверждения эквивалентны:
1) $\mathcal{R}$ — локальное кольцо;
2) в $\mathcal{R}$ ровно два идемпотента (0 и 1);
3) $\forall a \in \mathcal{R}$ один из элементов a либо $1-a$ обратим;
4) $\mathcal{R} = \mathcal{R}^* \cup J(\mathcal{R})$, где $\mathcal{R}^*$ — группа обратимых элементов кольца $\mathcal{R}$.

◀ "1)⇒ 2)" Допустим, что в $\mathcal{R}$ есть идемпотент e, отличный от 0 и 1. Тогда $1-e \neq 0, 1$ — тоже нетривиальный идемпотент. По определению $e, 1-e \notin J(\mathcal{R})$. В фактор-кольце $\mathcal{R}/J(\mathcal{R})$: $e+J(\mathcal{R}), 1-e+J(\mathcal{R})$ — ненулевые элементы, но $(e+J(\mathcal{R}))(1-e+J(\mathcal{R})) = 0+J(\mathcal{R})$. В поле $\mathcal{R}/J(\mathcal{R})$ нет делителей нуля, поэтому e или $1-e$ лежит в $J(\mathcal{R})$. Противоречие.

"2)⇒ 4)" Для произвольного $a \in \mathcal{R}$ по лемме 6.6 существует $k \in \mathbb{N}$, что a^k — идемпотент. По условию 2) возможны 2 случая: $a^k = 1$, либо $a^k = 0$. Если $a^k = 0$, то по определению $a \in J(\mathcal{R})$. Если $a^k = 1$, то $a \cdot a^{k-1} = 1$, т.е. $a^{k-1} = a^{-1}$ и $a \in \mathcal{R}^*$. Откуда $\mathcal{R} = \mathcal{R}^* \cup J(\mathcal{R})$.

"4)⇒ 3)" Для произвольного $a \in \mathcal{R}$, либо a сам обратим, либо $a \in J(\mathcal{R})$. Во втором случае $a^n = 0$ и $(1-a)(1+a+\cdots+a^{n-1}) = 1-a^n = 1$, $(1-a)^{-1} = 1+a+\cdots+a^{n-1}$, поэтому $1-a$ — обратимый элемент.

"3)⇒ 1)" Для произвольного $a \in \mathcal{R}$ один из элементов a либо $1-a$ обратим. Пусть $a \notin J(\mathcal{R})$. Тогда для некоторого $k \in \mathbb{N}$ $a^k = e$ — идемпотент. Единственный идемпотент в $J(\mathcal{R})$ — это 0, поскольку для идемпотента e и любого $k \in \mathbb{N}$: $e^k = e$, с другой стороны для $e \in J(\mathcal{R})$ существует $m \in \mathbb{N}$ $e^m = 0$, откуда $0 = e^m = e$. По условию $a^k \neq 0$, поэтому $e \notin J(\mathcal{R})$. Заметим, что если $e \neq 1$, то $e(1-e) = 0$ и e и $1-e$ — ненулевые делители нуля, следовательно, не могут быть обратимы. Противоречие с условием 3), значит, $e = 1$. Поэтому элемент $a+J(\mathcal{R})$ — обратим в фактор-кольце, т.е. в этом кольце любой ненулевой обратим и оно является полем. ▶

3°. Разложение конечного коммутативного кольца в прямую сумму локальных колец.

Теорема 6.16. Любое конечное коммутативное кольцо $\mathcal{R}$ с $1 \neq 0$ раскладывается в прямую сумму $\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$, где все $\mathcal{R}_i$ — локальные кольца.

◀ В $\mathcal{R}$ есть ПОМИ (например, из одного элемента 1). Возьмём среди них самую большую по числу элементов (такая существует в силу конечности $\mathcal{R}$) ПОМИ $e_1, \ldots, e_n$. $\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$ для $\mathcal{R}_i = \mathcal{R}e_i$.

Докажем, что для каждого $i = 1, \ldots, n$ кольцо $\mathcal{R}e_i$ локально. Допустим существует $e \in \mathcal{R}e_i$ — идемпотент и $e \neq 0, e_i$. Рассмотрим систему $e_1, \ldots, e_{i-1}, e, e_i - e, e_{i+1}, \ldots, e_n$. Имеем $e + (e_i - e) = e_i$, поэтому $e_1 + \ldots + e_{i-1} + e + e_i - e + e_{i+1} + \ldots + e_n = \sum\limits_{j=1}^{n} e_j = 1$. Также из условия $e \in \mathcal{R}e_i$ имеем $e = e_i e = e e_i$. Откуда $e(e_i - e) = 0$, $e e_j = e e_i e_j = 0$, $(e_i - e)e_j = 0 - 0 = 0$ для всех $j \neq i$. Получили бóльшую по числу элементов ПОМИ, противоречие. Таким образом, в кольце $\mathcal{R}e_i$ ровно два идемпотента и оно является локальным по условию (2) теоремы 6.15. ▶

Определение 6.17. Идемпотент $e \in \mathcal{R}$ называется *локальным идемпотентом*, если кольцо $\mathcal{R}e$ локально.

Следствие 6.18. Для произвольного конечного коммутативного кольца $\mathcal{R}$ с $1 \neq 0$ имеем $\mathcal{R}/J(\mathcal{R}) = \mathbb{F}_1 \oplus \ldots \oplus \mathbb{F}_n$, где все $\mathbb{F}_i$ — конечные поля.

◀ $\mathcal{R}/J(\mathcal{R}) = \bigoplus\limits_{i=1}^{n} (\mathcal{R}/J(\mathcal{R}))e_i$ по теореме 6.16. $(\mathcal{R}/J(\mathcal{R}))e_i$ — локальное кольцо с нулевым радикалом, поэтому оно само является полем. ▶

Лекция 7. Аннуляторы идеала в модуле и подмодуля в кольце. Лемма Накаямы. Радикал Джекобсона конечного коммутативного кольца и цоколь модуля, связь между ними. Системы образующих модуля.

Пусть $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$.

Определение 7.1. Внешняя *прямая сумма* $M_1 \oplus \ldots \oplus M_n$ $\mathcal{R}$-модулей $M_1, \ldots, M_n$ — множество всех строк $(m_1, \ldots, m_n)$, где $m_i \in M_i$ $\forall i \in \{1, \ldots, n\}$, с покомпонентными сложением и умножением на элементы кольца $\mathcal{R}$.

Предложение 7.2. Пусть $M_1, \ldots, M_n$— подмодули модуля M. Тогда следующие условия эквивалентны:
1) Если $x_1 + \ldots + x_n = 0$, где $x_i \in M_i$, $i = 1, \ldots, n$, то $x_1 = \ldots = x_n = 0$.
2) Для любого $i \in \{1, \ldots, n\}$:

$$M_i \cap (M_1 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_n) = 0.$$

Определение 7.3. Если для семейства подмодулей $M_1, \ldots, M_n$ модуля M выполнены условия предложения 7.2, то говорят, что это семейство образует *прямую сумму подмодулей*. В этом случае сумма данного семейства обозначается как прямая сумма: $M_1 \oplus \ldots \oplus M_n$. Подмодуль N модуля M называется *прямым слагаемым*, если существует подмодуль K модуля M, такой, что $M = N \oplus K$.

Определение 7.4. Пусть N — подмодуль правого $\mathcal{R}$-модуля M. Рассмотрим множество всех смежных классов $\{x + N : x \in M\}$ аддитивной группы модуля M по подгруппе N и зададим на этом множестве операции $(x + N) + (y + N) = (x + y) + N$, $(x + N)r = xr + N$ для любых $x, y \in M$ и $r \in \mathcal{R}$. Множество смежных классов, снабжённое этими операциями, оказывается правым $\mathcal{R}$-модулем. Этот модуль называется *фактор-модулем* модуля M по подмодулю N и обозначается M/N. Отображение $\pi : M \to M/N$, заданное равенством $\pi(x) = x + N$ для любого $x \in M$, называется *каноническим гомоморфизмом* модуля на фактор-модуль.

Определение 7.5. Модуль V называется *простым*, или *неприводимым*, если он содержит ровно два подмодуля (0 и V).

Определение 7.6. *Цоколем* модуля M называется сумма всех неприводимых подмодулей модуля M (обозначение $\mathrm{soc}M$). Если M не имеет простых подмодулей, то считаем $\mathrm{soc}M = 0$.

Определение 7.7. Модуль M называется *вполне приводимым*, если каждый подмодуль модуля M выделяется прямым слагаемым.

Лемма 7.8 (Лемма Накаямы)**.** Пусть M — правый $\mathcal{R}$-модуль. Если $MJ(\mathcal{R}) = M$, то $M = 0$.

◀ Пусть $MJ(\mathcal{R}) = M$. В этом случае $MJ(\mathcal{R})^2 = MJ(\mathcal{R}) = M$, и по индукции, $MJ(\mathcal{R})^n = M$ для всех $n \in \mathbb{N}$. Но по лемме 6.13 существует $n \in \mathbb{N}$, что $J(\mathcal{R})^n = 0$. Тогда $M = MJ(\mathcal{R})^n = 0$.▶

Лемма 7.9 (Лемма Накаямы, эквивалентная формулировка)**.** Пусть M — правый $\mathcal{R}$-модуль, $N \leq M$. Если $N + MJ(\mathcal{R}) = M$, то $N = M$.

◀ "$\Rightarrow$" Переходим к M/N. Имеем $M/N \cdot J(\mathcal{R}) = M/N$, тогда по лемме 7.8 выполнено $M/N = 0$, значит, $M = N$.

"$\Leftarrow$" Утверждение выполнено для всех модулей N. Возьмём $N = 0$. ▶

Предложение 7.10. Пусть $M \neq 0$ — конечный модуль. Тогда существуют неприводимые подмодули $V_1, \ldots, V_n \leq M$ такие, что

$$\mathrm{soc}M = V_1 \oplus \ldots \oplus V_n.$$

◀ В силу конечности существует ненулевой подмодуль $V \leq M$ с минимальным числом элементов. Условие минимальности в частности означает, что V — неприводимый модуль. Положим $V_1 = V$. Если $V = \mathrm{soc}M$, то всё готово, $\mathrm{soc}M = V_1$ — прямая сумма из одного слагаемого.

Иначе существует неприводимый модуль $V_2 \nsubseteq V = V_1$. Тогда $V_1 \cap V_2 \leq V_2$ и $V_1 \cap V_2 \neq V_2$, т.к. $V_2 \nsubseteq V_1$, значит, $V_1 \cap V_2 = 0$. Тогда $V_1 \oplus V_2 \leq \mathrm{soc}M$.

Аналогично предыдущему шагу имеем два варианта: либо $V_1 \oplus V_2 = \mathrm{soc}M$ и всё готово, либо существует неприводимый модуль $V_3 \nsubseteq V_1 \oplus V_2$. Во втором случае снова получаем прямую сумму $V_1 \oplus V_2 \oplus V_3$ и т.д. В силу конечности модуля M число шагов в этом процессе конечно, поэтому существует $n \in \mathbb{N}$, что $\mathrm{soc}M = V_1 \oplus \ldots \oplus V_n$.▶

Пусть M — правый $\mathcal{R}$-модуль.

Определение 7.11. Для $S \subseteq M$, $T \subseteq \mathcal{R}$ определим *аннуляторы*

$$\mathrm{ann}_{\mathcal{R}}(S) = \{r \in \mathcal{R} : \ Sr = 0\},$$

$$\mathrm{ann}_M(T) = \{m \in M : \ mT = 0\}.$$

По определению $\mathrm{ann}_{\mathcal{R}}(S) \lhd \mathcal{R}, \mathrm{ann}_M(T) \leq M$.

Отметим ещё некоторые свойства аннуляторов:

Предложение 7.12. Пусть M — правый $\mathcal{R}$-модуль, $S \subseteq M$, $T \subseteq \mathcal{R}$. Тогда
1) $S \subseteq \mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(S))$, $T \subseteq \mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(T))$;
2) если $N_1, N_2 \leq M$ и $N_1 \subseteq N_2$, то $\mathrm{ann}_{\mathcal{R}}(N_1) \supseteq \mathrm{ann}_{\mathcal{R}}(N_2)$, если $I_1, I_2 \lhd \mathcal{R}$ и $I_1 \subseteq I_2$, то $\mathrm{ann}_M(I_1) \supseteq \mathrm{ann}_M(I_2)$;
3) для $N \leq M$ и $I \lhd \mathcal{R}$ выполнены равенства:

$$\mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(N))) = \mathrm{ann}_{\mathcal{R}}(N),$$

$$\mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(I))) = \mathrm{ann}_M(I).$$

◀ 1) Пусть $s \in S$. Тогда $s \cdot \mathrm{ann}_{\mathcal{R}}(S) = 0$, следовательно, $s \in \mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(S))$. Аналогично, $T \subseteq \mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(T))$.

2) очевидно.

3) К $\mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(N)) \supseteq N$ применяем утверждение пункта 2): $\mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(N))) \subseteq \mathrm{ann}_{\mathcal{R}}(N)$. Обратное включение получается применением утверждения пункта 1) к $T = \mathrm{ann}_{\mathcal{R}}(N)$. Аналогично, применяя пункты 1) и 2), получаем, что $\mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(I))) = \mathrm{ann}_M(I)$.▶

Теорема 7.13. Пусть M — правый $\mathcal{R}$-модуль, $J(\mathcal{R})$ — радикал кольца $\mathcal{R}$. Тогда $\mathrm{soc}M = \mathrm{ann}_M(J(\mathcal{R}))$.

◀ Пусть $V \neq 0$ — неприводимый подмодуль модуля M. Докажем, что $V \subseteq \mathrm{ann}_M(J(\mathcal{R}))$. Имеем $VJ(\mathcal{R}) \leq V$. Если $VJ(\mathcal{R}) = 0$, то требуемое включение выполнено. Иначе, $VJ(\mathcal{R}) = V$. Тогда по лемме Накаямы (7.8) $V = 0$, противоречие. Таким образом, $\mathrm{soc}M \subseteq \mathrm{ann}_M(J(\mathcal{R}))$.

Обратно, пусть $N = \mathrm{ann}_M(J(\mathcal{R}))$. N превращается в модуль над кольцом $\mathcal{R}/J(\mathcal{R})$, если для $x \in N$ естественным образом положить $x(r + J(\mathcal{R})) = xr$. Согласно следствию 6.18, имеем $\bar{\mathcal{R}} = \mathcal{R}/J(\mathcal{R}) = \mathbb{F}_1 \oplus \ldots \oplus \mathbb{F}_n$, где все $\mathbb{F}_i$ — конечные поля, $\mathbb{F}_i \cong \bar{\mathcal{R}}e_i$, $e_1 + \ldots e_n = \bar{1}$, $e_i e_j = \bar{0}$, $\forall\ i \neq j$. Тогда $N = Ne_1 \oplus \ldots \oplus Ne_n$. Каждый модуль Ne_i является $\bar{\mathcal{R}}e_i$-модулем. Модуль над полем – это линейное пространство. Оно раскладывается в прямую сумму одномерных пространств (неприводимых модулей). Тогда Ne_i как сумма неприводимых модулей содержится в $\mathrm{soc}M$. Это верно для любого $i = 1, \ldots, n$. Откуда, $N \subseteq \mathrm{soc}M$. ▶

Определение 7.14. Пусть S — произвольное множество элементов правого модуля M над кольцом $\mathcal{R}$. Наименьший (по включению) подмодуль $\langle S\rangle_{\mathcal{R}}$ модуля M, содержащий множество S, называется *подмодулем, порождённым множеством* S. Аналогично определяется идеал $(T)_{\mathcal{R}}$, порождённый подмножеством T кольца $\mathcal{R}$. Если $N = \langle S\rangle_{\mathcal{R}}$, говорят также, что S — *система образующих подмодуля* N. Аналогично, если $I = (T)_{\mathcal{R}}$, то говорят, что T — *система образующих идеала* I.

Предложение 7.15. Пусть S — произвольное множество элементов правого модуля M над кольцом $\mathcal{R}$. Тогда

$$\langle S\rangle_{\mathcal{R}} = S\mathcal{R} = \{x_1r_1 + \ldots + x_nr_n : x_i \in S, r_i \in \mathcal{R}, i = 1,\ldots,n,\ n \geq 0\}.$$

Определение 7.16. Модуль, имеющий систему образующих из одного элемента, называется *циклическим* модулем. Идеал, имеющий систему образующих из одного элемента, называется *главным* идеалом. Модуль (идеал), имеющий конечную систему образующих, называется *конечно порождённым*. Для конечно порождённого модуля M через $\rho(M)$ обозначим минимальную мощность его системы образующих.

Из предложения 7.15 очевидно, что $|M| \leq |\mathcal{R}|^t$, где $t = \rho(M)$.

Определение 7.17. M — *свободный $\mathcal{R}$-модуль ранга* t, если у него существует линейно независимая над $\mathcal{R}$ система из t образующих.

Из определений очевидно следует

Предложение 7.18. M — свободный $\mathcal{R}$-модуль ранга t тогда и только тогда, когда $\rho(M) = t$ и $|M| = |\mathcal{R}|^t$.

По теореме 6.16 имеем $\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$, где все $\mathcal{R}_i$ — локальные кольца, $\mathcal{R}_i \cong \mathcal{R}e_i$. Тогда $M_{\mathcal{R}} = M_1 \oplus \ldots \oplus M_n$, где $M_s = Me_s$, $s = 1,\ldots,n$. Каждый модуль M_s является $\mathcal{R}_s$-модулем, поскольку $\mathcal{R}_s = \mathcal{R}e_s = e_s\mathcal{R}$.

Предложение 7.19. $\rho(M_{\mathcal{R}}) = \max\{\rho((M_s)_{\mathcal{R}_s}) : s \in \{1,\ldots,n\}\}$.

◀ Пусть $m_1,\ldots,m_r$ — система образующих модуля M. Тогда $m_1e_s,\ldots,m_re_s$ — образующие для $(M_s)_{\mathcal{R}_s}$. Потому $\rho(M) \geq \rho(M_s)$. Обратно, пусть $m_1^{(s)},\ldots,m_{r_s}^{(s)}$ — образующие $(M_s)_{\mathcal{R}_s}$, $s = 1,\ldots,n$. Положим $r = \max\{r_1,\ldots,r_n\}$ и дополним при необходимости все системы образующих нулями, чтобы считать, что $r = r_1 = \ldots = r_n$.

Тогда в M можно взять образующие $m_1 = m_1^{(1)} + \ldots + m_1^{(n)}, \ldots, m_r = m_r^{(1)} + \ldots + m_r^{(n)}$. ►

Обозначим $\widetilde{M} = M/MJ(\mathcal{R})$. Для $m \in M$ полагаем $\widetilde{m} = m + MJ(\mathcal{R}) \in \widetilde{M}$. По лемме Накаямы (7.8) если $M \neq 0$, то $\widetilde{M} \neq 0$. Если $\mathcal{R}$ — локальное кольцо, то фактор-кольцо $\overline{\mathcal{R}} = \mathcal{R}/J(\mathcal{R})$ — поле. Модуль $\widetilde{M}_{\mathcal{R}}$ превращается в пространство над $\overline{\mathcal{R}}$:

$$\forall \widetilde{m} \in \widetilde{M},\ \bar{\alpha} = \alpha + J(\mathcal{R}) \in \overline{\mathcal{R}} : \bar{\alpha}\widetilde{m} = \widetilde{m\alpha}.$$

При этом подмодули модуля $\widetilde{M}_{\mathcal{R}}$ и подпространства пространства ${}_{\overline{\mathcal{R}}}\widetilde{M}$ соответствуют друг другу.

Предложение 7.20. Если $\mathcal{R}$ —локальное кольцо, то $\rho(M_{\mathcal{R}}) = \dim_{\overline{\mathcal{R}}} \widetilde{M}$, и для любых $m_1, \ldots, m_t \in M$ равенства

$$M = \langle m_1, \ldots, m_t \rangle_{\mathcal{R}} \tag{7.1}$$

и

$$\widetilde{M} = {}_{\overline{\mathcal{R}}}\langle \widetilde{m_1}, \ldots, \widetilde{m_t} \rangle \tag{7.2}$$

эквивалентны.

◄ Равенство (7.2) равносильно условию $M = \langle m_1, \ldots, m_t \rangle_{\mathcal{R}} + J(\mathcal{R})M$. По лемме Накаямы 7.8 последнее равенство эквивалентно равенству (7.1).►

Предложение 7.21. Для модуля $M_{\mathcal{R}}$ над локальным кольцом $\mathcal{R}$ эквивалентны следующие утверждения:
1) $M_{\mathcal{R}}$ — неприводимый модуль;
2) $MJ(\mathcal{R}) = 0$ и $\dim_{\overline{\mathcal{R}}} \widetilde{M} = 1$;
3) $M_{\mathcal{R}} \cong \overline{\mathcal{R}}_{\mathcal{R}}$;
4) $|M| = |\overline{\mathcal{R}}|$.

◄ "1)⇒ 2)" Поскольку $M_{\mathcal{R}}$ — неприводимый модуль, то $M \neq 0$. Рассмотрим подмодуль $MJ(\mathcal{R})$ модуля M. По лемме Накаямы (7.8) $M \neq MJ(\mathcal{R})$. Но тогда из неприводимости M следует, что $MJ(\mathcal{R}) = 0$. В силу соответствия подмодулей модуля $\widetilde{M}_{\mathcal{R}}$ и подпространств пространства ${}_{\overline{\mathcal{R}}}\widetilde{M}$, пространство ${}_{\overline{\mathcal{R}}}\widetilde{M}$ не имеет нетривиальных подпространств, что возможно, только если $\dim_{\overline{\mathcal{R}}} \widetilde{M} = 1$.

Импликация "2)⇒ 3)" следует из предложения 7.20.

"3)⇒ 4)" Очевидно.

“4)$\Rightarrow$ 1)” Пусть $N \leq M$. Из предложения 7.20 следует, что если $N \neq 0$, то $|N| \geq |\overline{\mathcal{R}}| = q$. Значит, $|N| = |M|$, т.е. $N = M$, следовательно, модуль M является неприводимым. ►

Лекция 8. Модуль характеров конечного модуля. Инъективные модули. Критерий Бэра. Инъективность модуля характеров.

1°. Модуль характеров.

Определение 8.1. *Группой характеров* модуля M назовём абелеву группу $M^* = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$.

Предложение 8.2. 1) Имеет место изоморфизм групп $(M^*, +) \cong (M, +)$.
2) $\forall b \in M \setminus \{0\}\ \exists \chi \in M^* :\ \chi(b) \neq 0$.

◀ 1. Разложим абелеву группу M в прямую сумму примарных циклических подгрупп: $M = \langle a_1 \rangle_{n_1} \oplus \ldots \oplus \langle a_t \rangle_{n_t}$. Рассмотрим характер χ_i модуля M такой, что $\chi_i(a_j) = \delta_{ij} \dfrac{1}{n_i}$, здесь δ_{ij} — символ Кронекера, $i \in \{1, \ldots, t\}$. Тогда $n_i \chi_i \equiv 0$, $m\chi_i(a_i) = \dfrac{m}{n_i} \neq 0$, $1 \leq m < n_i$, поэтому $\mathrm{ord}(\chi_i) = n_i = \mathrm{ord}(a_i)$. Поскольку любой характер $\chi \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ задаётся образами порождающих элементов a_i, $i \in \{1, \ldots, t\}$, то $M^* \cong \langle \chi_1 \rangle_{n_1} \oplus \ldots \oplus \langle \chi_t \rangle_{n_t} \cong M$.

2. Если $b \in M \setminus \{0\}$, то в разложении $b = b_1 + \ldots + b_t$, $b_i \in \langle a_i \rangle_{n_i}$, хотя бы один элемент b_i отличен от нуля, $i \in \{1, \ldots, t\}$. В этом случае $b_i = ma_i$, где $1 \leq m < n_i$. Тогда в качестве искомого характера χ можно выбрать χ_i. Действительно, $\chi_i(b) = \chi_i(b_i) = \dfrac{m}{n_i} \neq 0$. ▶

Определение 8.3. Если M — левый $\mathcal{R}$-модуль, то определим произведение произвольного характера $\chi \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ на элемент r кольца $\mathcal{R}$ справа как характер χr, заданный формулой

$$\forall x \in M, \quad (\chi r)(x) = \chi(rx). \tag{8.1}$$

Легко проверить, что получается структура правого $\mathcal{R}$-модуля на группе $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ (заметим, что если $\chi \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, $r, s \in R$ и $x \in M$, то $((\chi r)s)(x) = (\chi r)(sx) = \chi(rsx) = (\chi(rs))(x)$). Полученный модуль будем называть *модулем характеров* модуля M и обозначим через M^*.

Аналогично, если M — правый $\mathcal{R}$-модуль, то на группе его характеров вводится умножение слева на элементы кольца $\mathcal{R}$ формулой

$$\forall x \in M, \quad (r\chi)(x) = \chi(xr), \tag{8.2}$$

которое определяет структуру левого $\mathcal{R}$-модуля на группе $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ (заметим, что $(r(s\chi))(x) = (s\chi)(xr) = \chi(xrs) = ((rs)\chi)(x)$).

Этот модуль мы также будем называть *модулем характеров* и обозначать через M^*.

Предложение 8.2 не обобщается в общем случае до утверждения об изоморфизме модулей M и M^*, однако справедлива

Теорема 8.4. Для любого модуля M существует канонический изоморфизм $\mathcal{R}$-модулей ${}_{\mathcal{R}}M \cong {}_{\mathcal{R}}M^{**}$.

◀ Для любого $m \in M$ определим гомоморфизм абелевых групп $\varphi_m : M^* \to \mathbb{Q}/\mathbb{Z}$ формулой $\varphi_m(\chi) = \chi(m)$. Заметим, что отображение $m \mapsto \varphi_m$ — гомоморфизм левых $\mathcal{R}$-модулей. Действительно, для любого $r \in \mathcal{R}$ имеем

$$\varphi_{(rm)}(\chi) = \chi(rm) \overset{(8.1)}{=} (\chi r)(m) = \varphi_m(\chi r) = (r\varphi_m)(\chi).$$

Если $m \neq 0$, то согласно пункту 2 предложения 8.2 существует характер $\chi \in M^*$ такой, что $\chi(m) \neq 0$. Следовательно, $\varphi_m \in M^{**} \setminus \{0\}$ и гомоморфизм $m \mapsto \varphi_m$ — мономорфизм.

В силу пункта 1 предложения 8.2 также имеем $|M| = |M^*| = |M^{**}|$. Следовательно, мономорфизм $m \mapsto \varphi_m$ есть изоморфизм. ▶
Для правого модуля M верно аналогичное утверждение.

Предложение 8.5. Если $M = M_1 \oplus M_2$ — прямая сумма модулей, то существует канонический изоморфизм $\mathcal{R}$-модулей $M^* \cong M_1^* \oplus M_2^*$.

◀ Произвольному элементу $\overrightarrow{\chi} = (\chi_1, \chi_2) \in M_1^* \oplus M_2^*$ сопоставим отображение $\chi_m : M \to \mathbb{Q}/\mathbb{Z}$, определённое на элементе $\overrightarrow{m} = (m_1, m_2) \in M_1 \oplus M_2$ правилом $\chi_m(\overrightarrow{m}) = \chi_1(m_1) + \chi_2(m_2)$. По построению очевидно, что χ_m есть характер группы $(M, +)$, и различным элементам из $M_1^* \oplus M_2^*$ соответствуют разные характеры. Поскольку в силу пункта 1 предложения 8.2 $|M_1^* \oplus M_2^*| = |M| = |M^*|$, то имеет место изоморфизм групп $M^* \cong M_1^* \oplus M_2^*$. Осталось доказать, что имеет место гомоморфизм модулей. Действительно, для любого $r \in \mathcal{R}$ имеем

$$(\overrightarrow{\chi}r)(\overrightarrow{m}) \overset{(8.1)}{=} \chi_m(r\overrightarrow{m}) = \chi_1(rm_1) + \chi_2(rm_2) = (\chi_1 r, \chi_2 r)(\overrightarrow{m}).$$

▶

2°. Инъективные модули. Критерий Бэра. Инъективность модуля характеров.

Определение 8.6. Левый $\mathcal{R}$-модуль M называется *инъективным*, если для произвольного левого $\mathcal{R}$-модуля L и для любого его подмодуля K каждый гомоморфизм $\varphi : {}_{\mathcal{R}}K \to {}_{\mathcal{R}}M$ может быть продолжен до гомоморфизма ${}_{\mathcal{R}}L \to {}_{\mathcal{R}}M$.

Теорема 8.7 (Критерий Бэра)**.** Следующие условия эквивалентны:
1) левый $\mathcal{R}$-модуль M инъективен;
2) для любого идеала $I \lhd \mathcal{R}$ и любого гомоморфизма $\varphi : {}_{\mathcal{R}}I \to {}_{\mathcal{R}}M$ существует такой элемент $m \in M$, что $\varphi(x) = xm$ для любого $x \in I$ (т.е. есть гомоморфизм $\psi : {}_{\mathcal{R}}\mathcal{R} \to {}_{\mathcal{R}}M$, продолжающий φ).

◀ "1)⇒ 2)" Пусть левый $\mathcal{R}$-модуль M инъективен, $I \lhd \mathcal{R}$. По определению существует такой гомоморфизм $\psi : \mathcal{R} \to M$, что $\varphi(x) = \psi(x) = \psi(1 \cdot x) = \psi(1)x$ для любого $x \in I$. Значит, можно положить $m = \psi(1)$.

"2)⇒ 1)" Мы проверим выполнение свойства инъективности для случая, когда модуль L — конечный. Пусть $\mathcal{S}$ — множество всех пар $(\widetilde{K}, \widetilde{\varphi})$, где $\widetilde{K}$ — подмодуль модуля L, $\widetilde{\varphi}$ — гомоморфизм $\widetilde{K}$ в M, продолжающий φ. Это множество непусто — в нём содержится пара (K, φ). В силу конечности среди всех таких пар можно выбрать такую пару $(K_{\max}, \varphi_{\max})$, в которой $\widetilde{K}$ — максимально возможный. Допустим, что $K_{\max} \neq L$ и выберем произвольный элемент $b \in L \setminus K_{\max}$. Рассмотрим идеал $I = \{r \in \mathcal{R} : rb \in K_{\max}\}$ (I выдерживает умножение сложение и умножение на элементы кольца, поскольку $K_{\max}$ — модуль). Тогда отображение $\theta(r) = \varphi_{\max}(rb)$ есть гомоморфизм $\theta : I \to M$. Выберем для него элемент $m \in M$ по условию 2 теоремы: $\theta(x) = xm$ для любого $x \in I$. Рассмотрим модуль $\overline{K} = K_{\max} + \mathcal{R}b$. Определим $\overline{\varphi} : \overline{K} \to M$ правилом $\overline{\varphi}(x + rb) = \varphi_{\max}(x) + rm$ для любых $x \in K_{\max}$ и $r \in \mathcal{R}$. Проверим, что отображение $\overline{\varphi}$ определено корректно. Действительно, если $x_1 + r_1 b = x_2 + r_2 b$, то $r_2 - r_1 \in I$ и $\varphi_{\max}(x_1) - \varphi_{\max}(x_2) = \varphi_{\max}(b(r_2 - r_1)) = \theta(r_2 - r_1) = r_2 m - r_1 m$, откуда $\varphi_{\max}(x_1) + r_1 m = \varphi_{\max}(x_2) + r_2 m$. Ясно, что $\overline{\varphi}|_{K_{\max}} = \varphi_{\max}$, поэтому пара $(\overline{K}, \overline{\varphi})$ принадлежит $\mathcal{S}$, но это противоречит максимальности модуля $K_{\max}$. ►
Доказательство обратной импликации в общем случае требует применения леммы Цорна.

Следствие 8.8. Абелева группа A (т.е. модуль над кольцом $\mathbb{Z}$) инъективна тогда и только тогда, когда она *делима*, т.е. для любого

$a \in A$ и любого $n \in \mathbb{Z} \setminus \{0\}$ существует такой элемент $x \in A$, что $a = nx$.

◀ Достаточно показать, что выполнение критерия Бэра для группы A равносильно делимости. Но любой идеал кольца $\mathbb{Z}$ — главный, т.е. имеет вид $I = n\mathbb{Z}$, а любой гомоморфизм $f : I \to A$ имеет вид $f(nz) = f(n)z$ для любого $z \in \mathbb{Z}$. Полагая $f(n) = a$, получаем $nm = a$ для элемента m из условия 2 теоремы 8.7. Случай $n = 0$ тривиален. ▶

Теорема 8.9. Левый модуль $(\mathcal{R}_\mathcal{R})^*$ инъективен.

◀ Пусть I — идеал кольца $\mathcal{R}$ и $f : I \to (\mathcal{R}_\mathcal{R})^*$ — гомоморфизм. Определим гомоморфизм абелевых групп $\omega : I \to \mathbb{Q}/\mathbb{Z}$ формулой $\omega(x) = f(x)(1)$. В силу делимости группы $\mathbb{Q}/\mathbb{Z}$, существует характер $\tilde{\omega} : \mathcal{R} \to \mathbb{Q}/\mathbb{Z}$, совпадающий с ω на I.

Теперь для любого $a \in I$ и любого $x \in \mathcal{R}$ имеем

$$(a\tilde{\omega})(x) \overset{(8.2)}{=} \tilde{\omega}(xa) \overset{xa \in I}{=} \omega(xa) = f(xa)(1) =$$
$$= (xf(a))(1) \overset{(8.2)}{=} f(a)(1x) = f(a)(x).$$

Значит, в силу произвольности $x \in \mathcal{R}$, $f(a) = a\tilde{\omega}$, и можно применить критерий Бэра. ▶

Лекция 9. Квазифробениусов модуль, существование и единственность с точностью до изоморфизма.

1°. Квазифробениусов модуль, существование.

Пусть M — левый $\mathcal{R}$-модуль. Для $S \subseteq M$, $T \subseteq \mathcal{R}$ напомним *аннуляторы*

$$\operatorname{ann}_{\mathcal{R}}(S) = \{r \in \mathcal{R} : \ rS = 0\},$$

$$\operatorname{ann}_{M}(T) = \{m \in M : \ Tm = 0\},$$

и их свойства $S \subseteq \operatorname{ann}_M(\operatorname{ann}_{\mathcal{R}}(S))$, $T \subseteq \operatorname{ann}_{\mathcal{R}}(\operatorname{ann}_M(T))$.

Определение 9.1. Модуль M называется *квазифробениусовым*, или QF-*модулем*, если для всех $I \lhd \mathcal{R}$ и $K \leq M$ имеют места равенства

$$K = \operatorname{ann}_M(\operatorname{ann}_{\mathcal{R}}(K)), \ I = \operatorname{ann}_{\mathcal{R}}(\operatorname{ann}_M(I)).$$

В этой ситуации модуль $K \leq {}_{\mathcal{R}}M$ также можно рассматривать как модуль над факторкольцом $\widehat{\mathcal{R}} = \mathcal{R}/\operatorname{ann}_{\mathcal{R}}(K)$, полагая $\widehat{r}m = rm$ для $m \in K$ и $\widehat{r} = r + \operatorname{ann}_{\mathcal{R}}(K) \in \widehat{\mathcal{R}}$. Аналогично модуль $\operatorname{ann}_M(I) \leq {}_{\mathcal{R}}M$ можно рассматривать как модуль над факторкольцом $\mathcal{R}/I$.

Предложение 9.2. Пусть ${}_{\mathcal{R}}M$ — QF-модуль, $I \lhd \mathcal{R}$ и $K \leq M$. Тогда
1) K — QF-модуль над факторкольцом $\widehat{\mathcal{R}} = \mathcal{R}/\operatorname{ann}_{\mathcal{R}}(K)$.
2) $\operatorname{ann}_M(I)$ — QF-модуль над факторкольцом $\mathcal{R}/I$.

◀ 1) Пусть $K' \leq {}_{\widehat{\mathcal{R}}}K$. Рассмотрим $\widehat{B} = \operatorname{ann}_{\widehat{\mathcal{R}}}(K')$. Имеем $\widehat{B} = B/\operatorname{ann}_{\mathcal{R}}(K)$ для $B = \operatorname{ann}_{\mathcal{R}}(K')$. Далее переходим к рассмотрению $\operatorname{ann}_K(\widehat{B})$. По определению имеем

$$\operatorname{ann}_K(\widehat{B}) = \left\{m \in K : \widehat{B}m = 0\right\} = \{m \in K : Bm = 0\} =$$
$$= \operatorname{ann}_K(B) = K \cap \operatorname{ann}_M(B) = K \cap K' = K'.$$

Использованное здесь равенство $\operatorname{ann}_M(B) = K'$ верно в силу условия, что модуль M — квазифробениусов. Таким образом мы получили, что

$$\operatorname{ann}_K(\operatorname{ann}_{\widehat{\mathcal{R}}}(K')) = K'.$$

Также доказывается равенство $\operatorname{ann}_{\widehat{\mathcal{R}}}(\operatorname{ann}_K(\widehat{B})) = \widehat{B}$ для произвольного идеала $\widehat{B} \lhd \widehat{\mathcal{R}}$.

Утверждение 2) доказывается аналогично. ►

Следующая теорема показывает существование квазифробениусова модуля.

Теорема 9.3. Модуль ${}_{\mathcal{R}}\mathcal{R}^*$ характеров модуля $\mathcal{R}_{\mathcal{R}}$ является QF-модулем.

◄ 1) Рассмотрим идеал $I \lhd \mathcal{R}$ и его аннулятор $K = \mathrm{ann}_{\mathcal{R}^*}(I) = \{\chi \in \mathcal{R}^* : I\chi = 0\}$. Поскольку для $r, s \in \mathcal{R}$ $(r\chi)(s) = \chi(rs)$, то из условия $\chi \in K$, т.е. $I\chi = 0$, получаем, что $\chi(rs) = 0$ для $r \in I$. Подставляя $s = 1$, получаем $\chi(r) = 0$. Значит, K — это те характеры $\chi \in \mathcal{R}^*$, что $I \subseteq \ker\chi$. Такие характеры корректно рассматривать как характеры факторгруппы $\widehat{\mathcal{R}} = \mathcal{R}/I$. При этом K — множество всех характеров группы $\widehat{\mathcal{R}}$.

Нам нужно доказать, что $\mathrm{ann}_{\mathcal{R}}(K) = I$. Включение $I \subseteq \mathrm{ann}_{\mathcal{R}}(K)$ всегда выполнено. Проверим, что $\mathrm{ann}_{\mathcal{R}}(K) \subseteq I$. Пусть $r \in \mathrm{ann}_{\mathcal{R}}(K)$. Тогда элемент $\widehat{r} = r + I \in \widehat{\mathcal{R}}$ аннулируется любым характером из K. Согласно утверждению (2) предложения 8.2 это означает, что $\widehat{r} = 0$, т.е. $r \in I$ и $\mathrm{ann}_{\mathcal{R}}(K) \subseteq I$.

2) Рассмотрим подмодуль $K \leq {}_{\mathcal{R}}\mathcal{R}^*$ и его аннулятор $I = \mathrm{ann}_{\mathcal{R}}(K)$. По теореме 8.4 о каноническом изоморфизме отождествим $\mathcal{R}$ с модулем характеров $\mathcal{R}^{**}$. Тогда I – это множество всех характеров модуля $\mathcal{R}^*$, аннулирующих K, поэтому также как и в пункте (1) получаем, что $\mathrm{ann}_{\mathcal{R}^*}(I) = K$. ►

2°. Квазифробениусов модуль, единственность.

Сперва сделаем редукцию к случаю локальных колец.

По теореме 6.16 имеем $\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$, где все $\mathcal{R}_i$ — локальные кольца, $\mathcal{R}_i \cong \mathcal{R}e_i$. Тогда ${}_{\mathcal{R}}M = M_1 \oplus \ldots \oplus M_n$, где $M_s = e_sM$ — $\mathcal{R}_s$-модуль, $s = 1, \ldots, n$.

Предложение 9.4. В вышеозначенных обозначениях ${}_{\mathcal{R}}M$ — QF-модуль тогда и только тогда, когда ${}_{\mathcal{R}_1}M_1, \ldots, {}_{\mathcal{R}_n}M_n$ есть QF-модули.

◄ Произвольный подмодуль $K \leq {}_{\mathcal{R}}M$ имеет разложение $K = K_1 \oplus \ldots \oplus K_n$, где $K_s = e_sK \leq {}_{\mathcal{R}_s}M_s$. Имеем

$$\mathrm{ann}_{\mathcal{R}}(K) = \mathrm{ann}_{\mathcal{R}_1}(K_1) \oplus \ldots \oplus \mathrm{ann}_{\mathcal{R}_n}(K_n)$$

(действительно, $0 = rK = (re_1 + \ldots + re_n)K = re_1K_1 + \ldots + re_nK_n \Leftrightarrow re_i \in \mathrm{ann}_{\mathcal{R}_i}(K_i)$) и

$$\mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(K)) = \mathrm{ann}_{M_1}(\mathrm{ann}_{\mathcal{R}_1}(K_1)) \oplus \ldots \oplus \mathrm{ann}_{M_n}(\mathrm{ann}_{\mathcal{R}_n}(K_n)).$$

Откуда равенство $\mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(K)) = K$ эквивалентно системе равенств $\mathrm{ann}_{M_s}(\mathrm{ann}_{\mathcal{R}_s}(K_s)) = K_s$, $s = 1, \ldots, n$. Аналогично, произвольный идеал $I \lhd \mathcal{R}$ раскладывается в сумму $I = I_1 \oplus \ldots \oplus I_n$, $I_s = e_s I \lhd \mathcal{R}_s$. Поэтому равенство $\mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(I)) = I$ эквивалентно системе равенств $\mathrm{ann}_{\mathcal{R}_s}(\mathrm{ann}_{M_s}(I_s)) = I_s$, $s = 1, \ldots, n$. ►

Отметим следующее полезное свойство: подмодули QF-модуля, имеющие одинаковые аннуляторы, равны. Действительно, если $\mathrm{ann}_{\mathcal{R}}(K) = \mathrm{ann}_{\mathcal{R}}(K')$, то

$$K = \mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(K)) = \mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(K')) = K'.$$

Аналогично, идеалы кольца, имеющие одинаковые аннуляторы в QF-модуле, равны (если $\mathrm{ann}_M(I) = \mathrm{ann}_M(I')$, то; $I = \mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(I)) = \mathrm{ann}_{\mathcal{R}}(\mathrm{ann}_M(I')) = I'$).

Модуль ${}_{\mathcal{R}}M$ называется *точным*, если $\mathrm{ann}_{\mathcal{R}}(M) = 0$. Произвольный QF-модуль M является точным, поскольку $M = \mathrm{ann}_M(\mathrm{ann}_{\mathcal{R}}(M)) = \mathrm{ann}_M(0)$, а значит, $\mathrm{ann}_{\mathcal{R}}(M) = 0$.

Для точного модуля над локальным кольцом свойство быть QF-модулем связано с его цоколем. Вспомним, что $\mathrm{soc}M = \mathrm{ann}_M(J(\mathcal{R}))$, поэтому как отмечено выше для произвольного идеала I и его аннулятора, $\mathrm{soc}M$ можно рассматривать как модуль над факторкольцом $\overline{\mathcal{R}} = \mathcal{R}/J(\mathcal{R})$, что в случае локального кольца означает пространство над полем.

Теорема 9.5. Для точного модуля ${}_{\mathcal{R}}M$ над локальным кольцом $\mathcal{R}$ эквивалентны следующие условия:
1) ${}_{\mathcal{R}}M \cong {}_{\mathcal{R}}\mathcal{R}^*$;
2) M — QF-модуль;
3) $\mathrm{soc}M$ — циклический подмодуль в M;
4) $\dim_{\overline{\mathcal{R}}} \mathrm{soc}M = 1$;
5) $\mathrm{soc}M$ — единственный минимальный (неприводимый) подмодуль модуля M;
6) модуль M содержит единственный минимальный подмодуль.

◄ Импликация "1)⇒ 2)" есть утверждение теоремы 9.3.

"2)⇒ 3)" Пусть $a \in \mathrm{soc}M \setminus \{0\}$. Имеем $J(\mathcal{R}) \subseteq \mathrm{ann}_{\mathcal{R}}(\mathcal{R}a) \neq \mathcal{R}$ (например, $1 \notin \mathrm{ann}_{\mathcal{R}}(\mathcal{R}a)$). С другой стороны, в локальном кольце любой элемент вне радикала обратим, а идеал, содержащий обратимый элемент, содержит и единицу кольца, т.е. это всё кольцо. Поэтому $J(\mathcal{R})$ — максимальный идеал, т.е. между $J(\mathcal{R})$ и $\mathcal{R}$ нет других идеалов. Следовательно, $\mathrm{ann}_{\mathcal{R}}(\mathcal{R}a) = J(\mathcal{R}) = \mathrm{ann}_{\mathcal{R}}(\mathrm{soc}M)$. Отку-

да пользуясь свойством QF-модуля, заключаем, что $\mathrm{soc}M = \mathcal{R}a$ — циклический модуль.

"3)$\Rightarrow$ 4) $\Rightarrow$ 5) $\Rightarrow$ 6)" следует из предложений 7.20 и 7.21.

"6)$\Rightarrow$ 1)" Пусть K — единственный минимальный подмодуль модуля M. Тогда в силу минимальности он не содержит собственных подмодулей, т.е. K — неприводимый модуль. Согласно предложению 7.21 все неприводимые $\mathcal{R}$-модули изоморфны, поэтому существует вложение $\varphi : {}_{\mathcal{R}}K \to {}_{\mathcal{R}}\mathcal{R}^*$. В силу инъективности модуля характеров (теорема 8.9) вложение φ может быть продолжено до гомоморфизма $\psi : {}_{\mathcal{R}}M \to {}_{\mathcal{R}}\mathcal{R}^*$. Рассмотрим ядро $\ker\psi$. Если $\ker\psi \neq 0$, то из условия 6) мы получим, что $K \subseteq \ker\psi$, противоречие с тем, что ψ на K совпадает с φ. Следовательно, $\ker\psi = 0$, и ψ — вложение. Допустим, что $\psi(M) \neq \mathcal{R}^*$. Поскольку по теореме 9.3 $\mathcal{R}^*$ – QF-модуль, то $\mathrm{ann}_{\mathcal{R}}(\psi(M)) \neq \mathrm{ann}_{\mathcal{R}}(\mathcal{R}^*) = 0$. С другой стороны, т.к. ψ— вложение, то $\mathrm{ann}_{\mathcal{R}}(\psi(M)) = \mathrm{ann}_{\mathcal{R}}(M)$. Условие $\mathrm{ann}_{\mathcal{R}}(M) \neq 0$ противоречит точности модуля M. Следовательно, $\psi(M) = \mathcal{R}^*$ и ψ — искомый изоморфизм.►

Теорема 9.6. Любой QF-модуль над конечным коммутативным кольцом $\mathcal{R}$ с единицей изоморфен модулю характеров ${}_{\mathcal{R}}\mathcal{R}^*$.

◄ Следует из предложения 9.4, утверждений 1) и 2) теоремы 9.5 и предложения 8.5.►

Следствие 9.7. Любой QF-модуль над конечным коммутативным кольцом $\mathcal{R}$ с единицей инъективен.

Лекция 10. Характеризация квазифробениусовых модулей с помощью различающих характеров.

Пусть M — левый $\mathcal{R}$-модуль. Договоримся при необходимости рассматривать M и как правый модуль, полагая $rm = mr$ для любых $r \in \mathcal{R}$, $m \in M$.

Определение 10.1. Назовём модуль M *различимым*, если существует характер $\chi \in M^*$, не равный тождественно нулю ни на каком ненулевом подмодуле модуля M. Такой характер χ назовём *различающим* для M.

Следующая лемма даёт эквивалентное определение различающего характера, из которого более понятен сам термин "различающий".

Лемма 10.2. Характер $\chi \in M^*$ является различающим тогда и только тогда, когда

$$\forall a, b \in M,\ a \neq b,\ \exists r \in \mathcal{R}:\ \chi(ra) \neq \chi(rb).$$

◀ "⇒" Пусть χ — различающий характер и $a, b \in M$, $a \neq b$. Рассмотрим ненулевой подмодуль $\mathcal{R}(a-b) \leq M$. Имеем $\chi(\mathcal{R}(a-b)) \neq 0$, значит, существует элемент $r \in \mathcal{R}$ такой, что $\chi(r(a-b)) \neq 0$. Следовательно, $\chi(ra) \neq \chi(rb)$ (по свойству гомоморфизма).

"⇐" Пусть $K \leq M$ — произвольный ненулевой подмодуль. Существует $a \in K \setminus \{0\}$. По условию существует элемент $r \in \mathcal{R}$ такой, что $\chi(ra) \neq \chi(r0) = 0$. Значит, $\chi(K) \neq 0$. ▶

Лемма 10.3. QF-модуль ${}_{\mathcal{R}}M$ является различимым.

◀ По теореме 9.6 можно считать, что $M = \mathcal{R}^*$. Тогда в силу теоремы 8.4 существует канонический изоморфизм $\mathcal{R}$-модулей $\varphi : {}_{\mathcal{R}}\mathcal{R} \to {}_{\mathcal{R}}\mathcal{R}^{**} = {}_{\mathcal{R}}M^*$, который ставит в соответствие элементу $r \in \mathcal{R}$ характер $\varphi(r) : \mathcal{R}^* \to \mathbb{Q}/\mathbb{Z}$, действующий на элементе $\chi \in \mathcal{R}^*$ по правилу $\varphi(r)(\chi) = \chi(r)$. Покажем, что характер $\varphi(1)$ является различающим для $\mathcal{R}^*$. Действительно, если $\chi, \psi \in \mathcal{R}^*$, $\chi \neq \psi$, то $\chi(r) \neq \psi(r)$ для некоторого $r \in \mathcal{R}$. Это означает, что $\varphi(1)(r\chi) \neq \varphi(1)(r\psi)$. Согласно лемме 10.2 получаем, что $\varphi(1)$ — различающий характер для модуля ${}_{\mathcal{R}}M$. ▶

Заметим, что в предыдущем доказательстве вместо 1 можно было взять любой обратимый элемент u кольца $\mathcal{R}$, характер $\varphi(u)$ также будет различающим.

Покажем, что верно обратное утверждение к лемме 10.3.

Сперва сделаем редукцию к случаю локальных колец.

По теореме 6.16 имеем $\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n$, где все $\mathcal{R}_i$ — локальные кольца, $\mathcal{R}_i \cong \mathcal{R}e_i$. Тогда ${}_{\mathcal{R}}M = M_1 \oplus \ldots \oplus M_n$, где $M_s = e_s M$ — $\mathcal{R}_s$-модуль, $s = 1, \ldots, n$.

Лемма 10.4. В вышеозначенных обозначениях модуль ${}_{\mathcal{R}}M$ различим тогда и только тогда, когда все модули ${}_{\mathcal{R}_1}M_1, \ldots, {}_{\mathcal{R}_n}M_n$ различимы.

◀ "$\Rightarrow$" Пусть χ — различающий характер модуля M. Поскольку произвольный подмодуль K_s модуля ${}_{\mathcal{R}_s}M_s$ является подмодулем модуля ${}_{\mathcal{R}}M$, то на ненулевом подмодуле $\chi(K_s) \neq 0$. Тогда ограничение χ на M_s будет искомым различающим характером модуля ${}_{\mathcal{R}_s}M_s$.

"$\Leftarrow$" Пусть все модули ${}_{\mathcal{R}_1}M_1, \ldots, {}_{\mathcal{R}_n}M_n$ различимы, $\chi_1, \ldots, \chi_n$ — их различающие характеры. Определим характер χ модуля M следующим образом: для произвольного элемента $a \in M$ берём его разложение $a = a_1 + \ldots + a_n$, $a_s \in M_s$, соответствующее разложению M в прямую сумму и полагаем $\chi(a) = \chi_1(a_1) + \ldots + \chi_n(a_n) \in \mathbb{Q}/\mathbb{Z}$. Из построения очевидно, что полученное отображение будет характером модуля M. Докажем, что он будет различающим. Пусть $K \leq M$, $K \neq 0$. В этом случае найдётся такой индекс $s \in \{1, \ldots, n\}$, что $K_s = e_s K \neq 0$. Тогда из условия, что K_s — ненулевой подмодуль модуля M_s, заключаем, что найдётся элемент $a_s \in K_s$, для которого $\psi_s(a_s) \neq 0$. Рассматривая a_s как элемент модуля K, получаем $\chi(a_s) = \chi_s(a_s) \neq 0$, т.е. $\chi(K) \neq 0$.▶

Лемма 10.5. Пусть ${}_{\mathcal{R}}M$ — точный модуль над локальным кольцом $\mathcal{R}$. Вспомним, что $\mathrm{soc}M = \mathrm{ann}_M(J(\mathcal{R}))$ и $\mathrm{soc}M$ можно рассматривать как модуль над факторкольцом $\overline{\mathcal{R}} = \mathcal{R}/J(\mathcal{R})$, что в случае локального кольца означает пространство над конечным полем. Обозначим $|\overline{\mathcal{R}}| = q = p^r$. Пусть $u_1, \ldots, u_r$ — произвольный базис поля $\overline{\mathcal{R}}$ над его простым подполем $\mathbb{F}_p$. Для произвольной подгруппы $H < (\mathrm{soc}M, +)$ обозначим через $L(H)$ сумму всех подпространств пространства ${}_{\overline{\mathcal{R}}}\mathrm{soc}M$, содержащихся в H, другими словами самое большое подпространство, содержащееся в H. Тогда $L(H) = \bigcap\limits_{i=1}^{r} u_i^{-1} H$.

◀ Покажем, что $L(H) = \bigcap\limits_{i=1}^{r} u_i^{-1} H$. Пусть $a \in L(H)$. По построению, это равносильно тому, что $\overline{\mathcal{R}}a \subseteq H$. В частности, для всех $i = 1, \ldots, r$

имеем $u_i a \in H$ и $a \in u_i^{-1}G$. Таким образом, $L(H) \subseteq \bigcap\limits_{i=1}^{r} u_i^{-1}H$. Наоборот, если $a \in \bigcap\limits_{i=1}^{r} u_i^{-1}H$, то $u_1 a, \ldots, u_r a \in H$. Поскольку H — группа, то $(\gamma_1 u_1 + \ldots + \gamma_r u_r)a \in H$ для всех $\gamma_1, \ldots, \gamma_r \in \mathbb{F}_p$. Вспоминая, что $u_1, \ldots, u_r$ — базис $\overline{\mathcal{R}}$ над $\mathbb{F}_p$, заключаем, что $\overline{\mathcal{R}}a \subseteq H$ и, следовательно, $a \in L(H)$. ►

Лемма 10.6. Различимый точный модуль ${}_{\mathcal{R}}M$ над локальным кольцом $\mathcal{R}$ является QF-модулем.

◄ Пусть χ — различающий характер модуля ${}_{\mathcal{R}}M$. Согласно пункту 4) теоремы 9.5 для того, чтобы доказать лемму, достаточно показать, что $\dim_{\overline{\mathcal{R}}} \mathrm{soc}M = 1$. Рассуждая от противного, предположим, что $\dim_{\overline{\mathcal{R}}} \mathrm{soc}M > 1$. В этом случае $|\mathrm{soc}M| = q^{\dim_{\overline{\mathcal{R}}} \mathrm{soc}M} \geq q^2$.

Рассмотрим ограничение $\overline{\chi}$ характера χ на $\mathrm{soc}M$. Пусть $G = \ker \overline{\chi}$. Поскольку группа $(\mathrm{soc}M, +)$ как аддитивная группа конечного пространства над полем характеристики p является элементарной p-группой, и $\chi(\mathrm{soc}M) \neq 0$ в силу выбора характера χ, то $\overline{\chi}(\mathrm{soc}M)$ — подгруппа порядка p в $\mathbb{Q}/\mathbb{Z}$. Следовательно, G — подгруппа индекса p в $\mathrm{soc}M$. Для подпространства $L(G)$, определённого в лемме 10.5, из утверждения $L(G) = \bigcap\limits_{i=1}^{r} u_i^{-1}G$ и значения индекса группы G следует, что $L(G)$ — подгруппа индекса, не превосходящего $p^r = q$. Тогда из ограничений на индекс $L(G)$ и на мощность $\mathrm{soc}M$ следует, что $L(G) \neq 0$. Таким образом, в группе $G = \ker \overline{\chi}$ содержится ненулевое подпространство $L(G)$. При этом $L(G)$ — подмодуль модуля ${}_{\overline{\mathcal{R}}}M$ (см. замечание перед предложением 7.20). Имеем $\chi(L(G)) = 0$, противоречие с тем, что χ — различающий характер модуля ${}_{\mathcal{R}}M$. ►

Теорема 10.7. Точный модуль ${}_{\mathcal{R}}M$ является различимым тогда и только тогда, когда он есть QF-модуль.

◄ Получается объединением лемм 10.3–10.4 и 10.6, с использованием предложения 9.4.►

Лекция 11. Линейные коды над квазифробениусовым модулем, двойственность между кодами над кольцом и кодами над квазифробениусовым модулем.

В данной лекции мы обобщим материал Лекции 4 на случай линейных кодов над кольцами и квазифробениусовыми модулями.

1°. Коды над квазифробениусовым модулем.

Теорема 11.1. Пусть M — левый $\mathcal{R}$-модуль. Следующие условия эквивалентны:
1) ${}_{\mathcal{R}}M$ есть QF-модуль;
2) для любого $N \in \mathbb{N}$ и любых линейных кодов $\mathcal{C} \leq {}_{\mathcal{R}}\mathcal{R}^N$, $\mathcal{K} \leq {}_{\mathcal{R}}M^N$ выполнены равенства

$$\operatorname{ann}_{M^N}(\operatorname{ann}_{\mathcal{R}^N}(\mathcal{K})) = \mathcal{K}, \tag{11.1}$$

$$\operatorname{ann}_{\mathcal{R}^N}(\operatorname{ann}_{M^N}(\mathcal{C})) = \mathcal{C}; \tag{11.2}$$

3) ${}_{\mathcal{R}}M$ — точный модуль и для любого $N \in \mathbb{N}$ и любого линейного кода $\mathcal{K} \leq {}_{\mathcal{R}}M^N$ выполнено равенство (11.1).

◀ "1) $\Rightarrow$ 2)" По теореме 9.6 можно считать, что $M = \mathcal{R}^*$. В этом случае согласно предложению 8.5, можно также считать, что $M^N = (\mathcal{R}^N)^*$. Тогда $\mathcal{L} = \operatorname{ann}_{M^N}(\mathcal{C})$ — множество характеров группы $\mathcal{R}^N$, аннулирующих $\mathcal{C}$, и $\operatorname{ann}_{\mathcal{R}^N}(\mathcal{L})$ — подгруппа элементов из $\mathcal{R}^N$, аннулируемых всеми характерами из $\mathcal{L}$. Повторяя рассуждения из доказательства теоремы 9.3, приходим к тому, что выполнено равенство (11.2). Равенство (11.1) доказывается аналогично путём отождествления $\mathcal{R}^N = (M^N)^*$ (с использованием теоремы 8.4).

"2) $\Rightarrow$ 3)" Очевидно.

"3) $\Rightarrow$ 1)" На основании предложения 9.4 достаточно рассмотреть случай, когда $\mathcal{R}$ — локальное кольцо. Пусть ${}_{\mathcal{R}}M$ — не QF-модуль. Тогда по теореме 9.5 в $\operatorname{soc}M = \operatorname{ann}(J(\mathcal{R}))$ содержится некоторый собственный подмодуль $\mathcal{K}$. Тогда $\operatorname{ann}_{\mathcal{R}}(\mathcal{K}) = J(\mathcal{R})$ (большего собственного идеала в $\mathcal{R}$ нет), но $\operatorname{ann}_M(\operatorname{ann}_{\mathcal{R}}(\mathcal{K})) = \operatorname{soc}M \neq \mathcal{K}$, противоречие с (11.1) для $N = 1$.) ▶

Напомним определение проверочной матрицы.

Определение 11.2. Пусть M — левый $\mathcal{R}$-модуль и $\mathcal{K}$ — код над M длины n. Матрица $H = (h_{ij})$ размера $r \times n$ над кольцом $\mathcal{R}$ называется

проверочной матрицей кода $\mathcal{K}$ длины n над M, если

$$\mathcal{K} = \left\{ \mathbf{a} \in M^n : \ H\mathbf{a}^T = 0 \right\}. \tag{11.3}$$

Пусть $\mathcal{H}$ — линейный код над $\mathcal{R}$, порождённый строками матрицы H, $\mathcal{H} \leq {}_{\mathcal{R}}\mathcal{R}^n$. Тогда из определения видно, что H — проверочная матрица кода $\mathcal{K}$ в том и только в том случае, если $\mathcal{K} = \mathrm{ann}_{M^n}(\mathcal{H})$, т.е. $\mathcal{K}$ — двойственный код к $\mathcal{H}$.

Для кодов над модулями и даже над кольцами проверочная матрица существует далеко не всегда, однако сейчас мы увидим, что именно для класса квазифробениусовых модулей утверждение о существовании проверочной матрицы верно.

Предложение 11.3. Пусть ${}_{\mathcal{R}}M$ — точный модуль. Тогда любой линейный код над M имеет проверочную матрицу над $\mathcal{R}$ тогда и только тогда, когда ${}_{\mathcal{R}}M$ есть QF-модуль.

◀ "$\Rightarrow$" Если ${}_{\mathcal{R}}M$ есть QF-модуль и $\mathcal{K} \leq {}_{\mathcal{R}}M^n$, то в силу равенства (11.1) матрица H над $\mathcal{R}$, строки которой порождают код $\mathcal{H} = \mathrm{ann}_{\mathcal{R}^n}(\mathcal{K})$, есть проверочная для $\mathcal{K}$.

"$\Leftarrow$" Если любой код $\mathcal{K} \leq {}_{\mathcal{R}}M^n$ имеет проверочную матрицу над $\mathcal{R}$, т.е. выполнено $\mathcal{K} = \mathrm{ann}_{M^n}(\mathcal{H})$ для некоторого кода $\mathcal{H} \leq {}_{\mathcal{R}}\mathcal{R}^n$, то верно равенство (11.1) и по теореме 11.1 ${}_{\mathcal{R}}M$ есть QF-модуль.▶

Пусть $\mathcal{C} \leq {}_{\mathcal{R}}\mathcal{R}^n$ — линейный код над кольцом. Если $\mathcal{R}$ не является полем, то проверочной матрицы для $\mathcal{C}$ над $\mathcal{R}$ опять же может не существовать, но возможно построить проверочную матрицу над QF-модулем. Договоримся при необходимости рассматривать левый $\mathcal{R}$-модуль M и как правый модуль, полагая $rm = mr$ для любых $r \in \mathcal{R}$, $m \in M$.

Определение 11.4. Пусть $\mathcal{C}$ — код над $\mathcal{R}$ длины n, M — левый $\mathcal{R}$-модуль. Матрица K размера $m \times n$ над модулем M называется *проверочной матрицей* кода $\mathcal{C}$, если

$$\mathcal{C} = \left\{ \mathbf{a} \in \mathcal{R}^n : \ K\mathbf{a}^T = 0 \right\}. \tag{11.4}$$

Пусть $\mathcal{K}$ — линейный код над M, порождённый строками матрицы K, $\mathcal{K} \leq {}_{\mathcal{R}}M^n$. Тогда из определения видно, что K — проверочная матрица кода $\mathcal{C}$ в том и только в том случае, если $\mathcal{C} = \mathrm{ann}_{\mathcal{R}^n}(\mathcal{K})$, и проверочная матрица для $\mathcal{C}$ над M существует тогда и только тогда, когда условию $\mathcal{C} = \mathrm{ann}_{\mathcal{R}^n}(\mathcal{K})$ удовлетворяет код $\mathcal{K} = \mathrm{ann}_{M^n}(\mathcal{C})$. В этом случае строки матрицы K выбираются как система образующих модуля $\mathcal{K}$. Из теоремы 11.1 получаем

Предложение 11.5. Любой линейный код над кольцом $\mathcal{R}$ имеет проверочную матрицу над QF-модулем ${}_{\mathcal{R}}M$.

Обращение этого утверждения неверно.

Пусть ${}_{\mathcal{R}}\mathcal{R}^{(N)}$ — модуль столбцов высоты N над кольцом $\mathcal{R}$.

Определение 11.6. Назовём матрицу K размера $m \times N$ над модулем ${}_{\mathcal{R}}M$ *проверочной* для матрицы H размера $N \times n$ над кольцом $\mathcal{R}$, если для любого столбца $b^{\downarrow} \in \mathcal{R}^{(N)}$ система $Hx^{\downarrow} = b^{\downarrow}$ разрешима тогда и только тогда, когда $Kb^{\downarrow} = 0^{\downarrow}$.

Над полем любая матрица H имеет проверочную матрицу K и размерность d многообразия решений любой совместной системы $Hx^{\downarrow} = b^{\downarrow}$ удовлетворяет равенствам $d = n - \mathrm{rk}H = \mathrm{rk}K + n - N$. Это утверждение допускает обобщение на случай квазифробениусова модуля:

Предложение 11.7. Любая матрица H размера $N \times n$ над кольцом $\mathcal{R}$ имеет проверочную матрицу K размера $m \times N$ над QF-модулем ${}_{\mathcal{R}}M$. При этом если $\mathcal{H}$ — линейный код над $\mathcal{R}$, порождённый столбцами матрицы H, $\mathcal{K}$ — линейный код над M, порождённый строками матрицы K, то число $D = D(H)$ решений любой совместной системы $Hx^{\downarrow} = b^{\downarrow}$ равно

$$D = |\mathcal{H}|^{-1}|\mathcal{R}|^n = |\mathcal{K}||\mathcal{R}|^{n-N}.$$

◀ Согласно предложению 11.5, существует матрица K над M такая, что для любого $b^{\downarrow} \in \mathcal{R}^{(N)}$

$$b^{\downarrow} \in \mathcal{H} \;\Leftrightarrow\; Kb^{\downarrow} = 0^{\downarrow}.$$

Матрица K — искомая, поскольку условие $b^{\downarrow} \in \mathcal{H}$ есть критерий совместности системы $Hx^{\downarrow} = b^{\downarrow}$.

Докажем равенство $D = |\mathcal{H}|^{-1}|\mathcal{R}|^n$. Обозначим $h_i^{\downarrow}$ — i-ый столбец матрицы H. Рассмотрим гомоморфизм $\mathcal{R}$-модулей $\varphi : \mathcal{R}^n \to \mathcal{H}$, $\varphi((x_1, \ldots, x_n)) = \sum\limits_{i=1}^{n} x_i h_i^{\downarrow}$. По построению $D = |\ker\varphi|$. По теореме о гомоморфизме для модулей в силу сюръективности отображения φ имеем $\mathcal{H} \cong \mathcal{R}^n/\ker\varphi$. Поэтому $D = |\ker\varphi| = |\mathcal{H}|^{-1}|\mathcal{R}|^n$. Поскольку $\mathcal{K}$ — двойственный код к $\mathcal{H}$, $\mathcal{K} = \mathrm{ann}_{M^N}(\mathcal{H})$. Вспомним, что $\mathrm{ann}_{M^N}(\mathcal{H})$ можно рассматривать как группу характеров факторгруппы $\mathcal{R}^N/\mathcal{H}$, что в силу утверждения 1) предложения об изоморфизме с группой характеров, влечёт равенство $|\mathrm{ann}_{M^N}(\mathcal{H})| = |\mathcal{R}^N/\mathcal{H}|$. Значит, $|\mathcal{K}|\cdot|\mathcal{H}| = \mathcal{R}^N$, откуда следует, что $D = |\mathcal{K}||\mathcal{R}|^{n-N}$.▶

2°. Теорема Мак-Вилльямс над QF-модулями

На лекции 2 мы показали, что теорема А.А. Маркова справедлива над любым алфавитом, в частности, для кодов над QF-модулями.

Теорему Мак-Вилльямс о продолжении изометрии так же можно обобщить на этот случай.

Определение 11.8. Пусть $M_{\mathcal{R}}$ — модуль над кольцом $\mathcal{R}$. Линейные коды $\mathcal{C}, \mathcal{L} \leqslant M^n$ *линейно изометричны*, если существует изоморфизм $\mathcal{R}$ модулей

$$\tau : {}_{\mathcal{R}}\mathcal{C} \to {}_{\mathcal{R}}\mathcal{L} \tag{11.5}$$

такой, что

$$d(\mathbf{a}, \mathbf{b}) = d(\tau(\mathbf{a}), \tau(\mathbf{b})) \ \forall \ \mathbf{a}, \mathbf{b} \in \mathcal{C}. \tag{11.6}$$

Теорема 11.9 (Хейфец, 2001)**.** Пусть M — QF-модуль над локальным кольцом $\mathcal{R}$. Тогда любая линейная изометрия линейных кодов (11.5) продолжается до линейного мономиального преобразования пространства Хэмминга M^n.

◄ Без доказательства.►

Лекция 12. Общая весовая функция линейного кода над кольцом и над модулем. Тождество Мак-Вилльямс для линейных кодов над кольцом и над квазифробениусовым модулем.

Пусть $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$. Положим $|\mathcal{R}| = r$, $\mathcal{R} = \{\rho_1, \ldots, \rho_r\}$. Пусть также M — левый $\mathcal{R}$-модуль, $|M| = m$, $M = \{\mu_1, \ldots, \mu_m\}$.

Определение 12.1. *Общей весовой функцией* кода $\mathcal{C} \leq {}_{\mathcal{R}}\mathcal{R}^N$ называется многочлен

$$W_{\mathcal{C}}(x_1, \ldots, x_r) = \sum_{\mathbf{u} \in \mathcal{C}} x_1^{s_1(\mathbf{u})} \cdots x_r^{s_r(\mathbf{u})}$$

над $\mathbb{Z}$, где $s_t(\mathbf{u})$ — число координат слова $\mathbf{u}$, равных ρ_t.

Аналогично, *общей весовой функцией* кода $\mathcal{K} \leq {}_{\mathcal{R}}M^N$ называется многочлен

$$W_{\mathcal{K}}(y_1, \ldots, y_m) = \sum_{\mathbf{a} \in \mathcal{K}} y_1^{\sigma_1(\mathbf{a})} \cdots y_m^{\sigma_m(\mathbf{a})}$$

над $\mathbb{Z}$, где $\sigma_t(\mathbf{a})$ — число координат слова $\mathbf{a}$, равных μ_t.

Очевидно, что это однородные многочлены степени N.

Напомним, что *комлексный характер* группы G — это гомоморфизм этой группы в группу $(\mathbb{C}^*, \cdot)$ (мультипликативную группу поля комплексных чисел).

Для любого рационального характера $\omega \in M^*$, $\omega : M \to \mathbb{Q}/\mathbb{Z}$ функция $\chi(x) = e^{2\pi i \omega(x)}$ есть комплексный характер группы $(M, +)$, причём ведённое соответствие $\omega \to \chi$ есть изоморфизм аддитивной группы рациональных характеров $(M^*, +)$ и мультипликативной группы комлексных характеров группы $(M, +)$.

Определение 12.2. Комплексный характер χ модуля M называется *различающим*, если $\chi(K) \neq \{1\}$ для любого ненулевого подмодуля $K \leq {}_{\mathcal{R}}M$.

Предложение 12.3. Точный модуль ${}_{\mathcal{R}}M$ имеет различающий комплексный характер тогда и только тогда, когда он есть QF-модуль.

◄ Следует из теоремы 10.7.►

Определение 12.4. Весовые функции кодов $\mathcal{C} \leq {}_{\mathcal{R}}\mathcal{R}^N$ и $\mathcal{K} = \mathrm{ann}_{M^N}(\mathcal{C})$ *связаны тождеством Мак-Вильямс*, если существует комплексный характер χ модуля M такой, что

$$W_{\mathcal{K}}(y_1, \ldots, y_m) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(\rho_1^M(\mathbf{y}), \ldots, \rho_r^M(\mathbf{y})), \tag{12.1}$$

где

$$\rho_j^M(\mathbf{y}) = \sum_{i=1}^{m} \chi(\rho_j \mu_i) y_i, \ j = 1, \ldots, r. \tag{12.2}$$

Лемма 12.5. Пусть χ — различающий комплексный характер модуля ${}_{\mathcal{R}}M$. Тогда для любого ненулевого подмодуля $K \leq {}_{\mathcal{R}}M$ справедливо равенство $\sum\limits_{\alpha \in K} \chi(\alpha) = 0$.

◀ В силу конечности модуля M, группа $G = \chi(K)$ как конечная подгруппа мультипликативной группы поля комплексных чисел является циклической. Следовательно, G совпадает с группой U_k корней степени k из единицы для некоторого $k \geq 2$. По теореме Виета $\sum\limits_{u \in U_k} u = 0$. Поэтому

$$\sum_{\alpha \in K} \chi(\alpha) = \frac{|K|}{|G|} \sum_{g \in G} g = 0.$$

▶

Теорема 12.6. Если ${}_{\mathcal{R}}M$ — QF-модуль и χ — его различающий комплексный характер, то для любого линейного кода $\mathcal{C} \leq {}_{\mathcal{R}}\mathcal{R}^N$ справедливо тождество Мак-Вилльямс (12.1). Если ${}_{\mathcal{R}}M$ — точный, но не QF-модуль, то существуют линейные коды $\mathcal{C} \leq {}_{\mathcal{R}}\mathcal{R}^N$ такие, что равенство (12.1) не выполняется ни для какого комплексного характера χ модуля ${}_{\mathcal{R}}M$.

◀ 1. Весовую функцию кода $\mathcal{K} = \mathrm{ann}_{M^N}(\mathcal{C})$ можно представить в виде

$$W_{\mathcal{K}}(y_1, \ldots, y_m) = \sum_{\mathbf{a} \in \mathcal{K}} f(\mathbf{a}), \text{ где } f(\mathbf{a}) = y_1^{\sigma_1(\mathbf{a})} \cdots y_m^{\sigma_m(\mathbf{a})}.$$

Для произвольного $\mathbf{u} \in \mathcal{R}^N$ положим

$$\widehat{f}(\mathbf{u}) = \sum_{\mathbf{a} \in M^N} \chi(\mathbf{ua}) f(\mathbf{a}) \tag{12.3}$$

и свяжем функцию $\widehat{f}$ с весовой функцией. Имеем

$$\sum_{\mathbf{u}\in\mathcal{C}}\widehat{f}(\mathbf{u})=\sum_{\mathbf{u}\in\mathcal{C}}\left(\sum_{\mathbf{a}\in M^N}\chi(\mathbf{ua})f(\mathbf{a})\right)=\sum_{\mathbf{a}\in M^N}\left(\sum_{\mathbf{u}\in\mathcal{C}}\chi(\mathbf{ua})\right)f(\mathbf{a}).$$

Есть две возможности. Если $\mathbf{a}\in\mathcal{K}$, то $\mathbf{ua}=0$ для всех $\mathbf{u}\in\mathcal{C}$ и $\chi(\mathbf{ua})=1$, откуда $\sum\limits_{\mathbf{u}\in\mathcal{C}}\chi(\mathbf{ua})=\sum\limits_{\mathbf{u}\in\mathcal{C}}1=|\mathcal{C}|$. Если $\mathbf{a}\notin\mathcal{K}$, то элементы вида $\mathbf{ua}$ образуют ненулевой подмодуль модуля M, откуда по лемме 12.5 получаем $\sum\limits_{\mathbf{u}\in\mathcal{C}}\chi(\mathbf{ua})=0$. Следовательно,

$$\sum_{\mathbf{u}\in\mathcal{C}}\widehat{f}(\mathbf{u})=|\mathcal{C}|\sum_{\mathbf{a}\in\mathcal{K}}f(\mathbf{a})=|\mathcal{C}|W_{\mathcal{K}}(y_1,\ldots,y_m),$$

или

$$W_{\mathcal{K}}(y_1,\ldots,y_m)=\frac{1}{|\mathcal{C}|}\sum_{\mathbf{u}\in\mathcal{C}}\widehat{f}(\mathbf{u}).$$

Далее преобразуем равенство (12.3), используя то, что χ — гомоморфизм: для $\mathbf{u}=(u_1,\ldots,u_N)$, $\mathbf{a}=(a_1,\ldots,a_N)$ получаем

$$\widehat{f}(\mathbf{u})=\sum_{a_1,\ldots,a_N\in M}\left(\prod_{t=1}^{N}\chi(u_ta_t)\right)y_1^{\sigma_1(\mathbf{a})}\cdots y_m^{\sigma_m(\mathbf{a})}.$$

Подставляя выражение

$$y_i^{\sigma_i(\mathbf{a})}=\prod_{t=1}^{N}y_i^{\sigma_i(a_t)},$$

делаем вывод, что

$$\widehat{f}(\mathbf{u})=\sum_{a_1,\ldots,a_N\in M}\left(\prod_{t=1}^{N}\chi(u_ta_t)y_1^{\sigma_1(a_t)}\cdots y_m^{\sigma_m(a_t)}\right).$$

Заметим, что при $a_t=\mu_\delta$ имеем $y_1^{\sigma_1(a_t)}\cdots y_m^{\sigma_m(a_t)}=y_\delta$, поэтому

$$\widehat{f}(\mathbf{u})=\sum_{\delta_1,\ldots,\delta_N\in\{1,\ldots,m\}}\left(\prod_{t=1}^{N}\chi(u_t\mu_{\delta_t})y_{\delta_t}\right)=\prod_{t=1}^{N}\left(\sum_{\delta=1}^{m}\chi(u_t\mu_\delta)y_\delta\right).$$

Поскольку u_t принимает каждое значение ρ_λ ровно $s_\lambda(\mathbf{u})$ раз, $\lambda=1,\ldots,r$, то окончательно получаем

$$\widehat{f}(\mathbf{u})=\prod_{\lambda=1}^{r}\left(\sum_{\delta=1}^{m}\chi(\rho_\lambda\mu_\delta)y_\delta\right)^{s_\lambda(\mathbf{u})}.$$

Таким образом, $\widehat{f}(\mathbf{u})$ получается из $x_1^{s_1(\mathbf{u})}\cdots x_r^{s_r(\mathbf{u})}$ заменой $x_\lambda = \rho_\lambda^M(\mathbf{y})$.

2. Построим контрпример для модуля, который не является квазифробениусовым. Положим $N = 1$, $\mathcal{C} = \mathcal{R}$. В этом случае $W_{\mathcal{C}}(x_1,\ldots,x_r) = x_1+\ldots+x_r$. Пусть $M = \{\mu_1,\ldots,\mu_m\}$, где $\mu_1 = 0$. Из условия точности модуля M получаем, что $\mathcal{K} = \operatorname{ann}_M\mathcal{C} = 0$, поэтому $W_{\mathcal{K}}(y_1,\ldots,y_m) = y_1$.

Пусть χ — произвольный комплексный характер χ модуля M. Из условия, что M — не квазифробениусов, следует, что существует ненулевой подмодуль $K < M$ такой, что $\chi(K) = 1$. Это означает, что множество $X = \{\mu \in M :\ \chi(\mathcal{R}\mu) = 1\}$ содержит элементы из K, т.е. $|X| = d \geq 2$. Пусть без ограничения общности $X = \{\mu_1,\ldots,\mu_d\}$. Тогда правая часть равенства (12.1) принимает вид

$$\frac{1}{|\mathcal{C}|}W_{\mathcal{C}}(\rho_1^M(\mathbf{y}),\ldots,\rho_r^M(\mathbf{y})) = \frac{1}{|\mathcal{R}|}(\rho_1^M(\mathbf{y})+\ldots+\rho_r^M(\mathbf{y})) =$$

$$= \frac{1}{|\mathcal{R}|}\sum_{\lambda=1}^{r}\sum_{\delta=1}^{m}\chi(\rho_\lambda\mu_\delta)y_\delta = \frac{1}{|\mathcal{R}|}\sum_{\delta=1}^{m}\left(\sum_{\rho\in\mathcal{R}}\chi(\rho\mu_\delta)\right)y_\delta.$$

При этом если $\mu_\delta \in X$, то $\chi(\mathcal{R}\mu_\delta) = 1$, и $\sum\limits_{\rho\in\mathcal{R}}\chi(\rho\mu_\delta) = |\mathcal{R}|$. Если $\mu_\delta \notin X$, то $\chi(\mathcal{R}\mu_\delta)$ — неединичная подгруппа мультипликативной группы поля комплексных чисел, и как и в лемме 12.5 имеем $\sum\limits_{\rho\in\mathcal{R}}\chi(\rho\mu_\delta) = 0$. Следовательно,

$$W_{\mathcal{C}}(\rho_1^M(\mathbf{y}),\ldots,\rho_r^M(\mathbf{y})) = y_1+\ldots+y_d \neq y_1 = W_{\mathcal{K}}(\mathbf{y}),$$

т.е. равенство (12.1) не выполняется. ►

Лекция 13. Пространство последовательностей над кольцом как модуль над кольцом многочленов. Линейные рекуррентные последовательности (ЛРП). Характеристический многочлен ЛРП. Порождающие элементы модуля ЛРП. Импульсная последовательность. Генератор ЛРП.

Пусть Ω — произвольное множество.

Определение 13.1. Под *последовательностью* над Ω мы будем понимать произвольную функцию $u : \mathbb{Z}_+ \to \Omega$. Для каждого $i \in \mathbb{Z}_+$ элемент $u(i)$ назовём *i-м членом* последовательности u. Множество всех последовательностей над Ω обозначим через Ω^∞. Последовательность $u \in \Omega^\infty$ можно также записывать в виде бесконечного вектора $u = (u(0), u(1), \ldots, u(i), \ldots)$.

Пусть $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$. Будем рассматривать последовательности над кольцом $\mathcal{R}$.

Определение 13.2. *Нулевую* последовательность $(0, 0, \ldots, 0, \ldots)$ обозначим через (0).

1°. Линейные рекуррентные последовательности (ЛРП). Характеристический многочлен ЛРП. Порождающие элементы модуля ЛРП как модуля над кольцом коэффициентов.

Определение 13.3. Последовательность $u \in \mathcal{R}^\infty$ называется *линейной рекуррентной последовательностью* (или сокращённо *ЛРП*) *порядка* $m > 0$ над $\mathcal{R}$, если существуют коэффициенты $\beta_0, \ldots, \beta_{m-1} \in \mathcal{R}$ такие, что

$$u(i+m) = \beta_{m-1}u(i+m-1) + \ldots + \beta_1 u(i+1) + \beta_0 u(i) \ \forall i \in \mathbb{Z}_+. \quad (13.1)$$

Соотношение (13.1) называют *законом рекурсии* ЛРП u, многочлен $F(x) = x^m - \beta_{m-1}x^{m-1} - \ldots - \beta_1 x - \beta_0 \in \mathcal{R}[x]$ — её *характеристическим многочленом*, а вектор $u(\overline{0, m-1}) = (u(0), \ldots, u_{m-1}) \in \mathcal{R}^m$ — *начальным вектором* ЛРП u. По определению также считаем, что нулевая последовательность (0) —ЛРП порядка 0 с характеристическим многочленом $F(x) = 1$, и (0) — единственная ЛРП порядка 0.

Примеры.
1. Геометрическая прогрессия $u = (a, aq, aq^2, \ldots, aq^i, \ldots)$, $a, q \in \mathcal{R}, a \neq 0$, есть ЛРП порядка 1 с характеристическим многочленом $x - q$ и начальным вектором $u(\overline{0}) = (a)$.
2. Арифметическая прогрессия $u \in \mathcal{R}^\infty$ с общим членом $u(i) = a + di$, $i \in \mathbb{Z}_+$, где $a, d \in \mathcal{R}$, $d \neq 0$, есть ЛРП порядка 2 с характеристическим многочленом $x^2 - 2x + 1$ и начальным вектором $u(\overline{0,1}) = (a, a + d)$.
3. Последовательность Фибоначчи $f \in \mathcal{R}^\infty$ с $f(0) = f(1) = 1$ и законом рекурсии $u(i + 2) = u(i + 1) + u(i)$ есть ЛРП порядка 2 с характеристическим многочленом $x^2 - x - 1$ и начальным вектором $u(\overline{0,1}) = (1, 1)$.

Определение 13.4. Определим *сумму* $u + v$ *последовательностей* $u, v \in \mathcal{R}^\infty$ как последовательность $w \in \mathcal{R}^\infty$, заданную правилом $w(i) = u(i) + v(i)$, $i \in \mathbb{Z}_+$. Определим *произведение* ru *последовательности* $u \in \mathcal{R}^\infty$ *на число* $r \in \mathcal{R}$ как последовательность $z \in \mathcal{R}^\infty$, заданную правилом $z(i) = ru(i)$, $i \in \mathbb{Z}_+$.

Очевидно, что эти операции задали на $\mathcal{R}^\infty$ структуру левого $\mathcal{R}$-модуля, а если $\mathcal{R}$ — поле, то структуру бесконечномерного линейного пространства.

Для фиксированного унитарного многочлена $F(x) = x^m - \beta_{m-1}x^{m-1} - \ldots - \beta_1 x - \beta_0 \in \mathcal{R}[x]$ степени $m \geq 0$ через $L_\mathcal{R}(F)$ обозначим множество всех ЛРП над $\mathcal{R}$ с характеристическим многочленом $F(x)$.

Предложение 13.5. Произвольная ЛРП $u \in L_\mathcal{R}(F)$ однозначно задаётся своим начальным вектором $u(\overline{0, m-1})$, при этом $|L_\mathcal{R}(F)| = |\mathcal{R}|^m$.

◀ Следует непосредственно из определения ЛРП.▶

Предложение 13.6. $L_\mathcal{R}(F)$ является конечным подмодулем модуля ${}_\mathcal{R}\mathcal{R}^\infty$.

◀ Следует из определений ЛРП, суммы последовательностей и произведения последовательности на число, и предыдущего предложения. ▶

Таким образом, ${}_\mathcal{R}L_\mathcal{R}(F)$ как конечный модуль будет и конечно порождённым модулем. В следующем утверждении мы найдём минимальную мощность его системы образующих и дадим описание базисов этого модуля.

Предложение 13.7. 1. $L_{\mathcal{R}}(F)$ является свободным $\mathcal{R}$-модулем ранга m.

2. Система элементов $u_1, \ldots, u_m \in L_{\mathcal{R}}(F)$ есть базис (т.е. линейно независимая над $\mathcal{R}$ система образующих) модуля $L_{\mathcal{R}}(F)$ тогда и только тогда, когда матрица

$$U = \begin{pmatrix} u_1(\overline{0, m-1}) \\ \vdots \\ u_m(\overline{0, m-1}) \end{pmatrix},$$

составленная из начальных векторов этих последовательностей, обратима над кольцом $\mathcal{R}$.

◀ 1. Согласно предложению 7.18, нам достаточно показать, что у $L_{\mathcal{R}}(F)$ есть базис мощности m. Это утверждение будет следовать из пункта 2, поскольку над $\mathcal{R}$ существуют обратимые матрицы, например, единичная матрица E_m.

2. "$\Leftarrow$" Пусть U — обратимая матрица. Тогда для любой строки $\mathbf{a} \in \mathcal{R}^m$ существует единственный набор коэффициентов $(b_1, \ldots, b_m) \in \mathcal{R}^m$ такой, что $\mathbf{a} = (b_1, \ldots, b_m)U$. В частности, для произвольной последовательности $u \in L_{\mathcal{R}}(F)$ существует единственный набор коэффициентов $(c_1, \ldots, c_m) \in \mathcal{R}^m$ такой, что

$$u(\overline{0, m-1}) = (c_1, \ldots, c_m)U. \tag{13.2}$$

Рассмотрим последовательность $v = c_1u_1 + \ldots + c_mu_m \in L_{\mathcal{R}}(F)$. По построению $v(\overline{0, m-1}) = (c_1, \ldots, c_m)U = u(\overline{0, m-1})$. Значит, согласно предложению 13.5, $v = u$, т.е. $u = c_1u_1 + \ldots + c_mu_m$. Единственность такого представления следует из единственности решения уравнения (13.2).

"$\Rightarrow$" Пусть система элементов $u_1, \ldots, u_m \in L_{\mathcal{R}}(F)$ есть базис модуля $L_{\mathcal{R}}(F)$. Определим для каждого $k = 1, \ldots, m$ ЛРП $e_k^F \in \mathcal{L}_{\mathcal{R}}(F)$ начальным вектором $e_k^F(\overline{0, m-1}) = e_k$ с 1 на k-м месте и нулями на остальных. По предположению каждая из последовательностей $e_k^F \mathcal{L}_{\mathcal{R}}(F)$ представляется в виде

$$e_k^F = c_{k1}u_1 + \ldots + c_{km}u_m.$$

Тогда для $m \times m$ матрицы $C = (c_{ij})$ выполнено соотношение

$$CU = \begin{pmatrix} e_1^F(\overline{0, m-1}) \\ \vdots \\ e_m^F(\overline{0, m-1}) \end{pmatrix} = E_m.$$

Следовательно, U — обратимая матрица.►

Следствие 13.8. Система ЛРП $e_k^F \in \mathcal{L}_{\mathcal{R}}(F)$, $k = 1, \ldots, m$, есть базис модуля $L_{\mathcal{R}}(F)$.

Следствие 13.9. Если $\mathcal{R} = \mathbb{F}$ — поле, то $\dim L_{\mathbb{F}}(F) = \deg F(x)$.

2°. Пространство последовательностей над кольцом как модуль над кольцом многочленов. Импульсная последовательность. Генератор ЛРП. Покажем, что на множестве $\mathcal{R}^\infty$ можно задать структуру $\mathcal{R}[x]$-модуля, которая даст ещё более "экономный" способ задания модуля $L_{\mathcal{R}}(F)$.

Определение 13.10. Для произвольного $k \in \mathbb{Z}_+$ определим *произведение* $x^k \cdot u$ *последовательности* $u \in \mathcal{R}^\infty$ *на одночлен* $x^k \in \mathcal{R}[x]$ как последовательность $v \in \mathcal{R}^\infty$, заданную правилом

$$v(i) = u(i+k),\ i \in \mathbb{Z}_+.$$

Другими словами, умножение на одночлен x^k есть сдвиг последовательности u на k шагов влево, либо вычёркивание из u первых k членов:

$$x^k \cdot (u(0), u(1), \ldots) = (u(k), u(k+1), \ldots).$$

Определение 13.11. Определим *произведение* $A(x) \cdot u$ *последовательности* $u \in \mathcal{R}^\infty$ *на многочлен* $A(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathcal{R}[x]$ как последовательность, заданную правилом

$$A(x) \cdot u = a_n(x^n \cdot u) + \ldots + a_1(x \cdot u) + a_0 u,$$

т.е. $A(x) \cdot u = w$, где

$$w(i) = \sum_{k=0}^{n} a_k u(i+k) \tag{13.3}$$

для всех $i \in \mathbb{Z}_+$.

Предложение 13.12. Для произвольного унитарного многочлена $F(x) \in \mathcal{R}[x]$ имеет место равенство

$$L_{\mathcal{R}}(F) = \{u \in \mathcal{R}^\infty :\ F(x) \cdot u = (0)\}.$$

◄ Если $F(x) = 1$, то по определению порядка ЛРП имеем $L_{\mathcal{R}}(F) = \{(0)\} = \{u \in \mathcal{R}^\infty : 1 \cdot u = (0)\}$. Пусть $\deg F(x) = m > 0$. Тогда для $u \in \mathcal{R}^\infty$, согласно равенству (13.3), имеем $F(x) \cdot u = v$, где $v(i) = u(i+m) - \beta_{m-1}u(i+m-1) - \ldots - \beta_0 u(i)$ для $i \in \mathbb{Z}_+$. Поэтому согласно закону рекурсии (13.1), условие $u \in L_{\mathcal{R}}(F)$ равносильно условию $F(x) \cdot u = (0)$.►

Теорема 13.13. Группа $(\mathcal{R}^\infty, +)$ является $\mathcal{R}[x]$-модулем относительно введённой операции умножения последовательности на многочлен.

◄ Проверим выполнение аксиом.

1. Пусть $A(x) = \sum\limits_{k=0}^{n} a_k x^k \in \mathcal{R}[x]$, $u, v \in \mathcal{R}^\infty$. Тогда

$$A(x) \cdot (u+v) = \sum_{k=0}^{n} a_k (x^k \cdot (u+v)) = \\ = \sum_{k=0}^{n} a_k (x^k \cdot u + x^k \cdot v) = A(x) \cdot u + A(x) \cdot v.$$

Аналогично, $(A(x) + B(x)) \cdot u = A(x) \cdot u + B(x) \cdot u$ для любых $A(x), B(x) \in \mathcal{R}[x]$, $u \in \mathcal{R}^\infty$.

2. По определению $1 \cdot u = u$ для всех $u \in \mathcal{R}^\infty$.

3. Осталось проверить, что $(A(x)B(x)) \cdot u = A(x) \cdot (B(x) \cdot u)$ для любых $A(x), B(x) \in \mathcal{R}[x]$, $u \in \mathcal{R}^\infty$. Для одночленов имеем:

$$ax^k \cdot (bx^l \cdot u) = ax^k \cdot (bu(l), bu(l+1), \ldots) = \\ = (abu(k+l), abu(k+l+1), \ldots) = abx^{k+l} \cdot u.$$

Поэтому для $A(x) = \sum\limits_{k \geq 0} a_k x^k$, $B(x) = \sum\limits_{l \geq 0} b_l x^l$ получаем, что

$$(A(x)B(x)) \cdot u = \left(\sum_{k,l \geq 0} a_k b_l x^{k+l} \right) \cdot u = \sum_{k,l \geq 0} a_k x^k \cdot (b_l x^l \cdot u) = \\ = \sum_{k0} a_k x^k \cdot (B(x) \cdot u) = A(x) \cdot (B(x) \cdot u).$$

►

Следствие 13.14. $L_{\mathcal{R}}(F)$ является подмодулем модуля ${}_{\mathcal{R}[x]}\mathcal{R}^{\infty}$.

◀ Если $u \in L_{\mathcal{R}}(F)$ и $A(x) \in \mathcal{R}[x]$, то $F(x)\cdot(A(x)\cdot u) = (F(x)A(x))\cdot u = A(x)\cdot(F(x)\cdot u) = A(x)\cdot(0) = (0)$. Следовательно, $A(x)\cdot u \in L_{\mathcal{R}}(F)$. ▶

Следующая теорема показывает, что $\mathcal{R}[x]$-модуль $L_{\mathcal{R}}(F)$ является циклическим, т.е. для его задания достаточно одной последовательности.

Теорема 13.15. Пусть $F(x) = x^m - \beta_{m-1}x^{m-1} - \ldots - \beta_1 x - \beta_0 \in \mathcal{R}[x]$, $m > 0$. Через $e^F \in L_{\mathcal{R}}(F)$ обозначим ЛРП с начальным вектором $e_m = (0, \ldots, 0, 1)$. Тогда для любой последовательности $u \in L_{\mathcal{R}}(F)$ существует единственный многочлен $\Phi(x) \in \mathcal{R}[x]$ степени $\deg\Phi(x) < m$ такой, что $u = \Phi(x)\cdot e^F$, имеющий вид

$$\Phi(x) = u(0)x^{m-1} + \sum_{k=1}^{m-1}(u(k) - \beta_{m-1}u(k-1) - \ldots \\ \ldots - \beta_{m-k}u(0))x^{m-1-k}. \quad (13.4)$$

◀ Система ЛРП $e^F, x\cdot e^F, \ldots, x^{m-1}\cdot e^F \in L_{\mathcal{R}}(F)$ есть базис $\mathcal{R}$-модуля $L_{\mathcal{R}}(F)$ по предложению 13.7, поскольку матрица, составленная из начальных векторов этих последовательностей, имеет вид

$$U = \begin{pmatrix} e^F(\overline{0, m-1}) \\ x\cdot e^F(\overline{0, m-1}) \\ \vdots \\ x^{m-1}\cdot e^F(\overline{0, m-1}) \end{pmatrix} = \begin{pmatrix} e^F(\overline{0, m-1}) \\ e^F(\overline{1, m}) \\ \vdots \\ e^F(\overline{m-1, 2m-2}) \end{pmatrix} = \\ = \begin{pmatrix} 0 & \ldots & \ldots & 0 & 1 \\ 0 & \ldots & \ldots & 1 & e^F(m) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & e^F(m) & \ldots & \ldots & e^F(2m-2) \end{pmatrix},$$

следовательно, обратима над $\mathcal{R}$. Таким образом, существует единственный набор коэффициентов $\varphi_0, \ldots, \varphi_{m-1} \in \mathcal{R}$ такой, что $u = \varphi_0 e^F + \varphi_1 x\cdot e^F + \ldots + \varphi_{m-1}x^{m-1}e^F$. Отсюда очевидно следует, что $\Phi(x) = \varphi_0 + \varphi_1 x + \ldots + \varphi_{m-1}x^{m-1}$ — искомый многочлен, и что он единственнен.

Осталось вывести формулу (13.4). По построению коэффициенты многочлена $\Phi(x)$ удовлетворяют равенству $(\varphi_0, \ldots, \varphi_{m-1}) =$

$u(\overline{0,m-1})U^{-1}$. Значит, нам достаточно доказать, что обратной для U является матрица

$$V = \begin{pmatrix} -\beta_1 & -\beta_2 & \dots & -\beta_{m-1} & 1 \\ -\beta_2 & -\beta_3 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ -\beta_{m-1} & 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & \dots & 0 \end{pmatrix}.$$

Рассмотрим произведение строки $\overrightarrow{v}_s$ матрицы V на столбец $u_t^{\downarrow}$ матрицы U. Имеем $\overrightarrow{v}_s = (-\beta_s, \dots, -\beta_{m-1}, 1, 0, \dots, 0)$, единица расположена на месте $m-s+1$; $u_t^{\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ e^F(m) \\ \vdots \\ e^F(m+t-2) \end{pmatrix}$, единица расположена на месте $m-t+1$. Из расположения нулей и единиц в этих векторах сразу видно, что $\overrightarrow{v}_s u_t^{\downarrow} = 0$, если 1 в $u_t^{\downarrow}$ расположена ниже позиции $m-s+1$, т.е. при всех $t < s$; и $\overrightarrow{v}_s u_t^{\downarrow} = 1$, если 1 в $u_t^{\downarrow}$ расположена в точности на месте $m-s+1$, т.е. при $t = s$. Пусть теперь $t \geq s+1$. Имеем

$$\overrightarrow{v}_s u_t^{\downarrow} = -\beta_s e^F(t-1) - \beta_{s+1} e^F(t) - \dots \\ \dots - \beta_{m-1} e^F(t+m-s-2) + e^F(t+m-s-1),$$

откуда, подставляя $j = t-s-1$ ($j \geq 0$ по условию на t и s), получаем

$$\overrightarrow{v}_s u_t^{\downarrow} = e^F(j+m) - \beta_{m-1} e^F(j+m-1) - \dots - \beta_s e^F(j+s).$$

Поскольку по определению $e^F(i) = 0$ при $i < m$, и $j+s = t-1 < m$, и в выражение для $\overrightarrow{v}_s u_t^{\downarrow}$ можно добавить нулевые слагаемые, то окончательно получим

$$\overrightarrow{v}_s u_t^{\downarrow} = e^F(j+m) - \beta_{m-1} e^F(j+m-1) - \dots \\ \dots - \beta_s e^F(j+s) - \beta_{s-1} e^F(j+s-1) - \dots - \beta_0 e^F(j).$$

Правая часть этого равенства обращается в 0, поскольку e^F есть ЛРП с характеристическим многочленом $F(x)$. Таким образом, $\overrightarrow{v}_s u_t^{\downarrow} = 0$. Следовательно, $VU = E_m$.▶

Определение 13.16. Последовательность $e^F \in L_{\mathcal{R}}(F)$ называется *импульсной последовательностью*. Многочлен $\Phi(X)$, определённый равенством (13.4), называется *генератором ЛРП и относительно её характеристического многочлена* $F(x)$.

Лекция 14. Минимальный многочлен ЛРП над полем и его свойства. Аннулятор ЛРП. Соотношения между семействами ЛРП с различными характеристическими многочленами.

Пусть $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$.

1°. Минимальный многочлен ЛРП над полем и его свойства. Аннулятор ЛРП.

Для фиксированного унитарного многочлена $F(x) = x^m - \beta_{m-1}x^{m-1} - \ldots - \beta_1 x - \beta_0 \in \mathcal{R}[x]$ степени $m \geq 0$ как и ранее через $L_{\mathcal{R}}(F)$ будем обозначать множество всех ЛРП над $\mathcal{R}$ с характеристическим многочленом $F(x)$.

Предложение 14.1. Любая ЛРП $u \in L_{\mathcal{R}}(F)$ имеет бесконечно много характеристических многочленов.

◀ Поскольку $L_{\mathcal{R}}(F)$ является подмодулем модуля ${}_{\mathcal{R}[x]}\mathcal{R}^{\infty}$, то любой унитарный многочлен $H(x) \in \mathcal{R}[x] \cdot F(x)$ является характеристическим для u. ▶

Определение 14.2. *Минимальным многочленом* ЛРП u называется её характеристический многочлен, имеющий наименьшую степень. Степень минимального многочлена называется *рангом* ЛРП u.

Из этого определения видно, что ранг u определён однозначно, поэтому корректно использовать обозначение $\mathrm{rk}u$. В то же время, ЛРП над кольцом может иметь несколько минимальных многочленов.

Пример.
Геометрическая прогрессия $u = (a, aq, aq^2, \ldots, aq^i, \ldots)$ при $a \neq 0$ есть ЛРП ранга 1, соответственно, её характеристический многочлен $F(x) = x - q$ является её минимальным многочленом. Возьмём делитель нуля $a \in \mathcal{R}$ и любой элемент $b \in \mathcal{R}$, $b \neq 0$, такой, что $ab = 0$. В этом случае минимальным многочленом для u будет также многочлен $F(x) + b$.

Отметим, что в этом примере кольцо $\mathcal{R}$ содержит делители нуля, т.е. не может быть полем. Докажем общее утверждение, что для ЛРП над полем минимальный многочлен всегда определён однозначно.

Определение 14.3. *Аннулятором последовательности* $u \in \mathcal{R}^{\infty}$ называется множество

$$\mathrm{ann}(u) = \{H(x) \in \mathcal{R}[x] : \ H(x) \cdot u = 0\}.$$

Заметим некоторые очевидные свойства аннулятора последовательности:

Предложение 14.4. 1. $\mathrm{ann}(u)$ является идеалом кольца $\mathcal{R}[x]$;
2. $u \in \mathcal{R}^\infty$ является ЛРП над $\mathcal{R}$ тогда и только тогда, когда $\mathrm{ann}(u)$ содержит унитарный многочлен;
3. Минимальным многочленом ЛРП u является любой унитарный многочлен наименьшей степени из $\mathrm{ann}(u)$.

Теорема 14.5. Любая ЛРП u над полем $\mathbb{F}$ имеет единственный минимальный многочлен $M_u(x) \in \mathbb{F}[x]$. Кроме того, он удовлетворяет равенству

$$\mathrm{ann}(u) = \mathbb{F}[x]M_u(x),$$

т.е. является образующим элементом идеала $\mathrm{ann}(u)$, и соответственно, делит все характеристические многочлены ЛРП u.

◀ Известно, что $\mathbb{F}[x]$ — кольцо главных идеалов, поэтому $\mathrm{ann}(u) = \mathbb{F}[x]G(x)$. Среди всех таких многочленов $G(x)$ существует единственный унитарный многочлен, обозначим его $M_u(x)$. Поскольку $M_u(x) \cdot u = (0)$, то многочлен $M_u(x)$ является характеристическим многочленом ЛРП u. По построению $M_u(x)$ делит все остальные характеристические многочлены ЛРП u, следовательно, он является её минимальным многочленом. Единственность характеристического многочлена данной степени уже доказана, что влечёт единственность минимального многочлена. ▶

В общем случае кольцо многочленов над кольцом $\mathcal{R}$ не обладает всеми свойствами кольца многочленов над полем. Например, из-за наличия необратимых элементов в кольце $\mathcal{R}$ к многочленам над $\mathcal{R}$ нельзя применить алгоритм деления столбиком даже в случае многочленов 0 степени. С другой стороны, в частном случае унитарного многочлена $G(x)$ алгоритм деления с остатком на $G(x)$ применим. Сохраняются понятия делимости многочленов и взаимной простоты:

Определение 14.6. Многочлены $F(x), G(x) \in \mathcal{R}[x]$ назовём *взаимно простыми* и обозначим $(F(x), G(x)) = 1$, если $\mathcal{R}[x]F(x) + \mathcal{R}[x]G(x) = \mathcal{R}[x]$, т.е. $A(x)F(x) + B(x)G(x) = 1$ для некоторых $A(x), B(x) \in \mathcal{R}[x]$.

Предложение 14.7. Для любых многочленов $F(x), G(x), H(x) \in \mathcal{R}[x]$ справедливы следующие утверждения:

1. если $(F(x), G(x)) = 1$ и $(F(x), H(x)) = 1$, то $(F(x), G(x)H(x)) = 1$;
2. если $(F(x), G(x)) = 1$ и $F(x)|(G(x)H(x))$, то $F(x)|H(x)$;
3. если $(F(x), G(x)) = 1$, $F(x)|H(x)$ и $G(x)|H(x)$, то $F(x)G(x)|H(x)$.

◄ Доказывается так же как и для многочленов над полем.►

Теорема 14.5 допускает некоторое расширение на общий случай ЛРП над кольцом:

Теорема 14.8. Для произвольных унитарного многочлена $G(x) \in \mathcal{R}[x]$ и последовательности $u \in \mathcal{R}^\infty$ следующие утверждения эквивалентны:
1. Последовательность u есть ЛРП с единственным минимальным многочленом $G(x)$;
2. $\mathrm{ann}(u) = \mathcal{R}[x]G(x)$.

◄ "1) $\Rightarrow$ 2)" Поскольку $G(x) \cdot u = (0)$, то $\mathcal{R}[x]G(x) \subseteq \mathrm{ann}(u)$. Обратно, пусть $H(x) \in \mathrm{ann}(u)$. Многочлен $H(x)$ можно разделить с остатком на унитарный многочлен $G(x)$:

$$H(x) = Q(x)G(x) + A(x),\ \deg A(x) < \deg G(x).$$

Поскольку по условию $H(x) \cdot u = G(x) \cdot u = (0)$, то $A(x) \cdot u = (0)$ и $A(x) \in \mathrm{ann}(u)$. В этом случае многочлен $G_1(x) = G(x) + A(x) \in \mathrm{ann}(u)$ — унитарный многочлен той же степени, что $G(x)$. В виду условия 1) отсюда следует, что $G_1(x) = G(x)$, т.е. $A(x) = 0$ и $H(x) = Q(x)G(x)$. Таким образом, $\mathrm{ann}(u) \subseteq \mathcal{R}[x]G(x)$.

"2) $\Rightarrow$ 1)" доказывается также, как теорема 14.5.►

Предложение 14.9. Пусть $F(x) \in \mathcal{R}[x]$ — унитарный многочлен степени $m > 0$, $u \in L_{\mathcal{R}}(F)$ имеет начальный вектор $u(\overline{0, m-1}) = (0, \ldots, 0, a)$, где $a \in \mathcal{R}$ — элемент, не являющийся делителем нуля. Тогда $F(x)$ — единственный минимальный многочлен ЛРП u.

◄ Пользуясь предыдущей теоремой 14.8, достаточно доказать, что $\mathrm{ann}(u) = \mathcal{R}[x]F(x)$. Включение $\mathcal{R}[x]F(x) \subseteq \mathrm{ann}(u)$ уже известно, поэтому осталось доказать, что в $\mathrm{ann}(u)$ любой многочлен $H(x)$ степени меньшей, чем m, равен 0. Предположим противное: пусть $H(x) = h_1 + h_1 x + \ldots + h_k x^k$, $h_k \neq 0$, $k < m$. Тогда последовательность $v = H(x) \cdot u$ имеет ненулевой член $v(m-k-1) = h_k u(m-1) = h_k a \neq 0$ в виду условия на $u(\overline{0, m-1})$ и a. Противоречие с условием $H(x) \cdot u = (0)$.►

Следствие 14.10. Для любого унитарного многочлена $F(x) \in \mathcal{R}[x]$ справедливо равенство $\operatorname{ann}(e^F) = \mathcal{R}[x]F(x)$.

Следующая теорема даёт способ нахождения минимального многочлена ЛРП над полем.

Теорема 14.11. Пусть u — ЛРП над полем $\mathbb{F}$ с характеристическим многочленом $F(x)$ и генератором $\Phi(x)$. Тогда

1. $M_u(x) = \dfrac{F(x)}{(F(x), \Phi(x))}$;
2. если $v = H(x) \cdot u$ для некоторого $H(x) \in \mathbb{F}[x]$, то $M_v(x) = \dfrac{M_u(x)}{(H(x), M_u(x))}$.

◀ По определению генератора и импульсной последовательности, имеем $u = \Phi(x) \cdot e^F$. Мы уже доказали, что $M_{e^F}(x) = F(x)$. Поэтому 1) следует из 2) как частный случай для $v = u$, $u = e^F$, $H(x) = \Phi(x)$.

Докажем утверждение 2). Пусть $A(x) \in \operatorname{ann}(v)$. Имеем цепочку эквивалентностей

$$A(x) \cdot v = (0) \Leftrightarrow A(x)H(x) \cdot u = (0) \Leftrightarrow M_u(x) | A(x)H(x) \Leftrightarrow$$
$$\Leftrightarrow \frac{M_u(x)}{(H(x), M_u(x))} \mid A(x).$$

Следовательно, многочлен $\dfrac{M_u(x)}{(H(x), M_u(x))}$ является образующим для идеала $\operatorname{ann}(v)$. Пользуясь теоремой 14.5, заключаем, что $\dfrac{M_u(x)}{(H(x), M_u(x))} = M_v(x)$. ▶

Следствие 14.12. Минимальный многочлен ЛРП $u \in L_{\mathbb{F}}(F)$ над полем $\mathbb{F}$ равен $F(x)$ тогда и только тогда, когда генератор u относительно $F(x)$ взаимно прост с $F(x)$. В частности, $F(x)$ является минимальным многочленом для любой ненулевой ЛРП из $L_{\mathbb{F}}(F)$ тогда и только тогда, когда $F(x)$ неприводим над полем $\mathbb{F}$.

2°. Соотношения между семействами ЛРП с различными характеристическими многочленами.

Предложение 14.13. Пусть $F(x), G(x) \in \mathcal{R}[x]$ — произвольные унитарные многочлены. Тогда $L_{\mathcal{R}}(G) \subset L_{\mathcal{R}}(F)$ если и только если $G(x) | F(x)$.

◀ "$\Rightarrow$" Пусть $L_{\mathcal{R}}(G) \subset L_{\mathcal{R}}(F)$. Тогда $e^G \in L_{\mathcal{R}}(F)$, значит, $F(x) \cdot e^G = (0)$, т.е. $F(x) \in \operatorname{ann}(e^G)$. Согласно следствию 14.10, $\operatorname{ann}(e^G) = \mathcal{R}[x]G(x)$, откуда получаем требуемое условие $G(x)|F(x)$.

"$\Leftarrow$" Пусть $G(x)|F(x)$. Возьмём произвольную ЛРП $u \in L_{\mathcal{R}}(G)$. Имеем $G(x) \cdot u = (0)$, откуда следует, что $F(x) \cdot u = (0)$. Таким образом, $u \in L_{\mathcal{R}}(F)$. ▶

Теорема 14.14. Пусть $F(x), G(x) \in \mathcal{R}[x]$ — унитарные взаимно простые многочлены и $H(x) = F(x)G(x)$. Тогда

$$L_{\mathcal{R}}(H) = L_{\mathcal{R}}(F) \oplus L_{\mathcal{R}}(G).$$

Если $\mathcal{R}$ — поле, ЛРП $w \in L_{\mathcal{R}}(H)$ представлена в виде $w = u + v$, $u \in L_{\mathcal{R}}(F)$, $v \in L_{\mathcal{R}}(G)$, то

$$(M_u(x), M_v(x)) = 1,\ M_w(x) = M_u(x)M_v(x).$$

◀ 1. Из предложения 14.13 следует, что $L_{\mathcal{R}}(F), L_{\mathcal{R}}(G) \subset L_{\mathcal{R}}(H)$. Откуда используя предложение 13.6, получаем, что $L_{\mathcal{R}}(F)+L_{\mathcal{R}}(G) \subset L_{\mathcal{R}}(H)$.

Для доказательства обратного включения возьмём подходящие многочлены $A(x), B(x) \in \mathcal{R}[x]$ такие, что $A(x)F(x) + B(x)G(x) = 1$. Пусть $w \in L_{\mathcal{R}}(H)$. Тогда $w = A(x)F(x) \cdot w + B(x)G(x) \cdot w$. Положим $u = B(x)G(x) \cdot w$, $v = A(x)F(x) \cdot w$. По построению очевидно, что $F(x) \cdot u = B(x) \cdot (H(x) \cdot w) = (0)$, т.е. $u \in L_{\mathcal{R}}(F)$. Аналогично, $v \in L_{\mathcal{R}}(G)$. Следовательно, $L_{\mathcal{R}}(H) \subseteq L_{\mathcal{R}}(F) + L_{\mathcal{R}}(G)$, и значит,

$$L_{\mathcal{R}}(H) = L_{\mathcal{R}}(F) + L_{\mathcal{R}}(G).$$

Если $w \in L_{\mathcal{R}}(F) \cap L_{\mathcal{R}}(G)$, то $F(x) \cdot w = G(x) \cdot w = (0)$, откуда для определённых выше ЛРП u, v также имеем $u = v = (0)$. Заключаем, что $w = (0)$, поэтому

$$L_{\mathcal{R}}(H) = L_{\mathcal{R}}(F) \oplus L_{\mathcal{R}}(G).$$

2. Пусть $\mathcal{R}$ — поле, ЛРП $w \in L_{\mathcal{R}}(H)$ представлена в виде $w = u+v$, $u \in L_{\mathcal{R}}(F)$, $v \in L_{\mathcal{R}}(G)$. По теореме 14.5 $M_u(x)|F(x)$, $M_v(x)|G(x)$, поэтому $(M_u(x), M_v(x)) = 1$ в силу взаимной простоты $F(x)$ и $G(x)$.

Также по построению $M_u(x)M_v(x) \in \operatorname{ann}(u) \cap \operatorname{ann}(v)$, поэтому $M_u(x)M_v(x) \in \operatorname{ann}(w)$ и $M_w(x)|M_u(x)M_v(x)$. С другой стороны, из условия $u = B(x)G(x) \cdot w$, $v = A(x)F(x) \cdot w$ и теоремы 14.11 следует,

что $M_u(x)|M_w(x)$, $M_v(x)|M_w(x)$. Тогда $M_u(x)M_v(x)|M_w(x)$. Окончательно получаем, что $M_w(x) = M_u(x)M_v(x)$. ►

Над полем это утверждение можно усилить.

Теорема 14.15. Пусть $F(x), G(x) \in \mathbb{F}[x]$ — унитарные многочлены над полем $\mathbb{F}$. Тогда
1. $L_{\mathbb{F}}(F) \cap L_{\mathbb{F}}(G) = L_{\mathbb{F}}(D)$, где $D(x) = (F(x), G(x))$;
2. $L_{\mathbb{F}}(F) + L_{\mathbb{F}}(G) = L_{\mathbb{F}}(H)$, где $H(x) = [F(x), G(x)]$.

◄ Из предложения 14.13 следует, что $L_{\mathbb{F}}(D) \subseteq L_{\mathbb{F}}(F) \cap L_{\mathbb{F}}(G)$. Для доказательства обратного включения возьмём подходящие многочлены $A(x), B(x) \in \mathbb{F}[x]$ такие, что $A(x)F(x) + B(x)G(x) = D(x)$. Пусть $u \in L_{\mathbb{F}}(F) \cap L_{\mathbb{F}}(H)$. Тогда $D(x) \cdot u = A(x)F(x) \cdot u + B(x)G(x) \cdot u = (0) + (0) = (0)$, поэтому $u \in L_{\mathbb{F}}(D)$.

Из предложения 14.13 следует, что $L_{\mathbb{F}}(F) + L_{\mathbb{F}}(G) \subseteq L_{\mathbb{F}}(H)$. Для доказательства равенства включенных пространств над полем достаточно доказать равенство размерностей данных пространств (используем следствие 13.9):

$$\begin{aligned}\dim(L_{\mathbb{F}}(F) + L_{\mathbb{F}}(G)) = \dim L_{\mathbb{F}}(F) + \dim L_{\mathbb{F}}(G) - \\ - \dim(L_{\mathbb{F}}(F) \cap L_{\mathbb{F}}(G)) = \deg F(x) + \deg G(x) - \deg D(x) = \\ = \deg H(x) = \dim L_{\mathbb{F}}(H).\end{aligned}$$

►

Лекция 15. Общие свойства и параметры периодических последовательностей. Периодичность ЛРП над конечным кольцом.

1°. Общие свойства и параметры периодических последовательностей. Пусть Ω — произвольное множество.

Определение 15.1. Последовательность $u \in \Omega^\infty$ называется *периодической*, если существуют индексы $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$ такие, что

$$u(i+t) = u(i) \ \forall i \geq \lambda. \tag{15.1}$$

Пусть $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$.

Заметим очевидную связь периодических последовательностей и ЛРП над кольцом:

Предложение 15.2. Пусть $u \in \mathcal{R}^\infty$. Тогда
1. условие (15.1) эквивалентно условию

$$x^\lambda (x^t - 1) \cdot u = (0); \tag{15.2}$$

2. если u — периодическая, то u является ЛРП над кольцом $\mathcal{R}$.

◄ Следует из предложения 13.12.►

В дальнейшем мы покажем, что верно и обратное утверждение, о том что любая ЛРП над конечным кольцом является периодической последовательностью. Для этого сперва докажем некоторые общие свойства периодических последовательностей.

Если $u \in \Omega^\infty$ — периодическая последовательность, то очевидно, что для неё существует не один набор параметров (λ, t), для которых выполнено равенство (15.1). Для того, чтобы описать все такие параметры, отдельно выделим наименьшие из них следующим образом:

Определение 15.3. Пусть $u \in \Omega^\infty$ — периодическая последовательность. *Периодом* $T(u)$ *последовательности* u называется наименьшее число $t \in \mathbb{N}$, для которого существует $\lambda \in \mathbb{Z}_+$ такое, что выполняется равенство (15.1), при этом *длиной подхода* $\Lambda(u)$ *последовательности* u называется наименьшее число $\lambda \in \mathbb{Z}_+$, для которого выполняется равенство

$$u(i+T(u)) = u(i) \ \forall i \geq \lambda. \tag{15.3}$$

Теорема 15.4. Пусть $u \in \Omega^\infty$ — периодическая последовательность. Числа $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$ удовлетворяют равенству (15.1) тогда и только тогда, когда

$$\lambda \geq \Lambda(u),\ T(u)|t.$$

◀ 1. Пусть сперва $\Omega = \mathbb{F}$ — конечное поле. Как отмечено в предложении 15.2, для фиксированных λ, t равенство (15.1) эквивалентно условию (15.2): $x^\lambda(x^t - 1) \cdot u = (0)$.

"$\Leftarrow$" Пусть $\lambda \geq \Lambda(u),\ T(u)|t$. Тогда $x^{\Lambda(u)}(x^{T(u)} - 1)|x^\lambda(x^t - 1)$, откуда следует, что $x^\lambda(x^t - 1) \cdot u = (0)$, т.е. условие (15.2) выполнено.

"$\Rightarrow$" Обратно, пусть $x^\lambda(x^t - 1) \cdot u = (0)$. Заметим, что

$$(x^\lambda(x^t - 1), x^{\Lambda(u)}(x^{T(u)} - 1)) = x^l(x^d - 1),$$

где $l = \min\{\lambda, \Lambda(u)\}$, $d = (t, T(u))$. Тогда используя утверждение о линейном выражении НОД многочленов, получим

$$x^l(x^d - 1) = A(x)(x^\lambda(x^t - 1)) + B(x)(x^{\Lambda(u)}(x^{T(u)} - 1)).$$

Из условия (15.2) и определения параметров $\Lambda(u)$ и $T(u)$ следует, что $x^l(x^d - 1) \cdot u = (0)$. По определению периода тогда $d \geq T(u)$, что вместе с условием $d|T(u)$, влечёт равенство $d = T(u)$. Тогда оценка $\lambda \geq \Lambda(u)$ следует из определения длины подхода последовательности u.

2. Для произвольного множества Ω рассмотрим множество S всех различных элементов из Ω, встречающихся в u. В силу периодичности последовательности u, имеем оценку $|S| \leq \Lambda(u) + T(u)$, в частности, S — конечное множество. Возьмём любое такое конечное поле $\mathbb{F}$, что $|\mathbb{F}| \geq |S|$. Существует инъекция φ из S в $\mathbb{F}$. Для последовательности v элементов $v(i) = \varphi(u(i))$ утверждение доказано в пункте 1. Ввиду инъективности отображения φ, периоды и длины подходов последовательностей u и v одинаковые, поэтому утверждение выполнено и для последовательности u. ▶

Следствие 15.5. Пусть $u \in \Omega^\infty$ — периодическая последовательность. Тогда её длина подхода $\Lambda(u)$ есть наименьшее число $\lambda \in \mathbb{Z}_+$, для которого существует такой номер $t \in \mathbb{N}$, что выполнено условие (15.1).

Следствие 15.6. Пусть $u \in \mathcal{R}^\infty$ — периодическая последовательность над кольцом $\mathcal{R}$. Тогда для любого многочлена $H(x) \in \mathcal{R}[x]$ последовательность $v = H(x) \cdot u$ также является периодической, причём $\Lambda(v) \leq \Lambda(u)$ и $T(v)|T(u)$.

◄ Заметим, что

$$x^{\Lambda(u)}(x^{T(u)}-1)\cdot v=(H(x)x^{\Lambda(u)}(x^{T(u)}-1))\cdot u=$$
$$=H(x)\cdot(x^{\Lambda(u)}(x^{T(u)}-1)\cdot u)=(0),$$

поэтому утверждение следует из теоремы 15.4.►

Предложение 15.7. Пусть $u,v\in\mathcal{R}^{\infty}$ — периодические последовательности над кольцом $\mathcal{R}$. Тогда
1. сумма этих последовательностей $w=u+w$ также является периодической последовательностью и

$$\Lambda(w)\le\max\{\Lambda(u),\Lambda(v)\},\ T(w)|[T(u),T(v)];\tag{15.4}$$

2. если $\Lambda(u)\ne\Lambda(v)$, то

$$\Lambda(w)=\max\{\Lambda(u),\Lambda(v)\};\tag{15.5}$$

3. если $(T(u),T(v))=1$, то

$$T(w)=[T(u),T(v)];\tag{15.6}$$

4. если u и v — ЛРП, обладающие взаимно простыми характеристическими многочленами, то также выполнены равенства (15.5) и (15.6).

◄ Для удобства положим $\lambda=\max\{\Lambda(u),\Lambda(v)\}$, $t=[T(u),T(v)]$.

1. По теореме 15.4 $x^{\lambda}(x^t-1)\cdot u=(0)$ и $x^{\lambda}(x^t-1)\cdot v=(0)$, откуда $x^{\lambda}(x^t-1)\cdot w=x^{\lambda}(x^t-1)\cdot(u+v)=(0)$. Следовательно, соотношения (15.4) также выполнены по теореме 15.4.

2. Без ограничения общности допустим, что $\Lambda(u)<\Lambda(v)$. Тогда $\lambda=\Lambda(v)$ и $x^{\lambda-1}(x^t-1)\cdot u=(0)$. Предположим, что $\Lambda(w)<\lambda$. Это означает, что $x^{\lambda-1}(x^t-1)\cdot w=(0)$. Откуда получаем, что $x^{\lambda-1}(x^t-1)\cdot v=x^{\lambda-1}(x^t-1)\cdot(w-u)=(0)$. Тогда по теореме 15.4 $\Lambda(v)\le\lambda-1$, противоречие. Следовательно, $\Lambda(w)=\lambda$.

3. Заметим, что $[T(w),T(u)]=kT(w)$, где $k=\dfrac{T(u)}{(T(w),T(u))}\ge 1$. По теореме 15.4 $x^{\lambda}(x^{kT(w)}-1)\cdot w=(0)$ и $x^{\lambda}(x^{kT(w)}-1)\cdot u=(0)$. Тогда $x^{\lambda}(x^{kT(w)}-1)\cdot v=(0)$ и $T(v)|kT(w)$. Если $(T(u),T(v))=1$, то $(k,T(v))=1$, поэтому $T(v)|T(w)$. Аналогично, $T(u)|T(w)$. Следовательно, $T(u)T(v)|T(w)$. Объединяя это с условием (15.4), получаем (15.6).

4. Пусть $u \in L_{\mathcal{R}}(F)$, $v \in L_{\mathcal{R}}(G)$, где $(F(x), G(x)) = 1$. Тогда $w \in L_{\mathcal{R}}(FG)$ и $L_{\mathcal{R}}(FG) = L_{\mathcal{R}}(F) \oplus L_{\mathcal{R}}(G)$ по теореме 14.14. Для любых $\lambda_1 \in \mathbb{Z}_+, t_1 \in \mathbb{N}$ имеем $x^{\lambda_1}(x^{t_1}-1)\cdot u \in L_{\mathcal{R}}(F)$, $x^{\lambda_1}(x^{t_1}-1)\cdot v \in L_{\mathcal{R}}(G)$, $x^{\lambda_1}(x^{t_1}-1)\cdot w = x^{\lambda_1}(x^{t_1}-1)\cdot u + x^{\lambda_1}(x^{t_1}-1)\cdot v$, поэтому из того, что сумма прямая получаем, что $x^{\lambda_1}(x^{t_1}-1)\cdot w = (0)$ тогда и только тогда, когда одновременно $x^{\lambda_1}(x^{t_1}-1)\cdot u = (0)$ и $x^{\lambda_1}(x^{t_1}-1)\cdot v = (0)$. Поэтому утверждение следует из теоремы 15.4.►

Выделим специальные классы периодических последовательностей:

Определение 15.8. Периодическая последовательность u над кольцом $\mathcal{R}$ называется *чисто периодической*, или *реверсивной*, если $\Lambda(u) = 0$.

Определение 15.9. Периодическая последовательность u над кольцом $\mathcal{R}$ называется *вырождающейся*, если $u = (u(0), \ldots, u(\lambda - 1), 0, \ldots, 0, \ldots)$ для некоторого $\lambda \in \mathbb{N}$.

Очевидно следующее утверждение:

Предложение 15.10. 1. $u \in \mathcal{R}^\infty$ — чисто периодическая последовательность тогда и только тогда, когда $u \in L_{\mathcal{R}}(x^t - 1)$ для некоторого $t \in \mathbb{N}$.
2. $u \in \mathcal{R}^\infty$ — вырождающаяся последовательность тогда и только тогда, когда $u \in L_{\mathcal{R}}(x^\lambda)$ для некоторого $\lambda \in \mathbb{Z}_+$.
3. Одновременно чисто периодической и вырождающейся является только нулевая последовательность.

Теорема 15.11. Любая периодическая последовательность u над кольцом $\mathcal{R}$ однозначно представляется в виде суммы $u = u_0 + u_1$, где u_0 — вырождающаяся, u_1 — чисто периодическая последовательности. При этом

$$\Lambda(u) = \Lambda(u_0),\ T(u) = T(u_1). \tag{15.7}$$

◄ По условию $u \in L_{\mathcal{R}}(x^{\Lambda(u)}(x^{T(u)} - 1))$. Ясно, что $(x^{\Lambda(u)}, x^{T(u)} - 1) = 1$. Значит, можно воспользоваться теоремой 14.14. Получаем, что

$$L_{\mathcal{R}}(x^{\Lambda(u)}(x^{T(u)} - 1)) = L_{\mathcal{R}}(x^{\Lambda(u)}) \oplus L_{\mathcal{R}}(x^{T(u)} - 1),$$

и последовательность u единственным образом представляется в виде

$$u = u_0 + u_1,\ u_0 \in L_{\mathcal{R}}(x^{\Lambda(u)}),\ u_1 \in L_{\mathcal{R}}(x^{T(u)} - 1).$$

Это и есть требуемое разложение. Равенства (15.7) следуют из предложения 15.7.

Пусть есть другое разложение $u = v_0 + v_1$, где v_0 — вырождающаяся, v_1 — чисто периодическая последовательности. Из предложения 15.7 получаем, что $\Lambda(v_0) = \Lambda(u)$, $T(v_1) = T(u)$. Следовательно, $v_0 \in L_{\mathcal{R}}(x^{\Lambda(u)})$, $v_1 \in L_{\mathcal{R}}(x^{T(u)} - 1)$. В силу утверждения о прямой сумме, отсюда следует, что $v_0 = u_0$, $v_1 = u_1$. ▶

2°. Периодические многочлены. Периодичность ЛРП над конечным кольцом.

Мы покажем, что над конечным кольцом любая ЛРП является периодической последовательностью. Заметим, что от условия конечности кольца нельзя отказаться. Над бесконечным кольцом не любая ЛРП периодична. Например, не является периодической ЛРП $u = (0, 1, 2, 3, \ldots)$ над $\mathbb{Z}$.

Пусть далее $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$.

Определение 15.12. Многочлен $F(x) \in \mathcal{R}[x]$ назовём *периодическим*, если существуют индексы $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$ такие, что

$$F(x) | x^{\lambda}(x^t - 1). \tag{15.8}$$

Периодом $T(F)$ *многочлена* $F(x)$ называется наименьшее число $t \in \mathbb{N}$, для которого существует $\lambda \in \mathbb{Z}_+$ такое, что выполняется равенство (15.8), при этом *длиной подхода* $\Lambda(F)$ *многочлена* $F(x)$ называется наименьшее число $\lambda \in \mathbb{Z}_+$, для которого выполняется равенство $F(x) | x^{\lambda}(x^{T(F)} - 1)$. Унитарный периодический многочлен $F(x)$ со свойством $\Lambda(F) = 0$ назовём *реверсивным*.

Покажем связь периодических многочленов с периодическими последовательностями:

Предложение 15.13. 1. Унитарный многочлен $F(x) \in \mathcal{R}[x]$ является периодическим тогда и только тогда, когда периодична ЛРП $e^F \in L_{\mathcal{R}}(F)$.
2. Если $F(x) \in \mathcal{R}[x]$ — периодический, то $\Lambda(F) = \Lambda(e^F)$, $T(F) = T(e^F)$.
3. Если $F(x) \in \mathcal{R}[x]$ — периодический, то любая ЛРП $u \in L_{\mathcal{R}}(F)$ есть периодическая последовательность, для которой $\Lambda(u) \leq \Lambda(F)$, $T(u) | T(F)$.

◄ 1 и 2. Согласно следствию 14.10, $\mathrm{ann}(e^F) = \mathcal{R}[x]F(x)$. Поэтому для $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$ утверждения $F(x)|x^\lambda(x^t-1)$ и $x^\lambda(x^t-1)\cdot e^F = (0)$ эквивалентны. Этим доказаны утверждения 1 и 2.

3. Пусть $u \in L_{\mathcal{R}}(F)$. В этом случае $F(x)\cdot u = (0)$. Поскольку $F(x)|x^{\Lambda(F)}(x^{T(F)}-1)$, то $x^{\Lambda(F)}(x^{T(F)}-1)\cdot u = (0)$. Таким образом, u — периодическая последовательность. Утверждение $\Lambda(u) \le \Lambda(F)$, $T(u)|T(F)$ выполнено согласно теореме 15.4.►

Следствие 15.14. Пусть $F(x) \in \mathcal{R}[x]$ — унитарный периодический многочлен. Для произвольных $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$, $F(x)|x^\lambda(x^t-1)$ тогда и только тогда, когда $\lambda \ge \Lambda(F)$ и $T(F)|t$.

Следствие 15.15. Пусть $F(x), G(x) \in \mathcal{R}[x]$ — унитарные периодические взаимно простые многочлены. Тогда многочлен $H(x) = F(x)G(x)$ является периодическим, и

$$\Lambda(H) = \max\{\Lambda(F), \Lambda(G)\},\ T(H) = [T(F), T(G)].$$

◄ Обозначим $\lambda = \max\{\Lambda(F), \Lambda(G)\}$, $t = [T(F), T(G)]$. По предыдущему следствию многочлен $x^\lambda(x^t-1)$ делится на $F(x)$ и на $G(x)$. Тогда $x^\lambda(x^t-1)$ делится на $H(x)$ согласно утверждению 3 предложения 14.7. Значит, $H(x)$ — периодический многочлен. По следствию 15.14 $\Lambda(H) \le \lambda$ и $T(H)|t$. Обратно, поскольку многочлен $x^{\Lambda(H)}(x^{T(H)}-1)$ делится на $H(x) = F(x)G(x)$, то $\Lambda(H) \ge \lambda$, $T(F)|T(H)$ и $T(G)|T(H)$, т.е. $t|T(H)$. ►

Теорема 15.16. Пусть $F(x) \in \mathcal{R}[x]$ — унитарный многочлен степени $m > 0$ над конечным кольцом $\mathcal{R}$. Тогда
1. $F(x)$ — периодический многочлен, причём если $|\mathcal{R}|^m > 2$, то

$$\Lambda(F) + T(F) \le |\mathcal{R}|^m - 1;$$

2. $F(x)$ — реверсивный многочлен тогда и только тогда, когда $F(0) \in \mathcal{R}^*$;
3. произвольная ЛРП $u \in L_{\mathcal{R}}(F)$ является периодической последовательностью, причём если $|\mathcal{R}|^m > 2$, то $\Lambda(u) + T(u) \le |\mathcal{R}|^m - 1$.

◄ 1. Рассмотрим факторкольцо $\mathcal{S} = \mathcal{R}[x]/(F(x))$ и последовательность над ним:

$$[1]_F, [x]_F, \ldots, [x^i]_F, \ldots.$$

Заметим, что так как $|\mathcal{S}| = |\mathcal{R}|^m$, то в этой последовательности есть повторения: $[x^\lambda]_F = [x^{\lambda+t}]_F$ для некоторых индексов $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$.

По определению, это равенство эквивалентно условию $F(x)|x^\lambda(x^t-1)$. Следовательно, $F(x)$ — периодический многочлен. Пусть $k \in \mathbb{N}$ — наибольшее число такое, что элементы

$$[1]_F, [x]_F, \ldots, [x^{k-1}]_F$$

кольца $\mathcal{S}$ попарно различны. Тогда пользуясь следствием 15.14, получаем, что $\Lambda(F)+T(F)=k$. Следовательно, всегда

$$\Lambda(F)+T(F) \le |\mathcal{S}| = |\mathcal{R}|^m.$$

Пусть теперь $|\mathcal{R}|^m > 2$. Покажем, что $k \le |\mathcal{S}|-1$. Допустим, $k > |\mathcal{S}|-1$, т.е. $k=|\mathcal{S}|$. Тогда

$$\mathcal{S} = \left\{[1]_F, [x]_F, \ldots, [x^{k-1}]_F\right\}.$$

Поскольку $[0]_F \in \mathcal{S}$, то $[0]_F = [x^{k-1}]_F = [x]_F^{k-1}$ (мы не могли получить $[0]_F$ раньше из соображений мощности). Значит, $[x]_F$ — делитель нуля в $\mathcal{S}$, поэтому $[1]_F$ является единственным обратимым элементом в $\mathcal{S}$. С другой стороны, $[1-x]_F[1+x+x^2+\ldots+x^{k-1}]_F = [1-x^k]_F = [1]_F$, т.е. элемент $[1-x]_F$ обратим в $\mathcal{S}$. Тогда $[1]_F = [1-x]_F$, $[x]_F = [0]_F$, т.е. $k-1=1$, $k=|\mathcal{S}|=2$, противоречие.

2. "$\Rightarrow$" Пусть $F(x)$ — реверсивный многочлен. Тогда $x^{T(F)}-1 = F(x)G(x)$ для некоторого $G(x) \in \mathcal{R}[x]$. Откуда $F(0)(-G(0)) = 1$, поэтому $F(0) \in \mathcal{R}^*$.

"$\Leftarrow$" Пусть $F(0) \in \mathcal{R}^*$. Поскольку $F(x)$ можно записать в виде $F(x) = F(0) + xU(x)$, то $1 = F(0)^{-1}F(x) - xF(0)^{-1}U(x)$, что означает взаимную простоту $F(x)$ и x. Следовательно, $(F(x), x^\lambda) = 1$ для любого $\lambda \in \mathbb{N}$ согласно пункту 1 утверждения 14.7. В силу периодичности $F(x)|x^{\Lambda(F)}(x^{T(F)}-1)$, откуда согласно пункту 2 утверждения 14.7 выполнено условие $F(x)|x^{T(F)}-1$. Значит, $F(x)$ — реверсивный многочлен.

3. Следует из пункта 1.

►

Пример. Пусть $|\mathcal{R}|^m = 2$, т.е. $m=1$, $|\mathcal{R}|=2$, $\mathcal{R}=\mathbb{Z}_2$. Возьмём $F(x)=x$, $u=(1,0,0,\ldots)$. Тогда $\Lambda(F)=\Lambda(u)=1$, $T(F)=T(u)=1$ и $\Lambda(F)+T(F)=|\mathcal{R}|^m$.

Лекция 16. Периоды многочленов и ЛРП над полем. Вычисление периода неприводимого многочлена. Вычисление периода произвольного многочлена над полем по его каноническому разложению. Существование и свойства ЛРП максимального периода над конечным полем.

Пусть $\mathbb{F} = GF(q)$, $q = p^n$, p — простое.

Период и длину подхода ЛРП над полем можно определить через её минимальный многочлен:

Предложение 16.1. Пусть u — ЛРП над полем $\mathbb{F}$. Тогда $\Lambda(u) = \Lambda(M_u(x))$, $T(u) = T(M_u(x))$.

◀ Следует из теоремы 14.5, поскольку

$$\forall \lambda \in \mathbb{Z}_+, t \in \mathbb{N}: \; x^\lambda (x^t - 1) \cdot u = (0) \Leftrightarrow M_u(x) | x^\lambda (x^t - 1).$$

▶

В дальнейшем мы покажем, как вычислить период и длину подхода произвольного унитарного многочлена. Задача сводится к разложению его на неприводимые сомножители, и определению соответствующих параметров неприводимых многочленов.

1°. Поле разложения и корни неприводимого многочлена над конечным полем.

Напомним, что *поле разложения* $\mathbb{E}$ *многочлена* $F(x) \in \mathbb{F}[x]$ — минимальное расширение $\mathbb{F}$, в котором $F(x)$ раскладывается на линейные множители. Заметим, что $\mathbb{E}$ как конечное расширение конечного поля само является конечным полем.

Теорема 16.2. Пусть $\mathbb{F} = GF(q)$, $q = p^n$, p — простое. Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m и $\mathbb{K} = \mathbb{F}(\alpha)$ — поле, порождённое некоторым (произвольным) корнем α многочлена $F(x)$. Тогда
1. $\mathbb{K} = \mathbb{E}$ — поле разложения многочлена $F(x)$, причём $F(x)$ имеет в $\mathbb{K}$ m различных корней

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

2. $F(x) | x^{q^m} - x$.

◄ 1. Пусть $F(x) = \sum\limits_{i=0}^{m} f_i x^i$, $f_i \in \mathbb{F}$. По следствию из теоремы Лагранжа имеем $f_i^q = f_i$ для всех $i = 0, \ldots, m$. Тогда для любого $s \in \mathbb{N}$ имеем

$$F(\alpha^{q^s}) =$$
$$= \sum_{i=0}^{m} f_i \cdot (\alpha^{q^s})^i = \sum_{i=0}^{m} f_i \cdot (\alpha^i)^{q^s} = \sum_{i=0}^{m} (f_i \alpha^i)^{q^s} = \left(\sum_{i=0}^{m} f_i \alpha^i \right)^{q^s} =$$
$$= (F(\alpha))^{q^s} = 0.$$

Поэтому все числа $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ являются корнями многочлена $F(x)$.

Докажем, что они различны. Предположим противное: $\alpha^{q^s} = \alpha^{q^t}$ для $0 \leq s < t \leq m-1$. Тогда при $r = t - s$ получаем $0 = \alpha^{q^{s+r}} - \alpha^{q^s} = (\alpha^{q^r} - \alpha)^{q^s}$. Значит, $\alpha^{q^r} = \alpha$ для некоторого $0 < r < m$.

Элементы поля $\mathbb{K}$ имеют вид $\beta = \sum\limits_{i=0}^{m-1} c_i \alpha^i$, $c_i \in \mathbb{F}$. Поскольку $c_i^{q^r} = c_i$ для всех $i = 0, \ldots, m-1$, то из доказанному выше получаем $\beta^{q^r} = \beta$. Следовательно, все q^m элементов поля $\mathbb{K}$ являются корнями многочлена $x^{q^r} - x$, что невозможно, поскольку $r < m$. Противоречие.

2. Известно, что $|\mathbb{K}| = q^m$ и все элементы поля $\mathbb{K}$ являются корнями многочлена $G(x) = x^{q^m} - x \in \mathbb{F}[x]$. Значит, $F(x)$ и $G(x)$ не взаимно просты над полем $\mathbb{K}$, а тогда и над $\mathbb{F}$. Ввиду неприводимости многочлена $F(x)$ над полем $\mathbb{F}$ получаем, что $F(x) | G(x)$.

►

Следствие 16.3. Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m, $F(x) \neq x$ и α, β — корни многочлена $F(x)$ в его поле разложения $\mathbb{E}$. Тогда в мультипликативной группе $\mathbb{E}^*$
1. $\mathrm{ord}\alpha = \mathrm{ord}\beta$;
2. $\mathrm{ord}\alpha | q^m - 1$;
3. $\mathrm{ord}\alpha \nmid q^r - 1$ для $0 < r < m$.

◄ 1. Пусть $\mathrm{ord}\alpha = d$. Тогда α — корень многочлена $x^d - 1 \in \mathbb{F}[x]$. Следовательно, $(F(x), x^d - 1) \neq 1$, поэтому $F(x) | x^d - 1$. Поскольку $F(\beta) = 0$, то $\mathrm{ord}\beta \leq d = \mathrm{ord}\alpha$. Аналогично, $\mathrm{ord}\alpha \leq \mathrm{ord}\beta$.

2. Согласно пункту 2 предыдущей теоремы $F(x) | x(x^{q^m - 1} - 1)$. Ввиду неприводимости многочлена $F(x)$ и условия $F(x) \neq x$ получаем, что $F(x) | x^{q^m - 1} - 1$. Откуда $\mathrm{ord}\alpha | q^m - 1$.

3. Следует из доказательства пункта 1 предыдущей теоремы.►

Определение 16.4. Для многочлена $F(x) \in \mathbb{F}[x]$ определим параметр $O(F)$ как НОК порядков всех ненулевых корней многочлена $F(x)$ в мультипликативной группе его поля разложения над $\mathbb{F}$; положим $O(F) = 1$ для $F(x) = x^l$, $l \in \mathbb{N}$.

2°. Вычисление периода неприводимого многочлена.

Теорема 16.5. Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m. Тогда
1. $\Lambda(F) = 0$, т.е. любой неприводимый многочлен над полем является реверсивным;
2. $T(F) = O(F)$;
3. $T(F)|q^m - 1$, в частности, $(T(F), p) = 1$, и $T(F) \nmid q^k - 1$ для $k \in \{1, \dots, m-1\}$.

◄ 1. В силу неприводимости $F(x)$ не делится на x, т.е. $F(0) \neq 0$, и реверсивность следует из пункта 2 теоремы о периодичности ЛРП.

2. Пусть $\mathbb{E}$ — поле разложения $F(x)$ над $\mathbb{F}$. Тогда порядки всех корней $F(x)$ в $\mathbb{E}$ одинаковы, поэтому $O(F) = \mathrm{ord}\alpha$ для произвольного корня $\alpha \in \mathbb{E}$.

Так как по определению $F(x)|x^{T(F)} - 1$, то $\alpha^{T(F)} = 1$, значит $O(F) = \mathrm{ord}\alpha | T(F)$.

Обратно, поскольку $\alpha^{O(F)} = 1$, то $(F(x), x^{O(F)} - 1) \neq 1$. Из неприводимости $F(x)$ тогда получаем, что $F(x)|x^{O(F)} - 1$, т.е. $T(F)|O(F)$. Следовательно, $T(F) = O(F)$.

3. Поскольку $\alpha \in \mathbb{E}^*$, то $\mathrm{ord}\alpha || \mathbb{E}^* | = q^m - 1$. Значит, по пункту 2, $T(F)|q^m - 1$. Заметим, что если $T(F)|q^k - 1$ при $k < m$, то $\alpha^{q^k} = \alpha$, противоречие с тем, что $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ — это все различные корни многочлена $F(x)$. ►

Алгоритм нахождения периода неприводимого многочлена. Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m.
Шаг 1. Находим все делители числа $q^m - 1$, не являющиеся делителями чисел $q-1, \dots, q^{m-1}-1$ и далее осуществляем по ним перебор.
Шаг 2. Для каждого найденного на Шаге 1 числа t проверяем выполнение условия

$$x^t \equiv 1 (\mod F(x)).$$

Шаг 3. Наименьшее из таких t, для которых выполнено условие Шага 2, и есть период $T(F)$.

3°. Вычисление периода произвольного многочлена над полем по его каноническому разложению.

Теорема 16.6. Пусть $F(x) \in \mathbb{F}[x]$ — унитарный многочлен, имеющий каноническое разложение

$$F(x) = x^l G_1(x)^{k_1} \cdots G_s(x)^{k_s}$$

на неприводимые множители. Положим

$$k = \max\{k_1, \ldots, k_s\},\ c = \lceil \log_p k \rceil,$$

т.е. число $c \in \mathbb{Z}_+$ находится из условия $p^{c-1} < k \leq p^c$. Тогда

$$\Lambda(F) = l,\ T(F) = p^c O(F) = p^c [T(G_1, \ldots, T(G_s)].$$

◀ Положим $H(x) = G_1(x)^{k_1} \cdots G_s(x)^{k_s}$. Согласно пункту 2 теоремы 15.16, многочлен $H(x)$ является реверсивным. По следствию 15.15 имеем: $\Lambda(F) = \Lambda(x^l) = l$, $T(F) = T(H)$.

Пусть далее $G(x) = G_1(x) \cdots G_s(x)$. Очевидно, что $O(F) = O(G) = [O(G_1), \ldots, O(G_s)]$. Из теоремы 16.5 следует, что выполнено равенство $[O(G_1), \ldots, O(G_s)] = [T(G_1), \ldots, T(G_s)]$. В свою очередь, $[T(G_1), \ldots, T(G_s)] = T(G)$ согласно следствию 15.15. Остаётся доказать равенство $T(H) = p^c T(G)$.

Поскольку $G(x) | x^{T(G)} - 1$, то по определению параметров k и c отсюда следует, что $H(x) | (x^{T(G)} - 1)^k$ и $H(x) | (x^{T(G)} - 1)^{p^c}$. Над полем характеристики p верно равенство $(x^{T(G)} - 1)^{p^c} = x^{T(G)p^c} - 1$. Отсюда получаем, что $T(H) | T(G)p^c$. Более того, $T(G) | T(H)$ (поскольку $G(x) | H(x)$), следовательно, $T(H) = T(G)p^d$ для некоторого $d \leq c$.

По пункту 3 теоремы 16.5 имеем $(T(G_i), p) = 1$, $i = 1, \ldots, s$. Значит, $(T(G), p) = 1$. Отсюда следует, что многочлен $x^{T(G)} - 1$ взаимно прост со своей производной, поэтому не имеет кратных множителей в каноническом разложении над $\mathbb{F}$. Тогда в каноническом разложении многочлена $x^{T(H)} - 1 = (x^{T(G)} - 1)^{p^d}$ каждый неприводимый множитель имеет кратность p^d. С другой стороны, $H(x) | x^{T(H)} - 1$, поэтому $k_i \leq p^d$, $i = 1, \ldots, s$, и значит, $k \leq p^d$. По определению параметра c отсюда следует, что $c \leq d$. Таким образом, $d = c$, и $T(H) = T(G)p^c$. ▶

4°. Существование и свойства ЛРП максимального периода над конечным полем. Пусть u — ЛРП ранга m над полем $\mathbb{F}$. По теореме 15.16 при условии $q^m > 2$ период и длина подхода последовательности u удовлетворяют неравенству $\Lambda(u) + T(u) \leq q^m - 1$. Интерес представляют последовательности, для которых эта оценка превращается в равенство, и более того, чтобы период был наибольшим, а именно:

Определение 16.7. Последовательность $u \in \mathbb{F}^\infty$ называется *ЛРП максимального периода над* $\mathbb{F}$, если для некоторого $m \in \mathbb{N}$ последовательность u есть ЛРП ранга m и периода $q^m - 1$.

Очевидно, что для $q^m > 2$ при этом ЛРП u максимального периода над $\mathbb{F}$ есть чисто периодическая последовательность ($\Lambda(u) = 0$), соответственно, её минимальный многочлен реверсивен.

Заметим, что ЛРП u максимального периода $q^m - 1$ над полем $\mathbb{F} = GF(q)$ не будет ЛРП максимального периода над его расширением $\mathbb{K} = GF(q^t)$, $t > 1$, поскольку $T(u) \neq q^{tm} - 1$.

Существование и свойства ЛРП максимального периода над конечным полем даёт следующая теорема:

Теорема 16.8. Пусть u — ЛРП над полем $\mathbb{F} = GF(q)$ с реверсивным минимальным многочленом $M_u(x)$ степени m, причём $q^m > 2$. Тогда следующие утверждения эквивалентны:
1. u — ЛРП максимального периода над $\mathbb{F}$;
2. любая ненулевая ЛРП $v \in L_{\mathbb{F}}(M_u)$ есть сдвиг последовательности u, т.е. $v = x^k \cdot u$ для некоторого $k \in \mathbb{Z}_+$;
3. многочлен $M_u(x)$ неприводим над $\mathbb{F}$, и его корень α в поле разложения $\mathbb{E} = GF(q^m)$ над $\mathbb{F}$ есть примитивный элемент поля $\mathbb{E}$;
4. $T(M_u) = q^m - 1$.

◀ "1) $\Rightarrow$ 2)" Так как $T(u) = q^m - 1$, то все последовательности $u, x \cdot u, \ldots, x^{q^m-1} \cdot u$ различны и принадлежат $L_{\mathbb{F}}(M_u) \setminus \{(0)\}$. Поскольку по предложению 13.5 $|L_{\mathbb{F}}(M_u) \setminus \{(0)\}| = q^m - 1$, то эти последовательности исчерпывают множество $L_{\mathbb{F}}(M_u) \setminus \{(0)\}$.

"2) $\Rightarrow$ 3)" По условию теоремы $(M_u(x), x) = 1$. Если любая ненулевая ЛРП $v \in L_{\mathbb{F}}(M_u)$ имеет вид $v = x^k \cdot u$, то по пункту 2 теоремы 14.11 получаем, что

$$M_v(x) = \frac{M_u(x)}{(M_u(x), x^k)} = M_u(x).$$

Тогда согласно следствию 14.12, многочлен $M_u(x)$ неприводим над $\mathbb{F}$. Как показано в доказательстве пункта 2 теоремы 16.5, $T(M_u) =$

$O(M_u) = \mathrm{ord}\alpha$. Из условия, что

$$|\left\{x^k \cdot u | k \in \mathbb{Z}_+\right\}| = |L_{\mathbb{F}}(M_u) \setminus \{(0)\}| = q^m - 1$$

следует, что $T(u) = q^m - 1$. Из равенства $T(M_u) = T(u) = q^m - 1$ следует, что α является образующим элементом группы $(\mathbb{E}^*, \cdot)$, т.е. примитивным элементом поля $\mathbb{E}$.

"3) $\Rightarrow$ 4)" При условии 3, $\mathrm{ord}\alpha = q^m - 1$ и $O(M_u) = \mathrm{ord}\alpha$, тогда согласно пункту 2 теоремы 16.5 имеем $T(M_u) = \mathrm{ord}\alpha = q^m - 1$.

"4) $\Rightarrow$ 1)" очевидно. ►

Теорема 16.8 показывает, что задача построения ЛРП максимального периода $q^m - 1$ над полем $\mathbb{F} = GF(q)$ сводится к построению реверсивного многочлена $F(x) \in \mathbb{F}[x]$, удовлетворяющего пункту 3 указанной теоремы.

Определение 16.9. Реверсивный многочлен $F(x) \in \mathbb{F}[x]$ называется *многочленом максимального периода*, или *примитивным* многочленом, над полем $\mathbb{F}$, если он имеет степень m и период $q^m - 1$.

Предложение 16.10. Число многочленов степени m максимального периода $q^m - 1$ над полем $\mathbb{F} = GF(q)$ равно $\frac{1}{m}\varphi(q^m - 1)$, где φ — функция Эйлера.

◄ Из теоремы 16.8 следует, что многочлен $F(x) \in \mathbb{F}[x]$ степени m максимального периода имеет в поле $\mathbb{E} = GF(q^m)$ в точности m корней, каждый из которых является примитивным элементом поля $\mathbb{E}$. Два различных унитарных неприводимых многочлена не могут иметь общий корень над $\mathbb{E}$, так как в этом случае они имели бы общий делитель положительной степени над $\mathbb{E}$, а значит, их НОД над $\mathbb{F}$ был бы положительной степени, что невозможно ввиду неприводимости. Число примитивных элементов вычисляется как число образующих циклической группы $(\mathbb{E}^*, \cdot)$ — оно равно $\varphi(q^m - 1)$. ►
Следующее утверждение даёт критерий проверки того, что многочлен является многочленом максимального периода:

Предложение 16.11. Неприводимый многочлен $F(x) \in \mathbb{F}[x]$ степени $m > 0$ является многочленом максимального периода над полем $\mathbb{F}$ тогда и только тогда, когда $F(x) \neq x$, и для каждого собственного простого делителя d числа $q^m - 1$ выполняется условие

$$x^{\frac{q^m-1}{d}} \neq 1 (\mod F(x)). \tag{16.1}$$

◄ Так как $F(x)$ неприводим над $\mathbb{F} = GF(q)$, то по теореме 16.5 $T(F)|q^m-1$ и условие, что $T(F) < q^m-1$ равносильно тому, что для некоторого собственного простого делителя d числа q^m-1 выполняется условие делимости $T(F)|\dfrac{q^m-1}{d}$, т.е. не выполняется равенство (16.1). ►

Алгоритм построения многочлена максимального периода. Выполняется перебор неприводимых многочленов степени m с проверкой равенства $T(F) = q^m - 1$ с помощью условия (16.1).

Следствие 16.12. Если 2^m-1 — простое число (это так называемые простые числа Мерсенна), то любой неприводимый многочлен над $GF(2)$ степени m есть многочлен максимального периода.

Список литературы

[1] М.М. Глухов, В.П. Елизаров, А.А. Нечаев. Алгебра, т. 1,2. Изд. “Гелиос АРВ”, М., 2003.

[2] В.Л. Куракин, А.А. Нечаев. Линейные коды и полилинейные рекурренты.

[3] Р. Лидл, Г. Нидеррайтер. Конечные поля, т. 1,2. Изд. “Мир”, М., 1988.

[4] В.Т. Марков, Конспект спецкурса “Теория колец” 2016/2017 учебного года. Тема «Кольца и модули в теории кодирования». http://halgebra.math.msu.su/wiki/doku.php/specialcourses:ringtheory

[5] А.А. Нечаев. Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам// Фундаментальная и прикладная математика, 1995, Т.1, № 1, 229-254.