Конспект лекций по курсу

ПРИКЛАДНАЯ АЛГЕБРА

группы 320–325, 327, 328 (III поток)
осенний семестр 2017/18 уч. года

Лектор *С. И. Гуров*
ассистент *Д. А. Кропотов*

(кафедра *Математических методов прогнозирования*)

2017

Предисловие

Мне бы хотелось, ... чтобы все добрые люди, как мужского, так и женского пола, почерпнули бы отсюда урок, что во время чтения надо шевелить мозгами.

Лоренс Стерн. Жизнь и мнения Тристрама Шенди, джентльмена

Данный конспект лекций предназначен, прежде всего, для студентов III-го («программистского») потока студентов-бакалавров факультета ВМК МГУ изучающих в 5-м семестре курс указанный курс.

Заметим, что стиль изложения в учебнике и конспекте лекций различен. Последний более свободный, «разговорный», и содержит, в основном, лишь формулировки определений и теорем (возможно, с доказательствами). В учебнике же данный материал обычно предваряется пояснениями и часто включается в более широкий контекст.

В данном пособии мы, в связи со спецификой преподавания курса, включаем в текст лекций достаточное количество примеров и задач.

Глава 3 написана совместно с Д. А. Кропотовым.

Оглавление

Глава 1

Группы, кольца, поля (напоминание)

1.1 Группы

Определение 1.1. *Группой* называется тройка $\langle G, \circ, e \rangle$, где G — непустое множество (*носитель*), $e \in G$ — единица группы, а $\circ$ — такая бинарная операция на носителе, что для любых его элементов x, y, z выполняются следующие *законы* или *аксиомы группы*:

$[0)$ $x \circ y \in G$ — *устойчивость* (замкнутость) носителя;$]$

1) $(x \circ y) \circ z = x \circ (y \circ z)$ — *ассоциативность*;

2) $e \circ x = x \circ e = x$ — *свойство единицы*;

3) $\forall\, x\ \exists!\, y : y \circ x = x \circ y = e$ — *существование обратного элемента* к x, символически $y = x^{-1}$.

В записи группы обозначение единичного элемента иногда опускают: $\langle G, \circ \rangle$.

Группы со свойством $x \circ y = y \circ x$ называются *коммутативными* или *абелевыми*. Для них используют *аддитивную запись* $x + y$ групповой операции, единичный элемент называют *нулем* (0), а обратный к x — *противоположным* $(-x)$.

Если $|G| = n$, то G — *конечная группа* и n — её *порядок*. В конечной группе операцию $\circ$ удобно задавать *таблицей умножения* (*таблицей Кэли*).

Пример 1.1 (Таблица умножения группы Клейна V_4).

$\circ$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$V_4 = \{e, a, b, ab\}$
— четверная группа Клейна
ab — один элемент,
группа абелева.

Мультипликативная запись групповой операции:

$$x \cdot y \text{ или } xy,\ a^0 = e,\ a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ раз}},\ n \in \mathbb{N},$$

и справедливы все обычные свойства степени:

$$a^{m+n} = a^m \cdot a^n,\ a^{m^n} = a^{mn},\ a^{-1}a = e,\ a^{-n} = (a^{-1})^n,\ \ldots.$$

Пример 1.2.

1. *Числовые группы* — все они абелевы:

   - $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно *сложения*.
   - *Ненулевые* элементы множеств $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно *умножения*.

2. *Бинарные наборы*: $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in B^n$ относительно $\oplus$. Аддитивная запись:

$$\widetilde{\alpha} \oplus \widetilde{\beta} = (\alpha_1 \oplus \beta_1, \ldots, \alpha_n \oplus \beta_n)$$

Нуль группы: $\widetilde{0} = (0, \ldots, 0)$.

3. *Симметрическая группа* S_n: все перестановки n-элементного множества $X = \{1, \ldots, n\}$ относительно композиции $*$. Нуль группы — единичная перестановка 1_X. Ясно, что $|S_n| = n!$.

Перестановки можно записывать в виде:

а) таблицы —

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ t_1 & t_2 & \ldots & t_i & \ldots & t_n \end{pmatrix},$$

Например (сначала выполняется 2-я перестановка, потом — 1-я):

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq$$
$$\neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

б) разложения на циклы —

$$\pi = \left(t_1^1 t_2^1 t_3^1 \ldots t_{k_1}^1\right)\left(t_1^2 t_2^2 t_3^2 \ldots t_{k_2}^2\right)\ldots\left(t_1^m t_2^m t_3^m \ldots t_{k_m}^m\right).$$

Внутри каждой пары скобок числа переставляются циклически:

$$\pi(t_1) = t_2,\ \pi(t_2) = t_3,\ \ldots,\ \pi(t_k) = t_1$$

и перестановка π содержит m циклов.

Циклы длины 1, т. е. вида (t), обычно опускают:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix} \leftrightarrow (154)(26)$$

Каноническое представление цикла $(t_1 t_2 \ldots t_k)$:
t_1 — наименьшее из чисел $\{t_1, t_2, \ldots, t_k\}$.

Например, для предыдущей композиции перестановок:

$$(123) * (23) = (12) \neq (13) = (23) * (123).$$

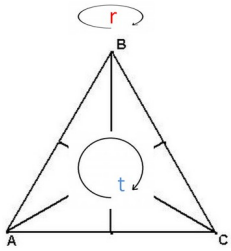
4. *Группы симметрии (самосовмещений) объекта — совокупность преобразований, совмещающих объект с самим собой.*

4.1. Группы *симметрии* правильного n-угольника — *группы диэдра* D_n

а) *У группы* D_{2k+1}, $k \in \mathbb{N}$ — *две* образующих:
(1) вращение вокруг центра на $\frac{360^\circ}{2k+1}$ в выбранном направлении — t и
(2) симметрия относительно оси, проходящей через выбранную вершину и середину противоположной стороны — r.

Например: группа симметрии правильного треугольника — перестановка его вершин

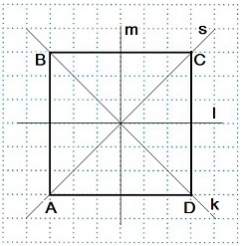
$$D_3 = \langle t, r \rangle = \{ e, (ABC), (ACB), (A)(BC), (B)(AC), (C)(AB) \} = S_3.$$



t — вращение на 120° в выбранном направлении,
r — симметрия относительно выбранной оси симметрии.
Любая перестановка вершин (сторон) описывается через образующие и имеет вид $t^m r^n$.

б) *У группы* D_{2k}, $k \in \mathbb{N}$ — *три* образующих: (1) вращение вокруг центра (в выбранном направлении) на $\frac{360^\circ}{2k}$ и две осевых симметрий — относительно фиксированных осей, проходящих через середины противоположных (2) сторон и (3) вершин.

Пример: группа симметрии квадрата

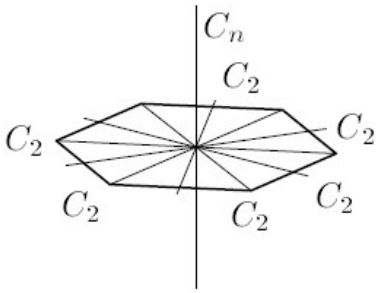


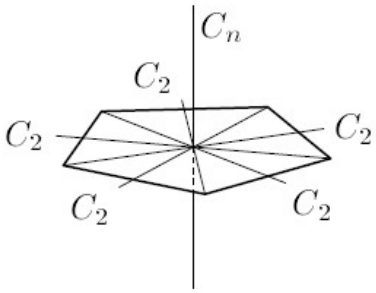
$D_4 = \langle t, r, f \rangle = \{ e, (ABCD), (AC)(BD), (ADCB), (AD)(BC), (AB)(CD), (BD), (AC) \}$.

t — вращение на 90° в выбранном направлении,
r — симметрия относительно оси m,
f — симметрия относительно оси симметрии A-C.

Любая перестановка вершин (сторон) описываться через образующие и имеет вид $t^m r^n f^k$.

Пример: группы диэдра D_6 и D_5.

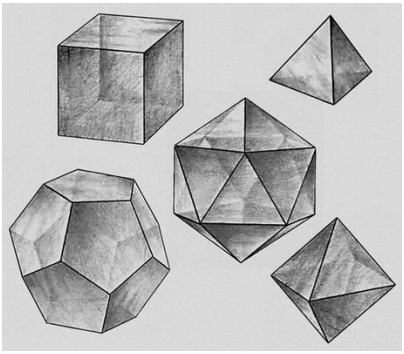




$|D_n| = 2n$: тождественная перестановка + $(n-1)$ поворотов вокруг оси C_n + n отражений вокруг осей C_2.

4.2. Группы *вращений* правильного многогранника — это не все симметрии многогранника, а только повороты, т. е. зеркальные отражения исключены.

Пять платоновых тел —



T — группа тетраэдра,
O — группа октаэдра (вращение октаэдра и куба),
Y — группа икосаэдра (вращение икосаэдра и додекаэдра).

Эти группы будут рассмотрены позже.

Ещё один пример: группа внутренних вращений *кубика Рубика*.

Порядок группы —

$$\frac{1}{2}\cdot 2^{11}\cdot 12!\cdot 3^{7}\cdot 8! = 43252003274489856000 \approx 4{,}3\cdot 10^{19}.$$

что является совсем небольшим числом по стандартам современной теории конечных групп ($\approx$ объём Мирового океана в кубометрах).

Подгруппы и смежные классы. Если $\langle G, \circ \rangle$ — группа, а H — подмножество G, само являющееся группой, то $\langle H, \circ \rangle$ — *подгруппа* G, символически $H \leqslant G$.

Единичная группа $E = \{e\}$ — подгруппа любой группы.

Определение левого и правого *смежных классов по подгруппе* H *(с представителем* x*)* соответственно:

$$H \leqslant G,\ x \in G \ \Rightarrow xH = \{\, xh \mid h \in H \,\},$$
$$Hx = \{\, hx \mid h \in H \,\}.$$

Утверждение 1.1. *Смежные классы (левые или правые) с разными представителями либо не пересекаются, либо совпадают.*

Если $\forall\, x \in G : xH = Hx$, то подгруппа H — *нормальная*. Нормальность — ослабленное условие коммутативности: *в абелевой группе все подгруппы нормальны.*

Определение 1.2. Множество смежных классов группы G по её нормальной подгруппе H снабжённое операцией

$$(aH) \circ (bH) = (ab)H.$$

называется *факторгруппой*, символически G/H.

Легко видеть, что результат $x \circ y$ находится $(ab)H$ не зависимо от выбора элементов x и y в классах смежности aH и bH.

Пример 1.3. $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$.

Определение 1.3. Для групп $\langle\, G, * \,\rangle$ и $\langle\, G', \circ \,\rangle$ отображение $\varphi : G \to G'$ называется *изоморфизмом*, если оно

1) взаимно однозначно (биективно);
2) сохраняет групповую операцию:

$$\forall\, a, b \in G\colon\ \varphi(a * b) = \varphi(a) \circ \varphi(b),$$

а такие группы — *изоморфными*, символически $G \cong G'$.

Свойства изоморфизма φ: $\varphi(e) = e'$ (сохранение единицы), $\varphi(a^{-1}) = \varphi(a)^{-1}$ (образ обратного элемента — обратный к его образу)...

Теорема 1.1 (Кэли). *Любая конечная группа порядка* n *изоморфна некоторой подгруппе симметрической группы* S_n.

Если в определении изоморфизма снять требование биективности φ, то получим определение *гомоморфизма групп*. *Например*, всегда существует гомоморфизм произвольной группы в единичную E.

Циклические группы. В *циклических группах* имеется *порождающий элемент* (*образующий элемент, генератор*) c такой, что каждый элемент группы может быть получен многократным (с учётом $c^0 = e$) применением к нему или к c^{-1} групповой операции, т. е. C — циклическая группа, если

$$\underset{C}{\exists}\, c \; \underset{C}{\forall}\, x \; \underset{\mathbb{Z}}{\exists}\, k \; : \; c^k = x, \quad \text{символически } \langle c \rangle = C.$$

Пример циклической группы: группа $\left\langle \frac{2\pi}{n} \right\rangle$ поворотов n-угольника вокруг центра с совпадающими исходным и полученным положениями.

Для циклических групп возможны два случая.

1. *Все степени порождающего элемента различны* — группа бесконечна, состоит из элементов

$\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$, т. е. она изоморфна группе $\langle\, \mathbb{Z},\, +,\, 0 \,\rangle$ целых чисел *по сложению*. Ясно, что это единственная с точностью до изоморфизма бесконечная циклическая группа.

Сколько в ней генераторов? Два: -1 и $+1$.

2. *Две различные степени порождающего элемента совпадают*: $a^{n+m} = a^n a^m = a^n \;\Rightarrow\; a^m = e$.

   $\operatorname{ord} a \;=\; \arg\min\limits_{m \,\in\, \mathbb{N}_0} \{a^m = e\}$ — *порядок элемента* a.

   В этом случае получаем конечную группу

   $$\mathbb{Z}_n \;=\; \langle\, \{0, 1, \ldots, n-1\},\, +_{\bmod n},\, 0 \,\rangle\,,$$

   которой изоморфны все конечные циклические группы с n элементами.

Все циклические группы абелевы и любая подгруппа циклической группы — циклическая.

В применении к единственной бесконечной циклической группе $\mathbb{Z}$ это даёт, что любая конечная подгруппа H группы $\mathbb{Z}$ имеет вид $H = \{\, mn \mid n \in \mathbb{Z} \,\} = m\mathbb{Z}$, где m — наименьшее положительное число из H. Поэтому *любая циклическая группа является гомоморфным образом группы* $\mathbb{Z}$.

Определение 1.4. Значение *функции Эйлера* $\varphi(n)$ — количество чисел из интервала $[\,1, \ldots, n-1\,]$, взаимно простых с n. По определению $\varphi(1) = 1$.

$\varphi(2) = 1$, при $n > 2$ значения функция Эйлера чётные

$$\varphi(3) = \varphi(4) = 2,\ \varphi(5) = 4,$$
$$\varphi(6) = \big|\{1,5\}\big| = 2,\ \varphi(7) = 6,\ \varphi(8) = 4,\ \ldots$$

Свойства (p здесь и далее — простое):

- $\varphi(p) = p - 1$;
- $\varphi(n^k) = n^{k-1}\varphi(n)$, откуда $\varphi(p^k) = p^{k-1}(p-1)$,
- если m и n *взаимно просты*, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Примеры: $\varphi(15) = \varphi(3{\cdot}5) = \varphi(3){\cdot}\varphi(5) = 2{\cdot}4 = 8$
$\varphi(16) = \varphi(2^4) = 2^3 \cdot 1 = 8.$

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Рис. 1.1. Первые 99 значений $\varphi(\cdot)$

- $\sum\limits_{d|n} \varphi(d) = n$. *Пример:*
  $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$;

У циклической группы порядка n существует ровно $\varphi(n)$ порождающих элементов (генераторов).

Теорема Лагранжа и следствия из неё

Теорема 1.2 (Лагранжа). *Порядок подгруппы конечной группы делит порядок самой группы:*

$$|G| = |H| \cdot [G : H].$$

$[G : H]$ — *индекс* подгруппы H по группе G.

Следствия. 1. *Порядок любого элемента конечной группы делит порядок группы.*

2. *Группа G простого порядка p:*
   - *не имеет нетривиальных (отличных от E и G) подгрупп;*
   - *циклическая и любой её отличный от единицы элемент — порождающий.*

1.2 Кольца и поля

Кольца: определение, основные свойства

Определение 1.5. Абелева группа $\langle R, +, 0 \rangle$ называется *кольцом*, символически $\langle R, +, \cdot, 0 \rangle$, если на ней определена бинарная операция *умножения* $\cdot$, связанная со сложением *дистрибутивными законами*

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{и} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Обычно рассматривают *ассоциативные кольца* с ассоциативной операцией умножения:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

Важный случай — *коммутативные кольца* с коммутативной операцией умножения:

$$x \cdot y = y \cdot x.$$

Если в кольце имеется единичный элемент 1 по умножению ($x \cdot 1 = 1 \cdot x = x$), то кольцо называется *кольцом с единицей* или *унитальным*, символически $\langle R, +, \cdot, 0, 1 \rangle$. *Тривиальное кольцо* — $\{0\}$, в нём и только в нём $0 = 1$.

Элемент a унитального кольца называется *обратимым*, если существует элемент b такой, что

$$a \cdot b = b \cdot a = 1.$$

Кольцо R *без делителей нуля* — со свойством

$$\underset{R}{\forall} a, b : (a \cdot b = 0) \Rightarrow (a = 0) \vee (b = 0).$$

Важное для нас

Определение 1.6. *Целостным кольцом* (областью целостности) называют нетривиальное унитальное ассоциативно-коммутативное кольцо без делителей нуля.

Пример 1.4.

1. Классический пример кольца — кольцо целых чисел $\mathbb{Z}$ с обычными операциями сложения и умножения. Это кольцо целостно и имеет два обратимых элемента: $+1$ и -1.
2. $2\mathbb{Z}$ — кольцо без единицы.
3. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ — *кольцо классов вычетов по модулю* n (*вычет* = *остаток*), результаты операций $+$ и $\cdot$ — по $\bmod n$.

   Это кольцо нецелостно при составном n: например в $\mathbb{Z}_6$: $3 \cdot 2 = 0$.

Определение 1.7. Непустое подмножество S кольца $\langle\, R, +, \cdot, 0\,\rangle$ называется его *подкольцом*, если оно устойчиво относительно вычитания (тогда и $0 \in S$) и произведения своих элементов.

Подкольцо *собственное*[1], если $S \neq R$.

При $n < m$ кольцо $\mathbb{Z}_n$ не есть подкольцо $\mathbb{Z}_m$: например, в $\mathbb{Z}_5$ — $3 \cdot 3 = 4$ и $3 + 3 = 1$, а в $\mathbb{Z}_8$ — $3 \cdot 3 = 1$ и $3 + 3 = 6$. Образно говоря, элементы 3 в этих кольцах суть *омонимы* — одинаково звучащие слова с разным смыслом.

Определение 1.8. Целостное кольцо, в котором каждый ненулевой элемент либо обратим, либо однозначно представляется в виде произведения неразложимых элементов с точностью до перестановки сомножителей и умножения на обратимый элемент, называется *факториальным* или *гауссовым*.

Примеры:

- $\mathbb{Z}$ — факториальное кольцо: для любого целого n справедливо представление
$$n \;=\; p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}.$$
- Кольцо $\mathbb{Z}_n$ является факториальным если и только если n просто.
- Кольцо $\left\{\, a \pm i\sqrt{5} \;\middle|\; a \in \mathbb{R} \,\right\}$ не факториально, т. к., например, число 9 имеет два представления в виде произведения неразложимых:
$$9 \;=\; 3 \cdot 3 \;=\; \left(2 + i\sqrt{5}\right) \cdot \left(2 - i\sqrt{5}\right).$$

[1] Кстати, термин *собственный* — неудачный перевод слова *proper*, следовало бы говорить *правильный* или *настоящий*, но так уж исторически сложилось и не исправить...

Идеалы колец и факторкóльца

Определение 1.9. Подмножество I коммутативного кольца $\langle R, +, \cdot, 0 \rangle$ называется его *(двусторонним) идеалом* [2], символически $I \lhd R$, если оно устойчиво относительно вычитания и $\underset{I}{\forall}\, i\ \underset{R}{\forall}\, r : i \cdot r \in I$.

Ясно, что идеал кольца R является его подкольцом и 0 принадлежит любому идеалу. Само кольцо и его нуль 0 — *тривиальные идеалы* кольца. Идеалы, не совпадающие со всем кольцом — *собственные*.

Можно определить сумму и произведение идеалов и работать с ними как с «идеальными числами» (это понятие вводится в работах Э. Куммера).

Определение 1.10. Идеал I унитального коммутативного кольца R называется *главным* и *порождённым элементом* $a \in R$, если

$$I = \{\, a \cdot r \mid r \in R \,\} = (a).$$

Целостные кольца, в которых все идеалы главные, называются *кольцами главных идеалов* (*КГИ*).

Все КГИ факториальны.

Кольцо целых $\mathbb{Z}$ — КГИ, и все его идеалы имеют вид $(n) = n\mathbb{Z}$.

Пример правого неглавного идеала в кольце матриц порядка n: совокупность матриц, у которых все столбцы, кроме 1-го — нулевые.

[2] Для некоммутативного кольца вводят понятия *правых* и *левых идеалов*, но они нам не понадобятся.

Классом вычетов по модулю идеала I *кольца* $\langle R, +, \cdot, 0 \rangle$ с представителем $r \in R$, называют множество

$$\overline{r}_I = \{ r + i \mid i \in I \}$$

(когда идеал фиксирован, класс вычетов вычетов обозначаем $\overline{r}$). Классы вычетов разных представителей по модулю данного идеала либо совпадают, либо не пересекаются и в объединении дают R, т. е. образуют *разбиение* кольца.

Множество классов вычетов кольца R по модулю идеала I образуют *факторкольцо*, символически R/I. В факторкольце естественным образом определены операции сложения и умножения, индуцированные операциями над представителями.

Пример 1.5. $I = (4) \lhd \mathbb{Z}$, $\quad \mathbb{Z}/(4) = \{ 0, 1, 2, 3 \}$.

$$\overline{1} + \overline{2} = \overline{3}, \quad \overline{3} + \overline{1} = \overline{0},$$
$$\overline{2} \cdot \overline{2} = \overline{0}, \quad \overline{3} \cdot \overline{2} = \overline{2} \text{ и т. д.}$$

Бинарное отношение $\lhd$ на множестве идеалов кольца является *частичным порядком.*

Определение 1.11. *Максимальным идеалом* коммутативного кольца называется всякий собственный идеал кольца, не содержащийся ни в каком другом собственном идеале.

Пример 1.6. В кольце $\mathbb{Z}$

1) идеалы (2) и (3) максимальны;
2) идеал (6) не максимален: он содержится и в (2), и в (3): любое число, делящееся на 6 делится также и на 2, и на 3.

Ясно, что в $\mathbb{Z}$ максимальные идеалы имеют вид (p), где p — простое число.

Утверждение 1.2. *В ассоциативно-коммутативном унитальном кольце существует максимальный идеал.*

Евклидовы кольца

Определение 1.12. Целостное кольцо $\langle R, +, \cdot, 0, 1 \rangle$ называется *евклидовым*, если для каждого его ненулевого элемента x определена норма $N(x) \in \mathbb{N}_0$ со свойствами для любых элементов a и $b \neq 0$:

1) существуют такие его элементы q и r, что
$$a = q \cdot b + r \quad \text{и либо } r = 0, \quad \text{либо } N(r) < N(b);$$

2) $a \mid b \Rightarrow N(a) \leqslant N(b)$.

Наличие нормы даёт возможность производить деление элементов кольца друг на друга с остатком.

Пример 1.7.
- Кольцо целых чисел $\mathbb{Z}$ евклидово, норма — абсолютная величина числа.
- Кольцо многочленов $\mathbb{R}[x]$ с действительными коэффициентами евклидово. Норма — степень многочлена.

Все евклидовы кольца — КГИ.

Поле

Определение 1.13. Целостное кольцо $\langle R, +, \cdot, 0, 1 \rangle$, в котором все элементы кроме 0 обратимы, называется *полем*.

Для нас важны следующие свойства поля:

1. Ненулевые элементы поля образуют группу относительно *умножения*, её называют *мультипликативной группой* данного поля.
2. Факторкольцо R/I является полем если и только если идеал I кольца R *максимальный*.
3. Кольцо многочленов $\Bbbk[x]$ над полем $\Bbbk$

$$\Bbbk[x] = \{ a_n x^n + \ldots + a_1 x + a_0 \mid a_0, \ldots, a_n \in \Bbbk, \; n = 0, 1, \ldots \}$$

евклидово.

Подмножество поля K, само являющееся полем и устойчивое относительно сужения на него операций из K, называется *подполем. Примеры бесконечных полей и подполей*: числовые поля $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Поле K, не обладающее никаким собственным подполем, называется *простым*. Например, поле $\mathbb{Q}$ — простое.

Утверждение 1.3. *В каждом поле содержится только одно простое подполе, которое изморфно либо* $\mathbb{Q}$, *либо* $\mathbb{Z}_p$, p — *простое.*

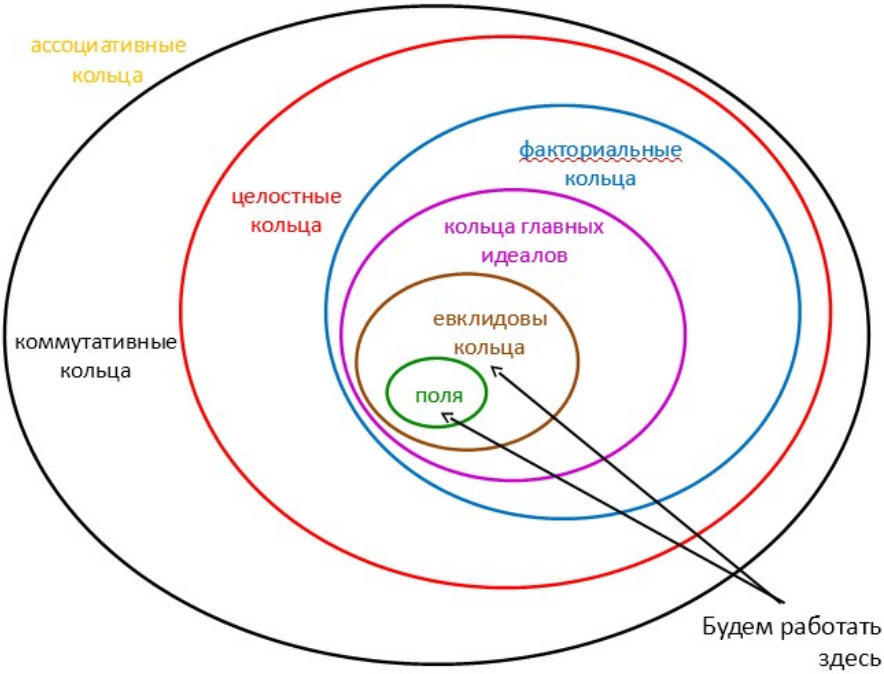


Рис. 1.2. От колец к полям

1.3 Задачи с решениями

Задача 1.1. *Выяснить, образуют ли группы следующие множества при указанной операции над элементами:*

1. Целые числа, кратные данному натуральному числу n, относительно сложения? *Да.*
2. Неотрицательные целые числа относительно сложения? *Нет* (противоположного элемента)
3. Нечетные целые числа относительно сложения? *Нет* (устойчивости)
4. Целые числа относительно вычитания? *Нет* (ассоциативности).

5. Рациональные числа относительно умножения? *Нет* (обратного у 0).

6. Рациональные числа, отличные от нуля, относительно умножения? *Да.*

7. Положительные рациональные числа относительно умножения? *Да.*

8. Положительные рациональные числа относительно деления? *Нет* (ассоциативности).

9. Корни n-й степени из единицы (как действительные, так и комплексные) относительно умножения? *Да.*

10. Матрицы порядка n с действительными элементами относительно умножения? *Нет* (обратных у всех).

11. Невырожденные матрицы порядка n с действительными элементами относительно умножения? *Да.*

12. Перестановки чисел $1, 2, \ldots, n$ относительно композиции перестановок? *Да.*

13. Преобразования множества M, т. е. взаимно однозначные отображения этого множества на себя, относительно композиции отображений? *Да.*

14. Элементы n-мерного векторного пространства $\mathbb{R}^n$ относительно сложения? *Да.*

15. Параллельные переносы трехмерного пространства $\mathbb{R}^3$ относительно композиции движений? *Да.*

16. Повороты трехмерного пространства $\mathbb{R}^n$ вокруг прямых, проходящих через данную точку O относительно композиции движений? *Да.*
17. Все движения трехмерного пространства $\mathbb{R}^n$ относительно композиции движений? *Да.*

Задача 1.2. *Найти степени и порядки всех элементов циклической группы 6-го порядка.*
Какие из них являются порождающими?

Решение. Любая циклическая 6-элементная группа изоморфна $\mathbb{Z}_6 = \langle \{0, 1 \ldots, 5\}, +, 0 \rangle$.

$\operatorname{ord} 0 = 1;$

$1, 1+1 = 2, \ldots = 6 \cdot 1 = 0 \Rightarrow \operatorname{ord} 1 = 6;$

$2, 2+2 = 4, 4+2 = 0 \Rightarrow \operatorname{ord} 2 = 3;$

$3, 3+3 = 0 \Rightarrow \operatorname{ord} 3 = 2;$

$4, 4+4 = 2, 2+4 = 0 \Rightarrow \operatorname{ord} 4 = 3;$

$5, 5+5 = 4, 4+5 = 3, \ldots, 6 \cdot 5 = 0 \Rightarrow \operatorname{ord} 5 = 6.$

Порождающие элементы — 1 и 5 с порядком 6.

Задача 1.3. *Найти все подгруппы и порождающие элементы циклической группы порядка* 24.

Решение. Любая циклическая 24-элементная группа изоморфна $Z_{24} = \langle \{0, 1, \ldots, 23\}, +, 0 \rangle$.

1. Все подгруппы циклической группы — циклические. Порождающими элементами подгрупп Z_{24} будут делители m порядка группы 24: т. е. $m = 1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 24 \equiv 0$.

Порядок соответствующей подгруппы — $24/m$.

$m = 1 : \{ 1, 2, \ldots, 23, 0 \} = \langle 1 \rangle = C \cong \mathbb{Z}_{24}$;
$m = 2 : \{ 2, 4, 6, \ldots, 22, 0 \} = \langle 2 \rangle \cong \mathbb{Z}_{12}$;
$m = 3 : \{ 3, 6, 9, \ldots, 21, 0 \} = \langle 3 \rangle \cong \mathbb{Z}_{8}$;
$m = 4 : \{ 4, 8, 12, \ldots, 20, 0 \} = \langle 4 \rangle \cong \mathbb{Z}_{6}$;
$m = 6 : \{ 6, 12, 18, 0 \} = \langle 6 \rangle \cong \mathbb{Z}_{4}$;
$m = 8 : \{ 8, 16, 0 \} = \langle 8 \rangle \cong \mathbb{Z}_{3}$;
$m = 12 : \{ 12, 0 \} = \langle 12 \rangle \cong \mathbb{Z}_{2}$;
$m = 24 : \{ 0 \} = \langle 0 \rangle \cong E$ — единичная.

2. Циклическая группа Z_{24} имеет $\varphi(24) = \varphi(2^3 \cdot 3) = 2^2 \cdot \varphi(2) \cdot \varphi(3) = 4 \cdot 1 \cdot 2 = 8$ генераторов m, взаимно простых с 24, т. е. $m = 1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23$.

Задача 1.4. *Показать, что*

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right),$$

если $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ *— примарное разложение* n.

Решение.

$$\begin{aligned}
\varphi(n) &= \varphi\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k}\right) = p_1^{\alpha_1 - 1} \varphi(p_1) \cdot \ldots \cdot p_k^{\alpha_k - 1} \varphi(p_k) = \\
&= p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} \varphi(p_1) \cdot \ldots \cdot \varphi(p_k) = \\
&= \frac{n}{p_1 \cdot \ldots \cdot p_k} (p_1 - 1) \cdot \ldots \cdot (p_k - 1) = \\
&= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

Задача 1.5. *Выяснить, какие из следующих множеств являются кольцами, а какие полями относительно естественных операций на них.*

1. Рациональные числа $\mathbb{Q}$? Поле.
2. Квадратные матрицы порядка n с *действительными* элементами относительно сложения и умножения матриц?
   Кольцо (обратной матрицы может не быть).
3. Многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения?
   Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ в случае $a_0 = 0$ необратимы).
4. Многочлены от одного неизвестного x с действительными коэффициентами относительно обычных операций?
   Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ в случае $a_0 = 0$ необратимы).

Задача 1.6.

Определение 1.14. Пусть $\langle R, +, \cdot \rangle$ и $\langle R', \oplus, \otimes \rangle$ — кольца. Отображение $\varphi : R \to R'$ называется *гомоморфизмом*, если

$$\varphi(r_1 + r_2) = \varphi(r_1) \oplus \varphi(r_2), \quad \varphi(r_1 \cdot r_2) = \varphi(r_1) \otimes \varphi(r_2).$$

Взаимно-однозначный гомоморфизм колец называется их *изоморфизмом*, символически $R \cong R'$.

Является ли отображение $f : \mathbb{Z} \to 2\mathbb{Z}$, $f(x) = 2x$ *гомоморфизмом колец?*

Решение. Нет!
Хотя $f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$, но $f(xy) = 2xy \neq (2x) \cdot (2y) = f(x) \cdot f(y)$.

Задача 1.7. *Является ли поле* $\mathbb{Z}_2$ *подполем поля* $\mathbb{Z}_5$*?*

Решение. Нет!
В $\mathbb{Z}_2 : 1 + 1 = 0$, а в $\mathbb{Z}_5$: $1 + 1 = 2$,
т. е. операция сложения в $\mathbb{Z}_5$ неустойчива при переходе к своему подмножеству $\{0, 1\}$.

Глава 2

Конечные поля

2.1 Поля вычетов

- $\mathbb{Z}$ — кольцо целых чисел.
- p — простое число.
- $(p) = p\mathbb{Z} = \{ 0, \pm p, \pm 2p, \ldots \}$ — *идеал*, порождённый числом p.
- $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z} = \{ \overline{0}, \overline{1}, \ldots, \overline{p-1} \}$ — *кольцо вычетов по модулю этого идеала* = классы остатков от деления на p:

$$\left.\begin{array}{ll} \overline{0} & = 0 + (p)\,, \\ \overline{1} & = 1 + (p)\,, \\ \ldots & \ldots\ldots \\ \overline{p-1} & = p - 1 + (p) \end{array}\right\} \Rightarrow \mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{p-1}.$$

Черту над символами классов вычетов часто не ставят.

Поскольку p — простое, то $\mathbb{Z}/(p)$ — не просто p-элементное факторкольцо, а *поле*, точнее *простое поле Галуа*, обозначение — $\mathbb{F}_p$ или $GF(p)$[1]. В нём результаты всех операций берутся по $\mod p$ и каждый ненулевой элемент обратим.

[1] первым обозначением обычно пользуются математики, а вторым — специалисты computer science

Примеры: таблицы сложения и умножения в поле $\mathbb{F}_3$ и фактор-кольце $\mathbb{Z}/(4)$ —

$\mathbb{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}/(4)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

В факторкольце $\mathbb{Z}/(4) \cong \mathbb{Z}_2 :\ 2 \times 2 = 0$!
Однако поле из 4-х элементов существует...

Характеристика поля. Пусть $\Bbbk$ — произвольное поле, 1 — его единица.
Складываем единицы: $1 = 1\,, \quad 1+1 = 2\,, \quad \ldots$.

В конечном поле всегда найдётся первое k такое, что

$$\underbrace{1 + \ldots + 1}_{k \text{ раз}} = 0.$$

Тогда k — *порядок аддитивной группы поля* $\Bbbk$ = = *характеристика поля* $\Bbbk$, символически $\operatorname{char} \Bbbk$.

Ясно, что $\operatorname{char} \Bbbk$ — простое число: иначе, если $\operatorname{char} \Bbbk = p \cdot q$, то получим $(p \cdot 1) \cdot (q \cdot 1) = 0$, т. е. наличие делителей нуля.

Если все суммы вида $1 + \ldots + 1$ различны, то полагают $\operatorname{char} \Bbbk = 0$ (а не ∞). Числовые поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — нулевой характеристики.

$\{0, 1, \ldots, \operatorname{char} \Bbbk - 1\} \cong \mathbb{Z}_{\operatorname{char} \Bbbk}$ — минимальное *подполе* любого поля $\Bbbk$ положительной характеристики.

Пример 2.1 (бесконечное поле с положительной характеристикой). Пусть $\Bbbk$ — некоторое поле. Построим:

1. $\Bbbk[x]$ — *кольцо многочленов* (от *формальной* переменной x) над полем $\Bbbk$:
$$\left\{ P(x) = a_0 + a_1 x + \ldots + a_n x^n \mid a_0, \ldots, a_n \in \Bbbk \right\};$$
$$\Bbbk[x] \leftrightarrow \left\{ (a_0, \ldots, a_n) \in \Bbbk^n \mid n \in \mathbb{N}_0 \right\}.$$

2. $\Bbbk(x)$ — *поле рациональных функций над* $\Bbbk$. Его элементами являются "дроби" P/Q (если $Q \neq 0$), где $P, Q, U, V \in \Bbbk[x]$ с отношением эквивалентности и операциями сложения, умножения и деления аналогичными для рациональных чисел в форме простых дробей.
При этом каждый многочлен $P \in \Bbbk[x]$ отождествляется с $P/1 \in \Bbbk(x)$, т. е. $\Bbbk[x] \subset \Bbbk(x)$.

Если в качестве $\Bbbk$ взять $\mathbb{F}_p$, то $\mathbb{F}_p(x)$ — *бесконечное поле положительной характеристики* p.

В конечном поле возможно сильное упрощение вычисления степеней сумм:

Лемма 2.1 (тождество Фробениуса). *В поле характеристики* $p > 0$ *выполнено тождество*
$$(a + b)^p = a^p + b^p.$$

Доказательство. В любом коммутативном кольце верна формула для степени бинома

$$(a+b)^p = a^p + \underbrace{C_p^1 a^{p-1}b + \ldots + C_p^{p-1}ab^{p-1}}_{=0} + b^p,$$

а при $i = 1, \ldots, p-1$

$$C_p^i = \frac{p!}{i!(p-i)!} = p \cdot \frac{(p-1)!}{i!(p-i)!} \equiv_p 0. \qquad \square$$

Следствие. *В поле характеристики* $p > 0$ *справедливо*

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

Мультипликативная группа и примитивный элемент конечного поля.

Обозначим $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ мультипликативную группу поля Галуа $GF(q)$, содержащего q элементов.

Утверждение 2.1. $\mathbb{F}_q^*$ — *циклическая по умножению группа порядка* $|q-1|$.

Мультипликативная циклическая группа $\mathbb{F}_p^*$ простого поля Галуа $\mathbb{F}_p$ содержит $p-1$ элементов, из них $\varphi(p-1)$ генераторов (любой элемент является одной из степеней $\{1, \ldots, p-1\}$ генератора).

Генераторы мультипликативной группы называют *примитивными элементами* поля.

Пример. Рассмотрим поле $\mathbb{F}_{11}$. Его мультипликативная группа есть $\mathbb{F}_{11}^* \cong \langle \{1, 2 \ldots, 10\}, \cdot 1 \rangle$ и она имеет $\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$ генераторов.

Поскольку элемент 1 не примитивен, проверяем элемент 2:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	5	10	9	7	3	6	1

— т. е. элемент 2 — примитивный в $\mathbb{F}_{11}^*$, т. к. $\operatorname{ord} 2 = 10$.

Проверяем элемент 3:

k	1	2	3	4	5
3^k	3	9	5	4	1

— т. е. $\operatorname{ord} 3 = 5$ и 3 — не примитивный, и т.д.

Как ускорить процесс?

Если примарное разложение числа $p-1$

— *известно* $\Rightarrow$ элемент $\alpha \in \mathbb{F}_p^*$ примитивен iff

$\alpha^{\frac{p-1}{q}} \not\equiv_p 1$ для каждого простого $q \mid (p-1)$.

Пример: 1) $p = 11$ (наш случай), $p-1 = 10 = 2 \cdot 5$, проверяем степени q из множества $\left\{ \frac{10}{2} = 5,\ \frac{10}{5} = 2 \right\}$:

$2^2 = 4 \neq 1,\ 2^5 = 32 \equiv_{11} 10 \neq 1 \Rightarrow 2$ — *примитивный*,

$3^2 = 9 \neq 1,\ 3^5 = 243 \equiv_{11} 1 \Rightarrow 3$ — не примитивный.

2) $p = 37$, $p-1 = 36 = 2^2 \cdot 3^2$. Находим: $\frac{36}{2} = 18$, $\frac{36}{3} = 12$; поэтому для выяснения, является ли α генератором, нужно проверить не более двух равенств: $\alpha^{12} = 1$ и $\alpha^{18} = 1$.

— *неизвестно* $\Rightarrow$ эффективного алгоритма не найдено; используют таблицы, вероятностные алгоритмы...

Если найден один примитивный элемент α поля $\mathbb{F}_p$, то любой другой его примитивный элемент может быть получен как степень α^k, где k — взаимно просто с $p-1$.

Пример (наш): $p = 11$ и 2 — примитивный элемент $\mathbb{F}_{11}$; $k \in \{1, 3, 7, 9\}$ — взаимно простые с 10, получим

$$2^1 = 2, \qquad 2^3 = 8,$$

$$2^7 = 128 \equiv_{11} 7, \qquad 2^9 = 512 \equiv_{11} 6,$$

т. е. 6, 7 и 8 — также примитивные элементы $\mathbb{F}_{11}$.

Деление в кольце многочленов. Поскольку кольцо многочленов $\Bbbk[x]$ над полем $\Bbbk$ евклидово, значит многочлены можно делить друг на друга с остатком.

Пример 2.2. В кольце $\mathbb{Z}_2[x]$ разделим «уголком» многочлен $f(x) = x^7 + x^4 + x^2 + 1$ на $g(x) = x^3 + x + 1$ с остатком:

$$\begin{array}{rl|l} -x^7+ & x^4+x^2+1 & x^3+x+1 \\ \underline{x^7+x^5+x^4} & & \underline{x^4+x^2+1} \\ -x^5+ & x^2+1 & \\ \underline{x^5+x^3+x^2} & & \\ -x^3+ & 1 & \\ \underline{x^3+x+1} & & \\ x & & \end{array}$$

Итак, $f(x) = g(x)(x^4 + x^2 + 1) + x$.

Самостоятельно: покажите, что частное от деления многочлена $2x^5 + x^4 + 4x + 3$ на многочлен $3x^2 + 1$ в кольце $\mathbb{F}_5[x]$ есть $4x^3 + 2x^2 + 2x + 1$, а остаток — $2x + 2$.

Неприводимые многочлены. Кольцо многочленов $\Bbbk[x]$ над полем $\Bbbk$ евклидово, следовательно оно факториально, и каждый многочлен однозначно с точностью до перестановок разлагается в произведение неразложимых (неприводимых).

Неразложимые элементы колец $\Bbbk[x]$ называют *неприводимыми многочленами*; например, все линейные многочлены (1-й степени) неразложимы.

Свойство «неприводимости» зависит от поля: многочлен $x^2 + 1$ неприводим в над $\mathbb{R}[x]$, но приводим над $\mathbb{F}_2[x]$: $x^2 + 1 = (x + 1) \cdot (x + 1)$.

Вопрос: как находить неприводимые многочлены в кольце многочленов над данным полем?

Многочлены с коэффициентами из:

$\mathbb{Q}$ — существуют неприводимые многочлены произвольной степени;

$\mathbb{R}$ — неприводимы линейные многочлены и квадратные с отрицательным дискриминантом;

$\mathbb{C}$ — неприводимы только линейные многочлены.

Далее нас будут интересовать неприводимые многочлены в кольцах над простыми полями Галуа.

Ясно, что количество *нормированных многочленов* степени n над полем $\mathbb{F}_p$, т. е. вида

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, \;\; a_i \in \mathbb{F}_p, \; i = \overline{0, n-1},$$

равно p^n.

Неприводимые многочлены кольца $\mathbb{F}_2[x]$ степеней $2, \ldots, 5$.

Вторая степень: $x^2 + ax + b$.
Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a) \;\Rightarrow$ ищем неприводимый многочлен в виде $x^2 + ax + 1$.
Если $a = 0$, то $x^2 + 1 = (x + 1)^2$;
$a = 1$, то получаем *единственный* неприводимый многочлен степени 2 над $\mathbb{F}_2$: $x^2 + x + 1$.

Третья степень: $x^3 + ax^2 + bx + 1$.

Исключая, как сделано ранее, делимость на $x + 1$, получаем условие $a + b = 1$, т. е.

$$\text{либо } a = 0,\, b = 1, \quad \text{либо } a = 1,\, b = 0.$$

Следовательно над $\mathbb{F}_2$ существует два неприводимых многочлена степени 3:

$$x^3+x^2+1 \quad \text{и} \quad x^3+x+1\,.$$

Четвёртая степень: $x^4+ax^3+bx^2+cx+1$.
Исключение делимости на $x+1$ приводит к условию $a+b+c=1$, т. е. имеется 4 варианта, которые дают:

a	b	c	многочлен
0	0	1	x^4+x+1
0	1	0	$x^4+x^2+1=(x^2+x+1)^2$ — *приводимый*
1	0	0	x^4+x^3+1
1	1	1	$x^4+x^3+x^2+x+1$

Пятая степень: $x^5+ax^4+bx^3+cx^2+dx+1$.
Исключение делимости на $x+1$ приводит к условию: число ненулевых коэффициентов a, b, c, d должно быть нечётно, т. е. либо 1, либо 3, что даёт 8 многочленов. Далее необходимо исключить делимость на многчлены 2-й и 3-й степени, но неприводимых многочленов 2-й степени один, а 3-й — два, и их произведение даёт два многочлена.

Итого: существует 6 неприводимых многочленов 5-й степени, вот они —

$$\begin{aligned} &x^5+x^2+1, && x^5+x^3+1,\\ &x^5+x^3+x^2+x+1, && x^5+x^4+x^2+x+1,\\ &x^5+x^4+x^3+x+1, && x^5+x^4+x^3+x^2+1. \end{aligned}$$

Неприводимые многочлены кольца $\mathbb{F}_3[x]$.

Все линейные многочлены:

$$x \qquad x+1 \qquad x+2$$
$$2x \qquad 2x+1 \qquad 2x+2$$

Неприводимые многочлены *степени* 2 в $\mathbb{F}_3[x]$ (они не имеют корней 0, 1, 2):

$$x^2+1 \qquad 2x^2+2$$
$$x^2+x+2 \qquad 2x^2+x+1$$
$$x^2+2x+2 \qquad 2x^2+2x+1$$

Теорема 2.1 (о существовании неприводимых многочленов). *Для любых простого* p *и натурального* n *в* $\mathbb{F}_p[x]$ *существует неприводимый многочлен степени* n.

— докажем позже.

Итак, в кольцах $\mathbb{F}_p[x]$ *есть неприводимые многочлены любой степени, но как их найти?*
Ответ: *нет эффективных алгоритмов*; имеются таблицы, алгоритм из 5-й главы «Алгебры» Ван дер Вардена, алгоритм Берлекэмпа...

Расширения простых полей. *Зачем нужны неприводимые многочлены?* С их помощью можно строить *новые конечные поля — расширения* простых полей аналогично построению самого простого поля $\mathbb{F}_p$:

1. Выбираем простое p — фиксируем поле $\mathbb{F}_p$.
2. Рассматриваем кольцо $\mathbb{F}_p[x]$ многочленов над $\mathbb{F}_p$.

3. Выбираем натуральное n и *неприводимый многочлен* над $\mathbb{F}_p$ —
$$a(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x],\ a_n \neq 0.$$

4. Идеал $(a(x))$ порождает фактор-кольцо $\mathbb{F}_p[x]/(a(x))$, элементы которого суть совокупности $\overline{r(x)}$ многочленов, дающих при делении на $a(x)$ остаток $r(x)$.

Иногда говорят, что элементы $f, g \in \overline{r(x)}$ *сравнимы по двойному двойному модулю* — p и $a(x)$:
$$a(x), f(x), g(x) \in \mathbb{F}_p[x], \quad f(x) \equiv_{a(x)} g(x).$$

Утверждение 2.2. *Множество* $\left\{\overline{r(x)}\right\}$ *является полем Галуа* $GF(p^n)$.

Доказательство. Кольцо многочленов $\mathbb{F}_p[x]$ евклидово, идеал $(a(x))$ — максимальный $\Rightarrow \left\{\overline{r(x)}\right\}$ — поле.

Его мощность = число многочленов над $\mathbb{F}_p$ степени не выше $n-1 = |\{a_0, \ldots, a_{n-1}\}| = p^n$. □

Поле $\left\{\overline{r(x)}\right\} = GF(p^n) = \mathbb{F}_p^n$ называется *расширением n-й степени* простого поля $\mathbb{F}_p$.

Почему в обозначении $\mathbb{F}_p^n$ не используется многочлен $a(x)$, с помощью которого построено поле?

Теорема 2.2. *Любое конечное поле изоморфно какому-нибудь полю Галуа $\mathbb{F}_p^n$, p — простое, n — натуральное.*

Пример 2.3 (построение поля $\mathbb{F}_3^2$). Выберем в $\mathbb{F}_3[x]$ неприводимый многочлен: пусть это будет x^2+1. Тогда искомое поле 9-элементное поле есть

$$\mathbb{F}_3^2 \cong \mathbb{F}_3[x]/\big(x^2+1\big) = \\ \big\{\,\overline{0},\,\overline{1},\,\overline{2},\,\overline{x},\,\overline{x+1},\,\overline{x+2},\,\overline{2x},\,\overline{2x+1},\,\overline{2x+2}\,\big\}.$$

Можно составить таблицы сложения и умножения в этом поле с учётом $x^2 = -1 \equiv_3 2$.
Например:

$$\overline{x+1}+\overline{x+2}=\overline{2x}, \qquad \overline{x}\cdot\overline{2x}=\overline{1},$$
$$\overline{2x+1}+\overline{x}=\overline{1}, \qquad \overline{2x+1}\cdot\overline{x}=\overline{x+1}, \quad \text{и т.д.}$$

Черту над элементами поля $\mathbb{F}_p[x]/(a(x))$ обычно не ставят и называют их «многочленами». Но надо помнить, что это *совокупности* многочленов, дающих при делении на $a(x)$ один и тот же остаток.

Заметим, что в построенном поле $\mathbb{F}_3^2$:

$$(x+1)^1 = x+1, \qquad (x+1)^5 = 2x+2,$$
$$(x+1)^2 = 2x, \qquad (x+1)^6 = x,$$
$$(x+1)^3 = 2x+1, \qquad (x+1)^7 = x+2,$$
$$(x+1)^4 = 2, \qquad (x+1)^8 = 1.$$

Это значит, что $x+1$ — примитивный элемент $\mathbb{F}_3^2$ (а x — нет, поскольку $x^4 = 4 \equiv_3 1$).

А что будет, если при построении поля вместо x^2+1 взять другой неприводимый в $\mathbb{F}_3[x]$ многочлен? Например, $2x^2+x+1$? Получится поле, *изоморфное построенному*.

Пример 2.4. Определить, является ли:

1. Многочлен $a(x) = x^3 + 2x + 4 \in \mathbb{F}_5[x]$ — неприводимым?
2. Элемент $4x^2 + 2$ — корнем $a(x)$ в факторкольце/поле $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$?

Решение. 1. Перебором элементов из $GF(5)$ —

$$a(0) = 4,\ a(1) = 2,\ a(2) = 1,\ a(3) = 2,\ a(4) = 1,$$

убеждаемся квадратный многочлен $a(x)$ неприводим.

Следовательно, фактор-кольцо $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$ *является полем* и в нём $x^3 = -2x - 4 = 3x + 1$.

2. $a(4x^2 + 1) = \big(2(2x^2 + 1)\big)^3 + 2 \cdot 2(2x^2 + 1) + 4 = 3(3x^6 + 2x^4 + x^2 + 1) + 3x^2 + 3 = 4x^6 + x^4 + x^2 + 1 = 4(3x + 1)^2 + 3x^2 + x + x^2 + 1 = x^2 + 4x + 4 + 3x^2 + x + x^2 + 1 = 0$ — да, является.

Аналогично простому полю Галуа, если α — примитивный элемент поля $F = \mathbb{F}_p^n$ и m взаимно просто с $p^n - 1$, то α^m — другой его примитивный элемент, и так могут быть получены *все* примитивные элементы F (их всего $\varphi(p^n - 1)$).

Например, в рассмотренном 9-элементном поле $\mathbb{F}_3^2$ имеется $\varphi(8) = 4$ примитивных элемента, образованных степенями 1, 3, 5, 7 (взаимно просты с 8) уже найденного генератора:

$$x + 1, \qquad (x + 1)^3 = 2x + 1,$$
$$(x + 1)^5 = 2x + 2, \qquad (x + 1)^7 = x + 2.$$

Вопрос от студента: *я что-то не понимаю: неприводимые многочлены — это примитивные элементы?* Ведь было: для поиска и тех, и других нет эффективных алгоритмов...
Ответ: это — разные вещи.

- *Неприводимые многочлены* ищут в *кольце многочленов* $\mathbb{F}_p[x]$ над простым полем $\mathbb{F}_p$ — например, чтобы построить расширение последнего.
- *Примитивные элементы* ищут в *мультипликативной группе* поля — например, чтобы иметь удобное представление ненулевых элементов поля через степени примитивного элемента.

Замечание. В *поле* понятие «неприводимый многочлен» не имеет смысла: там любой многочлен делится на любой ненулевой.

Примитивные многочлены. Заметим, что, например, в поле $F = \mathbb{F}_5[x]/\left(x^2+x+1\right)$ корень x многочлена $\left(x^2+x+1\right)$ *не есть* примитивный элемент F.

Действительно, в этом поле имеем

$$x^2 = -x-1 = 4x+4,$$
$$x^3 = 4x^2+4x = 16x+16+4x = 1.$$

Вопрос: когда же корень x неприводимого многочлена $a(x) \in \mathbb{F}_p[x]$ будет примитивным элементом поля $\mathbb{F}_p[x]/(a(x))$?

Ответ: это будет если и только если многочлен $a(x)$ *примитивен* для x, т. е. $m = p^n - 1$ — наименьший показатель, при котором $a(x) \mid x^m - 1$.

Пример 2.5. 1. Неприводимый над $\mathbb{F}_2$ многочлен x^3+x+1 *примитивен*:

$$x^{2^3-1}-1 \;=\; x^7+1 \;=\; (x^3+x+1)\cdot(x^4+x^2+x+1)$$

и $x^t-1 \;\vdots\!\!\!/\; x^3+x+1$ ни при каком $1 \leqslant t < 7 = m$.

Или, что то же, $\operatorname{ord} x \;=\; 7$ и

$$\mathbb{F}_2^*[x]/\big(x^3+x+1\big) \;=\; \big\{\, x^0=1,\, x^1,\, x^2,\, x^3=x+1,\\ x^4=x^2+x,\, x^5=x^2+x+1,\, x^6=x^2+1 \,\big\}$$

— все *многочлены* степени не выше 2.

2. Неприводимый над $\mathbb{F}_2$ многочлен $x^4+x^3+x^2+x+1$ *не примитивен*: он делит не только бином $x^{2^4-1}-1 \;=\; x^{15}-1$, но и бином x^5-1:

$$x^5-1 \;=\; x^5+1 \;=\; (x^4+x^3+x^2+x+1)\cdot(x+1),$$

или, что тоже, $\operatorname{ord} x \;=\; 5 \;\neq\; 15$:

$$x^5 \;=\; \underbrace{(x^4+x^3+x^2+x+1)\cdot(x+1)}_{=0}+1 \;=\; 1.$$

2.2 Вычисления в конечных полях по алгоритмам Евклида

Алгоритм Евклида — применяют для нахождения НОД(a,b) *натуральных* чисел a и b (считая, что $a \geqslant b$).

Поскольку общий делитель пары чисел (a,b) остаётся им и для пары $(a-kb,b)$, $a-kb \geqslant 0$, то вместо $a-kb$ можно взять *остаток* от деления нацело a на

b, и затем, переставив числа в паре, можно повторить процедуру; она закончится, т. к. числа в паре уменьшаются, но остаются неотрицательными. В результате за конечное число шагов образуется пара $(r_n, 0)$ и ясно, что $\text{НОД}(a, b) = r_n$ (НОД — англ. gcd).

Алгоритм Евклида: общая схема, $a \geqslant b$, $a, b \in \mathbb{N}$

Шаг (-2): $r_{-2} = a$ — полагаем для удобства;

Шаг (-1): $r_{-1} = b$ — полагаем для удобства;

Шаг 0: $r_{-2} = r_{-1}q_0 + r_0$ — делим r_{-2} на r_{-1}, остаток r_0;

Шаг 1: $r_{-1} = r_0q_1 + r_1$ — делим r_{-1} на r_0, остаток r_1;

... *всегда делим с остатком большее число на меньшее, на следующем шаге меньшее число становится большим, а остаток — меньшим*;

Шаг n: $r_{n-2} = r_{n-1}q_n + r_n$ — делим r_{n-2} на r_{n-1}, остаток r_n;

Шаг $n+1$: $r_{n-1} = r_nq_{n+1}$ — *деление нацело* $\Rightarrow$ *ОСТАНОВ*, $\text{НОД}\,(a, b) = r_n$.

Всегда $r_{-2} \geqslant r_{-1} > r_0 > r_1 > \ldots > r_n \geqslant 1$.

Данный алгоритм дважды описан в *Началах* Евклида, но не был им открыт (упоминается в *Топике* Аристотеля).

Пример 2.6. По алгоритму Евклида найдём $\text{НОД}\,(252, 105)$.

Шаг (-2): $r_{-2} = 252$;

Шаг (-1): $r_{-1} = 105 \Rightarrow (252, 105)$;

Шаг 0: $252 = 105 \cdot 2 + 42 \Rightarrow (105, 42)$;

Шаг 1: $105 = 42 \cdot 2 + 21 \Rightarrow (42, 21)$;

Шаг 2: $42 = 21 \cdot 2 + 0 \Rightarrow (\mathbf{21}, 0)$.

Ясно, что

$$\text{НОД}\,(a, b, c) = \text{НОД}\,(a, (\text{НОД}\,(b, c))$$

Утверждение 2.3 (соотношение Безу[2]). *Для любых натуральных a, b и $d = НОД(a, b)$ найдутся целые коэффициенты Безу x, y такие, что $d = ax + by$.*

Доказательство. Рассматриваем алгоритм Евклида с конца к началу: $d = r_n = r_{n-2} - r_{n-1}q_n$, затем, подставляя сюда значение $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, получаем

$$d = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \alpha r_{n-3} + \beta r_{n-2}$$

для некоторых $\alpha, \beta \in \mathbb{Z}$ и т.д. □

Замечание. Коэффициенты Безу определяются неоднозначно, например

$$\text{НОД}\,(12, 30) = 6 = 3 \cdot 12 + (-1) \cdot 30 = (-2) \cdot 12 + 1 \cdot 30.$$

[2] открыто Клодом Гаспаром Баше за 106 лет до рождения Э. Безу

Расширенный алгоритм Евклида — находит по двум *натуральным числам* a *и* b их *натуральный* НОД d и два *целых* x, y коэффициента Безу таких, что $|x| < |b/d|$, $|y| < |a/d|$.

Расширенный алгоритм Евклида повторяет схему простого алгоритма Евклида, при этом на каждом шаге:

1) дополнительно вычисляются x_i и y_i по формулам

$$x_i = x_{i-2} - q_i x_{i-1},\ y_i = y_{i-2} - q_i y_{i-1},\ i = 0, 1, ...;$$
$$x_{-2} = y_{-1} = 1\,,\ x_{-1} = y_{-2} = 0\,;$$

2) справедливо соотношение

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} = \\ &= (ax_{i-2} + by_{i-2}) - q_i(ax_{i-1} + by_{i-1}) = \\ &= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = ax_i + by_i. \end{aligned}$$

Пример 2.7. Расширенным алгоритмом Евклида найдём натуральное d и целые x и y такие, что

$$d = \text{НОД}\,(252, 105) = 252x + 105y.$$

Имеем $x_i = x_{i-2} - q_i x_{i-1},\ y_i = y_{i-2} - q_i y_{i-1}$. Сведём все вычисления в таблицу:

шаг i	r_{i-2}	r_{i-1}	q_i	r_i	x_i	y_i
-2				252	1	0
-1				105	0	1
0	252	105	2	42	1	-2
1	105	42	2	21	-2	5
2	42	21	2	0		

Ответ: $d = 21$, $x = -2$, $y = 5$, т. е.

$$21 \;=\; 252 \cdot (-2) + 105 \cdot 5.$$

Пример 2.8. В поле $\mathbb{Z}/(101)$ решить уравнение

$$4x \;=\; 1. \qquad (*)$$

Решение.

1. Перебор: $4x = 1 + k \cdot 101 \;=\; 102,\, 203,\, \mathbf{304} \vdots 4$; $x \;=\; 304/4 \;=\; 76$.
2. Поскольку $101y \equiv_{101} 0$, вместо $(*)$ можно расширенным алгоритмом Евклида решать уравнение
$$4x + 101y \;=\; 1\,.$$
В результате работы алгоритма получим:
$$4 \cdot 76 + 101 \cdot (-3) \;=\; 1.$$

Аналогично решаются уравнения

$$ax \;=\; c \quad \text{и} \quad ax + by \;=\; c$$

(a, b и c надо поделить на их общий НОД).

Алгоритм Евклида и его расширенная версия остаются справедливыми в любом *евклидовом кольце*, следовательно, и в любом *поле Галуа*.

Поэтому в поле $\mathbb{F}_p[x]/(a(x))$ обратный к элементу $b(x)$ элемент $y(x)$, определяемый соотношением

$$\underbrace{a(x) \cdot \chi(x)}_{=0} + b(x) \cdot y(x) \;=\; 1$$

может быть найден расширенным алгоритмом Евклида, применённым к паре многочленов $(a(x),\, b(x))$.

Решение данных соотношений существует *всегда*: т. к. $a(x)$ — неприводимый многочлен и $\deg b(x) < \deg a(x)$, то $\text{НОД}\,(a(x),\, b(x)) \;=\; 1$.

Пример 2.9. Найдём $(x^2+x+3)^{-1}$ в поле

$$\mathbb{F}_7[x]/\big(x^4+x^3+x^2+3\big).$$

Для этого расширенным алгоритмом Евклида решим соотношение

$$(x^4+x^3+x^2+3)\cdot\chi(x) + (x^2+x+3)\cdot y(x) = 1. \quad (*)$$

Шаг 0: // *Задание начальных значений*

$$r_{-2}(x) = x^4+x^3+x^2+3,$$
$$r_{-1}(x) = x^2+x+3,$$
$$y_{-2}(x) = 0,$$
$$y_{-1}(x) = 1.$$

Шаг 1:

$$r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$$
$$q_0(x) = x^2+5,$$
$$r_0(x) = 2x+2, \quad \deg r_0(x) = 1,$$
$$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -x^2-5.$$

Шаг 2:

$$r_{-1}(x) = r_{=0}(x)q_1(x) + r_1(x),$$
$$q_1(x) = 4x,$$
$$r_1(x) = 3, \quad \deg r_1(x) = 0,$$
$$y_1(x) = y_{-1}(x) - y_{=0}(x)q_1(x) = 1 + 4x(x^2+5) = 4x^3+6x+1.$$

Алгоритм заканчивает свою работу на шаге 2, т. к.

$$\deg r_1(x) = \deg 1 = 0$$

("1" — *многочлен* в правой части $(*)$).

Замечание: при итерациях алгоритма нет необходимости вычислять $\chi_i(x)$, т. к. нас интересует только значения $y_i(x)$, $i = 0, 1, \ldots$.

Остаток $r_1(x) = 3$, отличается от 1 на множитель-константу. Чтобы получить решение уравнения $(*)$ вычисляем элемент $3^{-1} \equiv_7 5$ и домножаем на него y_1:

$$5y_1(x) = 5(4x^3 + 6x + 1) \equiv_7 6x^3 + 2x + 5.$$

Ответ: в поле $\mathbb{F}_7[x]/\big(x^4 + x^3 + x^2 + 3\big)$ имеем

$$(x^2 + x + 3)^{-1} = 6x^3 + 2x + 5.$$

2.3 Алгебра векторов над конечным полем

Векторное пространство

Определение 2.1. *Абстрактным векторным пространством* над полем $\Bbbk = \{1, \alpha, \beta, \dots\}$ называется двухосновная алгебраическая система $\mathcal{V} = \langle V, \Bbbk; +, \cdot \rangle$, где

- $V = \{0, v, \dots\}$ — множество *векторов*,
- $+$ — бинарная операция *сложения элементов* V: $V \times V \xrightarrow{+} V$,
- $\cdot$ — бинарная операция *умножения элемента* («числá») *из* $\Bbbk$ *на вектор из* V: $\Bbbk \times V \xrightarrow{\cdot} V$,

причём операции $+$ и $\cdot$ удовлетворяют следующим аксиомам:

1) V — коммутативная группа по сложению и 0 — её нейтральный элемент;
2) $\alpha\cdot(v_1+v_2) = \alpha\cdot v_1+\alpha\cdot v_2$, $(\alpha_1+\alpha_2)\cdot v = \alpha_1\cdot v+\alpha_2\cdot v$;
3) $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$;

4) $1 \cdot v = v$.

Также имеет место дистрибутивность относительно вычитания $(\alpha - \beta) \cdot v = \alpha \cdot v - \beta \cdot v$:

$$(\alpha - \beta) \cdot v + \beta \cdot v = (\alpha - \beta + \beta) \cdot v = \alpha \cdot v$$

Отсюда получаем, что

- $0 \cdot v = 0$, так как $0 \cdot v = (1 - 1) \cdot v = v - v = 0$,
- и $-v = (-1) \cdot v$, так как
  $v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 - 1) \cdot v = 0 \cdot v = 0$.

Пример 2.10. Пусть $V = \Bbbk^n$ — *множество конечных последовательностей длины* n элементов поля $\Bbbk$. Сложение и умножение на число из $\Bbbk$ элементов из V определяются покомпонентно.

Получившаяся структура — векторное пространство, которое называют *n-мерным координатным пространством* над полем $\Bbbk$.

Утверждение 2.4. *Поле $GF(q)$ характеристики простого p есть векторное пространство над $GF(p)$.*

Доказательство. В поле $GF(q)$, $q \geqslant p$:

сложение — наследуется операция сложения в $GF(p)$;

умножение — поскольку

$$GF(p) = \left\{ \overline{0}, \overline{1}, \ldots, \overline{p-1} \right\} \subseteq GF(q),$$

то при умножении «чисел» из поля $GF(p)$ на векторы из $GF(q)$ можно заменять на умножение элементов $GF(q)$;

аксиомы векторного пространства — выполняются в силу свойств арифметических операций в поле $GF(q)$. □

Следствие. *Поле Галуа $GF(q)$ характеристики p состоит из p^n элементов: $q = p^n$.*

Представление элементов конечных полей. Поле $\mathbb{F}_p^n$ с элементами

$$M_{p,n}(x) = \\ = \left\{ a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_p \right\}$$

можно рассматривать как

1) *фактор-кольцо* $\mathbb{F}_p[x]/\big(a(x)\big)$ вычетов $\mathbb{F}_p[x]$ по идеалу некоторого неприводимого многочлена

$$a(x) = a_0 + a_1 x + \ldots + a_n x^n,\ a_0, a_1, \ldots, a_n \in \mathbb{F}_p$$

или как

2) *n-мерное координатное пространство* над $\mathbb{F}_p$:

$$\langle\, \mathcal{M}_{p,n}(x),\, \mathbb{F}_p;\, +,\, \cdot \,\rangle$$

(все операции — по $\mod p$) и в обоих случаях можно определить операцию деления на ненулевой элемент.

Теорема 2.3. *Базис $\mathbb{F}_p^n$ образуют элементы* $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$.

Доказательство. 1. Любой элемент $\mathbb{F}_p^n$ представим в виде линейной комбинации указанных векторов:

$$\overline{b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}} \;=\; b_0 \overline{1} + b_1 \overline{x} + \ldots + b_{n-1} \overline{x^{n-1}}.$$

2. Пусть

$$c(x) = c_0\overline{1} + c_1\overline{x} + \ldots + c_{n-1}\overline{x^{n-1}} = \overline{0}.$$

Это означает, что многочлен $c(x)$ степени $n-1$ делится на некоторый многочлен n-й степени, что возможно лишь при $c_0 = c_1 = \ldots = c_{n-1} = 0$, т. е. система $\left\{ \overline{1}, \overline{x}, \ldots, \overline{x^{n-1}} \right\}$ *линейно независима.* □

Замечание. Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных теорем справедливы *не только в случае конечных полей.*

Например:

1) рассмотрим поле действительных чисел $\mathbb{R}$ и кольцо многочленов $\mathbb{R}[x]$ над ним;
2) в $\mathbb{R}[x]$ возьмём неприводимый многочлен $x^2 + 1$;
3) построим поле F как фактор-кольцо: $F = \mathbb{R}[x]/\big(x^2+1\big)$;
4) F также и векторное пространство над $\mathbb{R}$; его базис — $\left\{ \overline{1}, \overline{x} \right\}$ и каждый его элемент $z \in F$ можно представить в виде $z = a\overline{1} + b\overline{x},\ a, b \in \mathbb{R}$;
5) поле F изоморфно полю *комплексных чисел*

$$\mathbb{C} = \left\{ a + ib \mid a, b \in \mathbb{R},\, i^2 = -1 \right\},$$

изоморфизм задаётся соответствием $\overline{1} \mapsto 1,\ \overline{x} \mapsto i$.

Лемма 2.2. *Поле* $\mathbb{F}_p^n$ *содержит подполе* $\mathbb{F}_p^k$ *iff* $k \mid n$.

Доказательство. Если поле $\Bbbk_1$ содержится в поле $\Bbbk_2$, то элементы $\Bbbk_2$ можно умножать на элементы из $\Bbbk_1$, а результаты складывать.

Поэтому поле $\Bbbk_2$ является векторным пространством над полем $\Bbbk_1$ некоторой размерности d — значит, в нём $|\Bbbk_1|^d$ элементов.

Наш случай: $p^n = (p^k)^d$, что и означает $k \mid n$.

Обратное следует из существования и единственности (с точностью до изоморфизма) полей Галуа. □

Ясно, что $\mathbb{F}_p$ — всегда подполе $\mathbb{F}_p^n$ (случай $k = 1$).

Наиболее употребимы два представления элементов конечного поля $F = \mathbb{F}_p^n$:

векторное — каждый элемент F записывается как вектор в базисе $\left\{ \overline{1}, \overline{x^1}, \overline{x^2}, \ldots, \overline{x^{n-1}} \right\}$;

степенное — каждый ненулевой элемент F записывается как некоторая степень генератора мультипликативной группы F^*.

Кстати, что такое $\overline{x}$ в поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$?
$\overline{x}$ можно понимать либо как

- совокупность всех многочленов из $\mathbb{F}_p[x]$, дающих при делении на $a(x)$ остаток x;

либо как

- вектор $(0, 1, 0, \ldots, 0) \in (\mathbb{F}_p)^n$.

Далее, как принято, вместо $\overline{x}$ обычно пишем просто x.

Замечание. Переход от степенного представления к векторному достаточно прост, а обратный переход — очень

сложен, т. к. связан с вычислением *дискретного логарифма* — натурального z в равенстве $a^z = b,\ a, b \in A$.

На сложности этой задачи (известны не более, чем субэкспоненциальные алгоритмы её решения) базируются многие методы криптографии с отрытым ключом.

2.4 Корни многочленов над конечным полем

Минимальный многочлен. Рассмотрим элемент β конечного поля и будем интересоваться многочленами, для которых он является *корнем*.

Определение 2.2. *Минимальным многочленом (м.м.)* элемента $\beta \in GF(p^n)$ называется *приведённый* многочлен $m_\beta(x) \in \mathbb{F}_p[x]$ наименьшей степени, для которого β является корнем.

Сразу заметим, что минимальный многочлен для $\overline{x}$ можно получить из порождающего поле неприводимого. Рассмотрим поле $F = \mathbb{F}_p[x]/(a(x))$, порождаемое неприводимым многочленом

$$a(x) = a_0 + a_1 x + \ldots + a_n x^n$$

и убедимся, что многочлен $a_n^{-1} a(x)$ — минимальный для элемента $\overline{x} = (0, 1, 0, \ldots, 0) \in F$.

Ясно, что

$$\overline{x}^2 = \overline{x^2} = (0,0,1,0,\ldots,0), \quad \ldots, \quad \overline{x^{n-1}} = (0,\ldots,0,1)$$

Далее, с одной стороны $\overline{x}$ — корень $a(x)$, т. к.

$$a_0 + a_1\overline{x} + \ldots + a_n(\overline{x})^n = \overline{a_0 + a_1x + \ldots + a_nx^n} = \overline{0},$$

а значит и $a_n^{-1}a(x)$.

С другой —

если $\exists\, b(x) = b_0 + b_1\overline{x} + \ldots + b_{n-1}(\overline{x})^{n-1} = \overline{0}$,

то $b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x^{n-1}} = \overline{0}$,

т. е. имеем линейную зависимость между элементами $\left\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\right\}$ — базиса поля F как векторного пространства над $\mathbb{F}_p$, что возможно только при $b_0 = b_1 = \ldots = b_{n-1} = 0$.

Вопрос: являются ли минимальные многочлены примитивными?

Проверим на примерах.

1. Многочлен $a(x) = x^3 + x + 1$ неприводим в $\mathbb{F}_2[x]$, следовательно $F = \mathbb{F}_2[x]/(a(x))$ — поле и по доказанному ранее $a(x)$ — *минимальный многочлен для* x.

   Примитивен ли этот элемент $x \in F^*$?

   Проверяем, что в $F = GF(2^3)$ $a(x) \nmid (x^t - 1)$ при $t = 3, 4, 5, 6$ (а делимость $x^7 - 1$ на $a(x)$ всегда будет иметь место:
   $x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$).

   Это означает, что x — *примитивный элемент* поля $F \Leftrightarrow$ генератор $F^* \Leftrightarrow \operatorname{ord} x = 7$.

2. Многочлен $a(x) = x^4 + x^3 + x^2 + x + 1$ неприводим в $\mathbb{F}_2[x]$, следовательно $F = \mathbb{F}_2[x]/(a(x))$ —

поле и по доказанному ранее $a(x)$ — минимальный многочлен для x.

Примитивен ли элемент x?

Имеем в $F = GF(2^4)$:
$a(x) \mid (x^5-1) : x^5+1 = (x^4+x^3+x^2+x+1)(x+1)$.
Или: $|F^*| = 15 = 3 \cdot 5$, $x^3 \neq 1$, но

$$x^5 = x \cdot x^4 = x \cdot (x^3 + x^2 + x + 1) = 1.$$

Это означает, что x — *не есть примитивный многочлен* и x — не генератор F^*, т. к. $\operatorname{ord} x = 5 \neq 15$.

Определение 2.3 (эквивалентное данному ранее). Минимальный многочлен примитивного элемента поля называется *примитивным многочленом.*

Свойства минимальных многочленов. Мы докажем далее, что м.м. для каждого элемента β: (а) существует, (б) единственен и (в) неприводим. Эти свойства позволят указать простой алгоритм нахождения м.м. для любого элемента поля.

Утверждение 2.5. *Минимальные многочлены неприводимы.*

Доказательство. Пусть $m_\beta(x)$ — м.м. степени m для β и $m_\beta(x) = m_1(x) \cdot m_2(x)$.

Тогда

$$m_\beta(\beta) = 0 \Rightarrow \left[\begin{array}{l} m_1(\beta) = 0 \\ m_2(\beta) = 0 \end{array} \right. ,$$

но степени многочленов $m_1(x)$ и $m_2(x)$ меньше m, и поэтому β не может быть их корнем. □

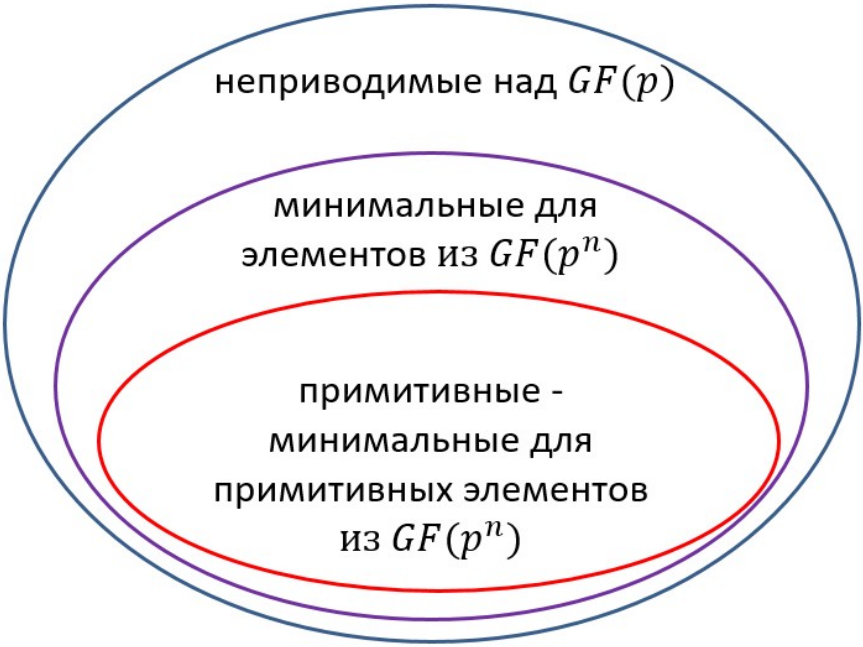


Рис. 2.1. Соотношение множеств неприводимых, минимальных и примитивных многочленов

Утверждение 2.6. *Пусть в некотором поле Галуа* $m_\beta(x)$ *— м.м. для элемента* β*, а* $f(x)$ *— многочлен такой, что* $f(\beta) = 0$*. Тогда* $f(x)$ *делится на* $m_\beta(x)$ *без остатка.*

Доказательство. Разделим $f(x)$ на $m_\beta(x)$ с остатком:

$$f(x) = u(x) \cdot m_\beta(x) + v(x), \quad 0 \leqslant \deg v < \deg m_\beta(x).$$

Подставляя в это равенство β вместо x, получаем

$$0 = f(\beta) = u(\beta) \cdot \underbrace{m_\beta(\beta)}_{=0} + v(\beta) = v(\beta)\,,$$

т. е. β — корень $v(x)$, что противоречит минимальности $m_\beta(x)$ и поэтому $v(x) \equiv 0$. □

Следствие. *Для каждого элемента поля существует не более одного м.м.*

Доказательство. Пусть минимальных многочленов два. Они взаимно делят друг друга, а значит, различаются на обратимый множитель-константу.

Поскольку минимальный многочлен нормирован, эта константа равна 1, т. е. данные многочлены совпадают. □

Утверждение 2.7. *Для каждого элемента β поля $\mathbb{F}_p^n$ существует м.м. $m_\beta(x)$ и его степень не превосходит n:* $\deg m_\beta(x) = d \leqslant n$.

Доказательство. Рассмотрим следующие элементы поля $\mathbb{F}_p^n$: $1, \beta, \beta^2, \ldots, \beta^n$. Их $n+1$ штук, а размерность $\mathbb{F}_p^n$ как векторного пространства равна n $\Rightarrow$ эти элементы линейно зависимы, т. е. существуют такие не все равные 0 коэффициенты $c_0, \ldots, c_n$, что

$$c_0 1 + c_1\beta + \ldots + c_n\beta^n = 0,$$

$\Rightarrow$ β — корень многочлена $f(x) = c_0 + c_1 x + \ldots + c_n x^n$.

Минимальным многочленом для β будет некоторый нормированный неприводимый делитель $f(x)$. □

Далее будут доказаны ещё два свойства м.м. $m_\beta(x)$ элемента β поля $\mathbb{F}_p^n$, $\deg m_\beta(x) = d$:

1. $m_\beta(x) \mid \left(x^{p^n} - x\right)$.
2. $m_\beta(x)$ минимален также и для *сопряжённых* с β элементов $\beta^p, \beta^{p^2}, \ldots, \beta^{p^{d-1}}$.

Свойства многочленов над конечным полем

Поле разложения многочлена $f(x) \in \mathbb{F}_p[x]$ — наименьшее по n расширение $\mathbb{F}_p^n$ поля $\mathbb{F}_p$, над которым $f(x)$ разлагается в *произведение линейных множителей.*

Теорема 2.4 (о поле разложения). *Любой ненулевой элемент поля* $F = \mathbb{F}_p^n$ *является корнем бинома* $x^{p^n-1}-1$*:*

$$x^{p^n-1} - 1 \;=\; (x-\beta_1)\cdot\ldots\cdot(x-\beta_{p^n-1})$$

где $\{\,\beta_1,\,\ldots,\,\beta_{p^n-1}\,\} = F^*$*, т. е.* F *— поле разложения данного бинома.*

Доказательство. F^* — циклическая группа по умножению порядка p^n-1.

Порядок $\operatorname{ord}\alpha$ любого её элемента α (= порядок циклической подгруппы $\langle\alpha\rangle$ — по теореме Лагранжа) делит порядок группы.

Поэтому $p^n-1 = q\cdot\operatorname{ord}\alpha$ и

$$\alpha^{p^n-1} - 1 \;=\; \alpha^{q\operatorname{ord}\alpha} - 1 \;=\; (\alpha^{\operatorname{ord}\alpha})^q - 1 \;=\; 1^q - 1 \;=\; 0,$$

т. е. α — корень $x^{p^n-1}-1$. □

Следствие (теорема Ферма). *Все элементы поля* $\mathbb{F}_p^n$*, не исключая нуля, являются корнями бинома* $x^{p^n}-x$.

Доказательство. Вынесем x за скобку:

$$x^{p^n} - x \;=\; x\cdot\left(x^{p^n-1}-1\right).$$

У второго сомножителя корнями будут все ненулевые элементы поля, а у первого — 0. □

Теорема 2.5. *В кольце многочленов над конечным полем*

$$(x^n - 1) \vdots (x^m - 1) \;\Leftrightarrow\; n \vdots m.$$

Доказательство.

- Пусть $n = mk$. Сделаем замену $x^m = y$, тогда $x^n - 1 = y^k - 1$ и $x^m - 1 = y - 1$.
  Делимость очевидна, т. к. 1 — корень $y^k - 1$.

- Предположим, что $n \not\vdots m$, т. е. $n = km + r$, $0 < r < m$, тогда

$$x^n - 1 = \frac{x^r(x^{mk} - 1)}{x^m - 1} \cdot (x^m - 1) + x^r - 1.$$

Это выражение задает результат деления $x^n - 1$ на $x^m - 1$ с остатком, поскольку $x^{mk} - 1$ делится на $x^m - 1$ по доказанному выше. Остаток $x^r - 1 \neq 0$ в силу $r > 0$.

Следовательно $x^n - 1$ *не делится* на $x^m - 1$. □

Теорема даёт возможность раскладывать биномы $x^n - 1$ при *составных* n на (возможно разложимые далее) многочлены над $\mathbb{F}_p$.

Пример 2.11. Многочлен $x^{15} + 1 \in \mathbb{F}_2[x]$ (где $-1 = +1$) должен делиться на $x^3 + 1$ и на $x^5 + 1$.

Действительно,

$$\begin{aligned} x^{15} + 1 &= (x^3 + 1)(x^{12} + x^9 + x^6 + x^3 + 1) = \\ &= (x^5 + 1)(x^{10} + x^5 + 1). \end{aligned}$$

Возможность раскладывать биномы *специального вида* на *неприводимые* даёт следующая

Теорема 2.6. *Бином* $x^{p^n} - x$ *делят все неприводимые многочлены* n*-й степени над* $\mathbb{F}_p$.

Доказательство.

$n = 1$. Убеждаемся, что $(x - a) \mid (x^p - x)$, где $a \in \mathbb{F}_p$: поскольку $a^p = a$, оба данных многочлена имеют корень a.

$n > 1$. Выбираем неприводимый нормированный многочлен $f(x)$ степени n из $\mathbb{F}_p[n]$ (*пока не доказано!*[3]) и строим поле $\mathbb{F}_p[x]/\big(f(x)\big)$.
В нём x — корень и своего м.м. $f(x) = m_x(x)$, и бинома $x^{p^n-1} - 1$.
По свойствам м.м. (Утверждение (2.6)) $x^{p^n-1} - 1$ делится на $f(x)$.

□

Пример 2.12 (продолжение *Примера* 2.11). Продолжаем разложение $x^{15} + 1 \in \mathbb{F}_2[x]$.

Поскольку $15 = 2^4 - 1$, все неприводимые многочлены 4-й степени будут делителями $x^{16} - x$ и, следовательно, $x^{15} + 1$. Таких многочленов 3:

$$x^4 + x + 1, \quad x^4 + x^3 + 1 \quad \text{и} \quad x^4 + x^3 + x^2 + x + 1.$$

Имеем

$$x^{15}+1 \;=\; (x^3+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Замечаем, что $3 = 2^2 - 1$, и поэтому все неприводимые многочлены 2-й степени будут делителями $x^4 - x$ и, следовательно, x^3+1. Такой многочлен только один: $x^2 + x + 1$.

[3] Теорема 2.1

Окончательно получаем разложение $x^{15}+1$ на неразложимые над $\mathbb{F}_2$ многочлены:

$$x^{15}+1 = (x+1)(x^2+x+1)\cdot \\ \cdot (x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Теорема 2.7. *Любой неприводимый многочлен, делящий бином $x^{p^n}-x$, имеет степень, не превосходящую n.*

Доказательство. Пусть φ — неприводимый делитель $x^{p^n}-x$ степени k.

Тогда $F \stackrel{\text{def}}{=} \mathbb{F}_p/(\varphi)$ — поле, которое рассмотрим как векторное пространство над $\mathbb{F}_p$ с базисом $\left\{\overline{1}, \overline{x}, \ldots, \overline{x^{k-1}}\right\}$.

Обозначим $\overline{x} = \alpha$. Поскольку $(x^{p^n}-x) \vdots \varphi$, то в F имеем $\alpha^{p^n}-\alpha = 0$.

Любой элемент F выражается через базис:

$$\beta = \sum_{i=0}^{k-1} a_i \alpha^i.$$

Возведя обе части этого равенства в степень p^n, получим

$$\beta^{p^n} = \left(\sum_{i=0}^{k-1} a_i \alpha^i\right)^{p^n} = \sum_{i=0}^{k-1} a_i \alpha^i = \beta,$$

т. е. β — корень уравнения

$$x^{p^n} - x = 0 \qquad (*)$$

Итак, каждый элемент поля F является корнем $(*)$, но у $(*)$ не более p^n различных корней, а $|F| = p^k$; поэтому $n \geqslant k$. $\square$

Вывод. Бином $x^{p^n} - x$ делится на следующие неприводимые многочлены из $\mathbb{F}_p[x]$: любые степени n и, возможно, некоторые степени $< n$.

Следующая теорема позволяет находить все корни неприводимого многочлена по одному известному.

Теорема 2.8 (свойство корней неприводимого многочлена). *Если* $\beta \in \mathbb{F}_p^n$ *— корень неприводимого многочлена* $f(x) \in \mathbb{F}_p[x]$, *то элементы* β, β^p, β^{p^2}, $\ldots$, $\beta^{p^{n-1}}$ *все различны и исчерпывают список всех* n *его корней.*

Доказательство. 1. Покажем, что если β — корень $f(x)$, то β^p — тоже корень.

Поскольку $a^p = a$ для всех $a \in \mathbb{F}_p$, то справедливо

$$\begin{aligned}\left(a_0 + a_1 x + \ldots + a_k x^k\right)^p &= \\ &= a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots + a_k^p x^{kp} = \\ &= a_0 + a_1 (x^p) + a_2 (x^p)^2 + \ldots + a_k (x^p)^k,\end{aligned}$$

т. е. для любого многочлена $\varphi(x) \in \mathbb{F}_p[x]$ выполняется равенство

$$(\varphi(x))^p = \varphi(x^p). \qquad (*)$$

Отсюда $f(\beta) = 0 \Leftrightarrow (f(\beta))^p = 0 \Leftrightarrow f(\beta^p) = 0$ и β, β^p, $\ldots$, $\beta^{p^{n-1}}$ — корни многочлена $f(x)$.

2. Осталось доказать, что все β, β^p, $\ldots$, $\beta^{p^{n-1}}$ различны, и тогда (многочлен степени n имеет не более n корней) можно утверждать, что найдены *все* корни многочлена $f(x)$.

Предположим, что $\beta^{p^l} = \beta^{p^k}$, считая $l \leqslant k$. Далее, поскольку

$$\beta = \beta^{p^n} = \beta^{p^k \cdot p^{n-k}} = \left(\beta^{p^k}\right)^{p^{n-k}} = \left(\beta^{p^l}\right)^{p^{n-k}} = \beta^{p^{n-k+l}},$$

то β — корень уравнения $x^{p^{n-k+l}-1} - 1 = 0$.

По *Теореме* 2.7 получаем $n - k + l \geqslant n \;\Rightarrow\; l \geqslant k$, т. е. $l = k$ и все вышеописанные корни различны. □

Корни β, β^p, β^{p^2}, …, $\beta^{p^{n-1}}$ неприводимого многочлена $f(x)$ степени n называют *сопряжёнными* и ясно, что они лежат в поле $\mathbb{F}_p[x]/(f(x))$.

Нахождение корней неприводимого многочлена. Для нахождения всех корней *неприводимого* многочлена $f(x) \in \mathbb{F}_p[x]$ нужно построить поле $\mathbb{F}_p[x]/(f(x))$. Первый искомый корень есть x, а остальные получаются применением Теоремы 2.8.

Пример 2.13. 1. Найти корни неприводимого над $\mathbb{F}_2$ многочлена

$$f(x) = x^4 + x^3 + 1.$$

Решение. Один корень получаем немедленно — это x, а остальные корни в поле $\mathbb{F}_2[x]/(f(x))$ суть

$$\begin{aligned} &x^2, \quad x^4 = x^3 + 1, \\ &x^8 = x^6 + 1 = (x^5 + x^2) + 1 = \\ &= (x^4 + x) + x^2 + 1 = x^3 + 1 + x + x^2 + 1 = \\ &= x^3 + x^2 + x. \end{aligned}$$

Покажем, что, например, x^2 — действительно корень $f(x)$: поскольку

$$f(x^2) = x^4 + x^3 + 1\big|_{x \mapsto x^2} = x^8 + x^6 + 1$$

и $x^8 = x^6 + 1$, то $f(x^2) = 0$.

2. Решить уравнение

$$f(x) = x^4 + x^3 + x^2 + x + 1 = 0, \quad f(x) \in \mathbb{F}_2[x].$$

Решение. Убеждаемся, что многочлен $f(x)$ неприводим в $\mathbb{F}_2[x]$. Поэтому один его корень — x, а остальные в поле $\mathbb{F}_2[x]/(f(x))$ суть

$$x^2, \quad x^4 = x^3 + x^2 + x + 1, \quad x^8 = x^6 + x^4 + x^2 + 1 = \ldots = x^3.$$

Покажите самостоятельно, что x^3 — действительно корень $f(x)$, т. е. что

$$f(x^3) = x^{12} + x^9 + x^6 + x^3 + 1 = 0.$$

3. Решить уравнение

$$f(x) = x^2 + 2x - 1 = 0, \text{ где } f(x) \in \mathbb{F}_3[x].$$

Решение. Перебором элементов $x \in \mathbb{F}_3 = \{0, 1, 2\}$ убеждаемся $f(x)$ — неприводимый многочлен.
Но тогда в поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right)$ он имеет корни x и x^3.

Поскольку $x^2 = -2x + 1 = x + 1$, то

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

Убедимся, что $2x + 1$ — корень $f(x)$:

$$f(x^2 + x) = (2x + 1)^2 + x + 1 =$$
$$= x^2 + x + 1 + x + 1 = 3 \cdot (x + 1) = 0.$$

Ответ: многочлен $f(x) = x^2 + 2x - 1 \in \mathbb{F}_3[x]$ имеет корни x и $2x + 1$ в поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right)$.

В общем случае для нахождения корней приводимого многочлена уметь раскладывать его на неприводимые множители.

Нахождение минимальных многочленов. Для нахождения м.м. $m_\beta(x)$ элемента $\beta \neq x$ поля $\mathbb{F}_p[x]/\big(a(x)\big)$ вычисляем сопряжённые элементы β^p, β^{p^2}, ..., пока на некотором шаге d окажется, что

1) $\beta^{p^d} = \beta$, тогда
$$m_\beta(x) = (x-\beta)\cdot(x-\beta^p)\cdot\ldots\cdot\left(x-\beta^{p^{d-1}}\right).$$

2) $\beta^{p^d} = x$, тогда $m_\beta(x)$ — многочлен $a(x)$ после нормировки.

Пример 2.14. Найдём минимальные многочлены для элементов x^2+x, $x+1$ поля
$$F = \mathbb{F}_2[x]/\big(x^4+x+1\big).$$

В этом поле $x^4 = x+1$.

1. $\underline{\beta = x^2+x.}$ Вычисляем элементы, сопряжённые с β:
$$\beta^2 = (x^2+x)^2 = x^4+x^2 = x^2+x+1,$$
$$\beta^4 = (x^2+x+1)^2 = x^4+x^2+1 = x+\cancel{1}+x^2+\cancel{1} = x^2+x = \beta.$$

Т.о. м.м. $m_\beta(x)$ — квадратный и
$$m_\beta(x) = (x-\beta)(x-\beta^2) = x^2+(\beta^2+\beta)\,x+\beta^3.$$
Вычисляем коэффициенты полинома:
$$\beta^2+\beta = (x^2+x+1)+(x^2+x) = 1,$$
$$\beta^3 = (x^2+x+1)(x^2+x) =$$

$$= x^4 + \cancel{x^3} + \cancel{x^3} + \cancel{x^2} + \cancel{x^2} + x = \\ = (x+1) + x = 1,$$

и окончательно $m_\beta(x) = x^2 + x + 1$.

Ясно, что коэффициенты перед степенями x могут оказаться только константы 0 или 1, иначе — ошибка в вычислениях.

Заметим также, что в данном случае вычислений коэффициентов можно было не проводить, т. к. $x^2 + x + 1$ — единственный неприводимый многочлен 2-й степени над $\mathbb{F}_2$.

2. $\underline{\beta = x + 1.}$ Элементы, сопряжённые с β:

$$\beta^2 = x^2 + 1, \\ \beta^4 = x^4 + 1 = x + 1 + 1 = x,$$

поэтому $m_\beta(x) = m_x(x) = a(x) = x^4 + x + 1$.

Ясно, что $a(x)$ является м.м. также и для сопряжённых с x элементов

$$x^2, \quad x^4 = \beta = x + 1, \quad x^8 = \beta^2 = x^2 + 1.$$

2.5 Существование и единственность поля $GF(p^n)$

Вычисления в мультипликативной группе расширения поля. Построим поле $\mathbb{F}_2^4$. Его можно представить как факторкольцо $\mathbb{F}_2/(a(x))$ по любому (*пока не доказано!*) из трех неприводимых над $\mathbb{F}_2$ многочленов 4-й степени:

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

Сделаем это, взяв многочлен $a(x) = x^4+x+1$.

Будем задавать элементы $\mathbb{F}_2^4$ наборами коэффициентов многочлена-остатка при делении на $a(x)$, записывая их в порядке возрастания степеней.

Порождающим является элемент $\alpha = x$, который записывается как $(0,1,0,0)$. Вычислим степени α, сведя результаты в таблицу (антилогарифмов).

$\alpha^4 = \alpha + 1$ степень α	1	x	x^2	x^3
α	(0,	1,	0,	0)
α^2	(0,	0,	1,	0)
α^3	(0,	0,	0,	1)
$1+\alpha = \alpha^4$	(1,	1,	0,	0)
$\alpha+\alpha^2 = \alpha^5$	(0,	1,	1,	0)
$\alpha^2+\alpha^3 = \alpha^6$	(0,	0,	1,	1)
$\alpha^3+\alpha+1 = \alpha^3+\alpha^4 = \alpha^3\alpha^4 = \alpha^7$	(1,	1,	0,	1)
$1+\alpha^2 = \alpha+1+\alpha^2+\alpha = \alpha^8$	(1,	0,	1,	0)
$\alpha+\alpha^3 = \alpha^9$	(0,	1,	0,	1)
$\alpha^2+1+\alpha = \alpha^2+\alpha^4 = \alpha^{10}$	(1,	1,	1,	0)
$\alpha+\alpha^2+\alpha^3 = \alpha^{11}$	(0,	1,	1,	1)
$1+\alpha+\alpha^2+\alpha^3 = \alpha^2+\alpha^3+\alpha^4 = \alpha^{12}$	(1,	1,	1,	1)
$1+\alpha^2+\alpha^3 = \alpha+\alpha^2+\alpha^3+\alpha^4 = \alpha^{13}$	(1,	0,	1,	1)
$1+\alpha^3 = \alpha+\alpha^3+\alpha^4 = \alpha^{14}$	(1,	0,	0,	1)
$1 = \alpha+\alpha^4 = \alpha^{15}$	(1,	0,	0,	0)

Имея такую таблицу, можно очень просто производить умножение.

Пример 2.15. Как найти $P = (x^3+x+1)\cdot(x^2+x+1)$?

1. Перемножить, учитывая $x^4 = x+1$ — можно, но сложно...
2. С помощью таблицы:
   - представляем многочлены в векторной форме и по ней — в виде степеней α:
   $$x^3+x+1 \longleftrightarrow (1,1,0,1) \longleftrightarrow \alpha^7,$$
   $$x^2+x+1 \longleftrightarrow (1,1,1,0) \longleftrightarrow \alpha^{10}$$
   - перемножая, с учётом $\alpha^{15}=1$, получаем:
   $$P = \alpha^7\alpha^{10} = \alpha^{17} = \alpha^2 = x^2.$$

Существование поля $GF(p^n)$ для всех n. Установим существование неприводимого нормированного многочлена f степени n над $GF(p)$, откуда последует существование поля из $GF(p^n)$ как факторкольца по идеалу (f).

Символом $((n))$ обозначим число нормированных неприводимых многочленов степени n над полем $\mathbb{F}_p$.

Лемма 2.3. $\displaystyle\sum_{d|n} d\cdot((d)) = p^n.$

Следствием этого результата является существование неприводимых многочленов любой степени: из

$$n((n)) = p^n - \sum_{k|n,\,k<n} k\cdot((k)) \geqslant p^n - \sum_{k=0}^{n-1} p^k =$$
$$= p^n - \frac{p^n-1}{p-1} > 0\,.$$

следует, что $((n)) > 0$, т. е. для любых простого p и натурального n над полем $\mathbb{F}_p$ существует *хотя бы один* неприводимый нормированный многочлен степени n.

Приведём ещё одну формулу для $((n))$.

Функция Мёбиуса $\mu(n)$ определяется для всех $n \in \mathbb{N}$: $\mu(n) = 1$ и для $n > 1$

$$\mu(n) = \begin{cases} 1, & \text{если примарное разложение } n \text{ состоит} \\ & \text{из } \textit{чётного числа различных} \\ & \text{сомножителей;} \\ -1, & \text{если примарное разложение } n \text{ состоит} \\ & \text{из } \textit{нечётного числа различных} \\ & \text{сомножителей;} \\ 0, & \text{иначе (примарное разложение} \\ & \text{не свободно от квадратов).} \end{cases}$$

Например: $\mu(p) = -1$, p — простое,

$\mu(6) = \mu(2 \cdot 3) = 1$, $\mu(30) = \mu(2 \cdot 3 \cdot 5) = -1$,

$\mu(4) = \mu(2^2) = 0$.

Основное свойство функции Мёбиуса:

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

Теорема 2.9 (формула Гаусса).

$$((n)) = \frac{1}{n} \sum_{d|n} \mu(d)\, p^{\frac{n}{d}}.$$

Например:

$$p=2,\ ((4)) \;=\; \tfrac{1}{4}\left[\,\mu(1)2^4+\mu(2)2^2+\mu(4)2\,\right] = \\ = \tfrac{1}{4}\left[\,2^4-2^2+0\,\right] \;=\; 3;$$

$$p=2,\ ((5)) \;=\; \tfrac{1}{5}\left[\,\mu(1)2^5+\mu(5)2\,\right] \;=\; \tfrac{1}{5}\left[32-2\right] \;=\; 6;$$

$$p=3,\ ((6)) \;=\; \tfrac{1}{6}\left[\,\mu(1)3^6+\mu(2)3^3+\mu(3)3^2+\mu(6)3\,\right] = \\ = 116.$$

Без доказательства укажем теорему, откуда следует изоморфизм *любых двух полей с одинаковым числом элементов.*

Теорема 2.10. *Пусть* $m_\alpha(x)$ *— м.м. элемента* $\alpha\in\mathbb{F}_p^n$ *и* $d=\operatorname{ord}\alpha$. *Тогда поле* $\mathbb{F}_p[x]/\big(m_\alpha(x)\big)$ *изоморфно подполю* $\mathbb{F}_p^d$, *порожденному степенями* α.

2.6 Циклические подпространства колец вычетов

Далее будем рассматривать кольцо многочленов $R=\mathbb{F}_p[x]/(f)$ по модулю главного идеала (f) *возможно приводимого* многочлена $f\in\mathbb{F}_p[x]$.

Идеалы в кольцах классов вычетов. Если f неприводим, то R — поле и этот случай уже рассмотрен. Но в любом случае R — векторное пространство над $\mathbb{F}_p$, совокупность всех многочленов степени меньшей $\deg f$.

Теорема 2.11. *Пусть* $f,\varphi\in\mathbb{F}_p[x]$, $\varphi\mid f$, *а* φ *— неприводимый нормированный многочлен.*

1. *совокупность всех многочленов, кратных* φ, *образует идеал* (φ) *в кольце* $\mathbb{F}_p[x]/(f)$.
2. φ — *единственный в* (φ) *нормированный многочлен минимальной степени.*
3. *идеал* (φ) — *векторное пространство размерности* $\deg f - \deg \varphi$.

Доказательство. $u, v, \varphi \in \mathbb{F}_p[x], \quad k = \deg \varphi \leqslant \deg f,$

$$\varphi = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + x^k, \quad f = \psi\varphi.$$

1. Проверим, что (φ) — идеал в кольце $\mathbb{F}_p[x]/(f)$. Во-первых,

$$\begin{cases} \overline{g} \in (\varphi) \\ \overline{h} \in \mathbb{F}_p[x]/(f),\ \overline{h} \subseteq \overline{g} \end{cases} \Leftrightarrow \begin{cases} \overline{g} = u\varphi \\ \overline{h} = vg = vu\varphi \end{cases} \Rightarrow \Rightarrow \overline{h} \in (\varphi).$$

И, во-вторых,

$$\overline{g}, \overline{h} \in (\varphi) \Leftrightarrow \begin{cases} \overline{g} = u\varphi \\ \overline{h} = v\varphi \end{cases} \Rightarrow \overline{g} + \overline{h} = (u+v)\varphi \in (\varphi).$$

2. Покажем, что в (φ) нет других, кроме

$$\varphi = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + x^k$$

нормированных многочленов степени, меньшей $k = \deg \varphi$.

Пусть $g = b_0 + b_1 x + \ldots + x^m$. Тогда

$$\overline{g} \in (\varphi) \Leftrightarrow g = u\varphi \Rightarrow \deg g = m \geqslant \deg \varphi = k.$$

3. Без доказательства. □

Циклическое пространство. Пусть V — n-мерное векторное пространство над некоторым полем F. При фиксировании некоторого базиса получаем

$$V \cong F^n = \{ (a_0, \ldots, a_{n-1}) \mid a_i \in F,\ i = 0, 1, \ldots, n-1 \}$$

— координатное пространство.

Определение 2.4. Подпространство координатного пространства F^n называется *циклическим*, если вместе с набором $(a_0, \ldots, a_{n-1})$ оно содержит циклический сдвиг вправо этого набора (т.е. $(a_{n-1}, a_0, \ldots, a_{n-2})$, а следовательно и все циклические сдвиги на произвольное число позиций влево и вправо).

Конкретно, в кольце $\mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как векторное пространство имеется естественный базис $\left\{ \overline{1}, \overline{x}, \ldots, \overline{x^{n-1}} \right\}$.

Циклический сдвиг координат в этом базисе равносилен умножению на $\overline{x}$:

$$\overline{a_0 + a_1 x + \ldots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}} \cdot \overline{x} =$$
$$= \overline{a_0 x + a_1 x^2 + \ldots + a_{n-2}x^{n-1} + a_{n-1}\underbrace{x^n}_{1}} =$$
$$= \overline{a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2}x^{n-1}}.$$

Теорема 2.12. *В кольце классов вычетов по модулю многочлена $x^n - 1$ подпространство является циклическим iff оно идеал.*

Доказательство. Если подпространство I — идеал, то оно замкнуто относительно умножения на $\overline{x}$, а это

умножение и есть циклический сдвиг $\Rightarrow$ I — циклическое.

И в обратную сторону, пусть I — циклическое подпространство кольца $\mathbb{F}_p/(x^n-1)$ и $g \in I$.
Тогда $g \cdot \overline{x}$, $g \cdot \overline{x^2}$, ... — циклические сдвиги, т. е. также принадлежат I.
Значит, $g \cdot \overline{f} \in I$ для любого многочлена f, поэтому I — идеал. □

Разложение бинома $x^n - 1$ на неприводимые множители. Легко показать, что корни бинома $x^n - 1 = 0$ (корни из 1) образуют *циклическую группу.*

Вопрос: какие корни из единицы будут порождать в неприводимый делитель $f(x)$ бинома $x^n - 1$?

Пусть бином $x^n - 1$ разлагаться в произведение k неприводимых многочленов степеней $d_1, \ldots, d_k$. Если β — корень неприводимого многочлена $f(x)$ степени d, то β^p, β^{p^2}, ... $\beta^{p^{d-1}}$ — также его корни.

Подгруппа в циклической группе существует iff её порядок делит порядок циклической группы. Поэтому все степени $d_1, \ldots, d_k$ должны быть делителями $p^n - 1$ (и F_p^n — поле разложения $x^n - 1$) и количество и степени многочленов-неприводимых делителей $x^n - 1$ можно найти, разбив $\mathbb{F}_p$ на *орбиты* отображения

$$t \mapsto pt \mod n.$$

Пример 2.16. 1. Рассмотрим ещё раз разложение многочлена $x^{15} - 1$ над $\mathbb{F}_2$. Относительно умножения на 2

вычеты по модулю 15 — $\{0, 1, \ldots, 14\}$ — разбиваются на орбиты:

$$\{\overline{0}\}, \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}, \{\overline{3}, \overline{6}, \overline{12}, \overline{9}\}, \{\overline{5}, \overline{10}\},$$
$$\{\overline{7}, \overline{14}, \overline{13}, \overline{11}\}$$

Поэтому $x^{15} - 1$ разлагается в произведение

- одного неприводимого многочлена степени 1,
- одного неприводимого многочлена степени 2,
- трех неприводимых многочленов степени 4.

Конкретно (разложение было раньше):

$$x^{15} + 1 = (x + 1) \cdot (x^2 + x + 1) \cdot (x^4 + x + 1) \cdot$$
$$\cdot (x^4 + x^3 + 1) \cdot (x^4 + x^3 + x^2 + x + 1).$$

2. Рассмотрим разложение многочлена $x^{23} - 1$ над $\mathbb{F}_2$. Относительно умножения на 2 вычеты по модулю 23 разбиваются на три орбиты:

$$\{\overline{0}\}, \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{9}, \overline{18}, \overline{13}, \overline{3}, \overline{6}, \overline{12}\},$$
$$\{\overline{5}, \overline{10}, \overline{20}, \overline{17}, \overline{11}, \overline{22}, \overline{21}, \overline{19}, \overline{15}, \overline{7}, \overline{14}\}$$

Поэтому $x^{23} - 1$ разлагается в произведение одного неприводимого многочлена степени 1 и двух неприводимых многочленов степени 11.

Кольца многочленов над конечным полем и конечные поля: резюме

- Характеристика конечного поля — простое число.
- Любое конечное поле характеристики p состоит из $q = p^n$ элементов $n \in \mathbb{N}$.
- $\alpha \in \big\{GF(q) \setminus 0\big\} \Rightarrow \operatorname{ord}\alpha \mid (q-1)$.
- Мультипликативная группа поля $GF(q)$ является циклической: в ней существует $\varphi(q-1)$ примитивных элементов (генераторов, элементов порядка $q-1$).

  Для нахождения самих примитивных элементов нет эффективных алгоритмов.
- Любые два конечных поля, содержащих одинаковое количество элементов, изоморфны.
- $GF\,(p^m)$ — подполе $GF\,(p^n) \Leftrightarrow m \mid n$.
- Одночлены $\left\{\overline{1}, \overline{x}, \overline{x^2}, \ldots \overline{x^{n-1}}\right\}$ — базис в векторном пространстве над кольцом $\mathbb{F}_p[x]/\big(a(x)\big)$, $\deg a(x) = n$.
- Для каждого натурального n в кольце многочленов $\mathbb{F}_p[x]$ над простым полем $\mathbb{F}_p$ имеются неприводимые многочлены.

  $\mathbb{F}_p[x]$ — кольцо с однозначным разложением многочленов на неприводимые. Для нахождения неприводимых многочленов нет эффективных алгоритмов.

- Идеал $\big(a(x)\big)$, порождённый многочленом $a(x) \in \mathbb{F}_p[x]$ составляют многочлены, кратные $a(x)$.

- Фактор-кольцо $\mathbb{F}_p[x]/(a(x))$ является полем, если и только если $a(x)$ — неприводимый многочлен в кольце $\mathbb{F}_p[x]$.

  Если при этом $\deg a(x) = n$, то элементы $\mathbb{F}_p[x]/\big(a(x)\big)$ — классы многочленов степени $< n$ (их всего p^n элементов).

- Минимальный многочлен элемента $\beta \in GF(p^n)$ есть нормированный многочлен минимальной степени, для которого β является корнем. Минимальные многочлены неприводимы и единственны для каждого β.

- Любой элемент поля $F = \mathbb{F}_p^n$ является корнем многочлена $x^{p^n} - x$:

$$x^{p^n} - x = \prod_{a \in F} (x - a).$$

- Для того, чтобы векторное подпространство V кольца $R = \mathbb{F}_p[x]/(x^n - 1)$ было циклическим, необходимо и достаточно, чтобы оно было идеалом R.

  Многочлен $g(x)$ порождает идеал R, если он является делителем $x^n - 1$.

2.7 Задачи с решениями

Задача 2.1. *В поле* $F = \mathbb{F}_2^2$ *вычислить произведение*

$$P = \prod_{i=1}^{3}(x - \beta_i),$$

где β_1, β_2, β_3 — *все ненулевые элементы поля.*

Решение. Имеем

$F = \mathbb{F}_2[x]/(x^2 + x + 1) = \{\, 0,\, 1 = \alpha^3,\, \alpha,\, \alpha + 1 = \alpha^2 \,\}$,

где α — порождающий элемент мультипликативной группы F^*. Поэтому

$$\begin{aligned} P = \prod_{i=1}^{3}(x - \beta_i) &= (x+1)(x+\alpha)(x+\alpha+1) = \\ &= (x+1)\left(x^2 + \alpha x + x + \alpha x + \alpha^2 + \alpha\right) = \\ &= (x+1)\left(x^2 + x + \alpha^2 + \alpha\right) = \\ &= \left(x^3 + (\alpha+1)x^2 + (\alpha+1)x^2 + (\alpha^2+\alpha+1)x + \right. \\ &\qquad \left. + \alpha^2 + \alpha\right) = x^3 + 1, \end{aligned}$$

как и следует по Теореме 2.4 о поле разложения:

$$(x - \beta_1) \cdot \ldots \cdot (x - \beta_{p^n-1}) = x^{p^n-1} - 1.$$

Задача 2.2. *Сумму ненулевых элементов поля* $\mathbb{F}_p$.

Решение. Все элементы $\mathbb{F}_p^*$ — корни уравнения

$$x^{p-1} - 1 = 0,$$

их *сумма* по теореме Виета есть коэффициент при x^{p-2} в этом уравнении), т. е. 0.

Задача 2.3 (Теорема Вильсона). *Доказать, что*

$$(p-1)! \equiv_p -1$$

для простого p.

Решение. При $p = 2$ утверждение тривиально.

При $p > 2$ порядки всех элементов мультипликативной циклической группы $\mathbb{F}_p^* = \{1, \ldots, p-1\}$ делят её порядок т. е. все они являются корнями уравнения

$$x^{p-1} - 1 = 0. \qquad (*)$$

Других корней у этого уравнения нет (многочлен степени $p-1$ имеет не больше $p-1$ корней). По теореме Виета их произведение равно свободному члену многочлена $(*)$, т. е. -1.

Ещё одно Решение. Для $p = 2, 3$ утверждение тривиально. При $p > 3$ обозначим

$$P = 1 \cdot \overbrace{\underbrace{2 \cdot \ldots \cdot (p-2)}_{\text{чётное число сомножителей}}}^{\pi} \cdot (p-1) = (p-1)!$$

и заметим, что $(p-1)^2 = p^2 - 2p + 1 \equiv_p 1$.

Легко видеть, что $\pi = 1$: каждый из элементов $2, \ldots, p-2$ поля $\mathbb{F}_p$ имеет единственный обратный, но это не $p-1$, т. к. он обратен сам к себе.

Отсюда $P = p-1$, или, что то же, $(p-1)! \equiv_p -1$.

Задача 2.4. *Построить поле из* 4*-х элементов.*

Решение. Это поле $\mathbb{F}_2^2$, оно может быть построено как фактор-кольцо $\mathbb{F}_2[x]/(a(x))$, где $a(x)$ — неприводимый

многочлен из $\mathbb{F}_2[x]$ степени 2. Но такой многочлен только один: $x^2 + x + 1$.

Следовательно, $\mathbb{F}_2^2 = \{0, 1, x, x+1\}$ и $x^2 = x+1$ (черту над элементами не пишем).

Таблицы сложения и умножения в построенном поле[4]:

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

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Альтернативная запись поля:

$$\mathbb{F}_2^2 = \left\{0, 1, x, x^2\right\}, \; x^2 = x + 1.$$

Задача 2.5. *Доказать, что если производная ненулевого многочлена над полем характеристики p тождественно равна 0, то он приводим.*

Решение. Имеем:

- производная монома $(x^k)' = kx^{k-1}$ тождественно равна 0 iff $k \equiv_p 0 \Leftrightarrow p \mid k$;
- $f' \equiv 0 \;\Rightarrow$ показатели степеней всех мономов многочлена f делятся на p;

[4] операции с 0 опускаем

- поэтому $f(x) = g(x^p) = g^p(x)$.

Задача 2.6. *Найти над* $\mathbb{Z}_2[x]$

$$НОД\left(x^5 + x^2 + x + 1,\ x^3 + x^2 + x + 1\right).$$

Решение. Воспользуемся алгоритмом Евклида:

$$x^5 + x^2 + x + 1 = (x^2 + x)(x^3 + x^2 + x + 1) + \underline{(x^2 + 1)},$$
$$x^3 + x^2 + x + 1 = (x + 1)\underline{(x^2 + 1)}.$$

Ответ: НОД $\left(x^5 + x^2 + x + 1,\ x^3 + x^2 + x + 1\right) = x^2 + 1$.

Задача 2.7. *В расширении* F *простого поля* $\mathbb{F}_2$, *построенного с помощью образующего полинома*

$$a(x) = x^3 + x + 1$$

1. *построить таблицу соответствий между полиномиальным и степенным представлением его ненулевых элементов;*
2. *построить таблицу умножения элементов;*
3. *для каждого элемента поля указать обратные;*
4. *найти порождающие элементы поля;*
5. *найти минимальные многочлены всех элементов поля.*

Решение.
Поле $F = \mathbb{F}_2[x]/(x^3 + x + 1)$ содержит 8 элементов: 0 и степени $1, \ldots, 7$ порождающего элемента α. Можно полагать $x = \alpha$, т. к. $a(x)$ — примитивный многочлен.

1. Таблица соответствий между полиномиальным и степенным представлением его ненулевых элементов:

$x^3 = x + 1$ степень x	1	x	x^2
x	(0,	1,	0)
x^2	(0,	0,	1)
$x^3 = x + 1$	(1,	1,	0)
$x^4 = x^2 + x$	(0,	1,	1)
$x^5 = x^2 + x + 1$	(1,	1,	1)
$x^6 = x^2 + 1$	(1,	0,	1)
$x^7 = 1$	(1,	0,	0)

2. Таблица умножения:

$\times$	x	x^2	x^3	x^4	x^5	x^6
x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1
x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1	x
x^3	x^2+x	x^2+x+1	x^2+1	1	x	x^2
x^4	x^2+x+1	x^2+1	1	x	x^2	$x+1$
x^5	x^2+1	1	x	x^2	$x+1$	x^2+x
x^6	1	x	x^2	$x+1$	x^2+x	x^2+x+1

3. Обратные элементы:

x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1
x^2+1	x^2+x+1	x^2+x	$x+1$	x^2	x

4. Поле F имеет $\varphi(7) = 6$ порождающих элементов: все кроме 0 и 1.

5. Находим м.м. элементов поля. Ясно, что
   - $m_0(x) = x$;
   - $m_1(x) = x + 1$;
   - остальные элементы F суть порождающие его мультипликативной группы, и их м.м. будут совпадать с $a(x)$.

Задача 2.8. *Перечислить все подполя поля* $GF\left(2^{30}\right)$.

Решение. Поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$ iff $k \mid n$, поэтому подполями $GF\left(2^{30}\right)$ будут поля $GF\left(2^k\right)$, $k \in D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$, $GF(2)$ — *простейшее* и $GF\left(2^{30}\right)$ — *несобственное* подполя.

Задача 2.9. *Многочлен* $f(x) = x^5 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ *разложить на неприводимые множители.*

Решение. В поле $\mathbb{F}_2$ имеем $x - 1 = x + 1$.

1. $f(1) = 0 \Rightarrow 1$ — корень f.
2. Делим $f(x)$ на $x + 1$, получаем

$$x^4 + x^3 + x + 1 = f_1(x).$$

3. $f_1(1) = 0 \Rightarrow 1$ — корень f_1; $\frac{f_1}{x+1} = x^3+1 = f_2(x)$.
4. $f_2(1) = 0 \Rightarrow 1$ — корень f_2; $\frac{f_2}{x+1} = x^2 + x + 1$.
5. Многочлен $x^2 + x + 1$ неприводим.

Ответ: $x^5 + x^3 + x^2 + 1 = (x+1)^3(x^2+x+1)$.

Задача 2.10. *Многочлен* $f(x) = x^3+2x^2+4x+1 \in \mathbb{F}_5[x]$ *разложить на неприводимые множители.*

Решение.

1. $f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2^2 + 1 = 25 \equiv_5 0$,
   $(x-2) \equiv_5 (x+3)$
2. $$\begin{array}{r|l} x^3 + 2x^2 + 4x + 1 & x+3 \\ \cline{2-2} \underline{x^3 + 3x^2} & x^2 + 4x + 2 \\ \quad 4x^2 + 4x & \\ \quad \underline{4x^2 + 2x} & \\ \quad\quad 2x + 1 & \\ \quad\quad \underline{2x + 1} & \\ \quad\quad\quad 0 & \end{array}$$
3. Перебором убеждаемся, что многочлен x^2+4x+2 неприводим в $\mathbb{F}_5$.

Ответ: $x^3 + 2x^2 + 4x + 1 = (x+3)(x^2+4x+2)$.

Задача 2.11. *Многочлен* $f(x) = x^4 + x^3 + x + 2 \in \mathbb{F}_3[x]$ *разложить на неприводимые множители.*

Решение.

1. 0, 1, 2 — не корни $f(x) \Rightarrow f(x)$ линейных делителей не содержит.
2. Неприводимые многочлены над $\mathbb{F}_3$ степени 2:
   $$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2.$$

3. Подбором получаем: $f(x) = (x^2+1)(x^2+x+2)$.

Ответ: $x^4+x^3+x+2 = (x^2+1)(x^2+x+2)$.

Задача 2.12. *Многочлен*

$$f(x) = x^4+3x^3+2x^2+x+4 \in \mathbb{F}_5[x]$$

разложить на неприводимые множители.

Решение. 1. $f(x) \neq 0$ ни при каком $x = 0,1,2,3,4$, т. е. $f(x)$ не имеет линейных делителей.

2. Перебирая неприводимые многочлены степени 2 над $\mathbb{F}_5$, получаем

Ответ: $f(x) = (x^2+x+1)(x^2+2x+4)$.

Задача 2.13. *Разложить на неприводимые множители все нормированные многочлены 3-й степени из* $\mathbb{F}_2[x]$.

Решение. Вычисляя значения при $x = 0, 1$ всех нормированных многочленов 3-й степени из $\mathbb{F}_2[x]$, определяем их линейные делители и получаем, что

$$\begin{aligned}
f_1(x) &= x^3 = x\cdot x\cdot x,\\
f_2(x) &= x^3+1 = (x+1)(x^2+x+1),\\
f_3(x) &= x^3+x = x(x+1)^2,\\
f_4(x) &= x^3+x^2 = x^2(x+1),\\
f_5(x) &= x^3+x+1 \text{ — неприводим},\\
f_6(x) &= x^3+x^2+1 \text{ — неприводим},
\end{aligned}$$

$$f_7(x) = x^3 + x^2 + x = x(x^2 + x + 1),$$
$$f_8(x) = x^3 + x^2 + x + 1 = (x + 1)^3.$$

Задача 2.14. *Найти все нормированные неприводимые многочлены 2-й степени над* $GF(3)$.

Решение. Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

Перебором коэффициентов $b, c \in \{\, 0,\ 1,\ 2 \,\}$ в выражении $x^2 + bx + c$, находим подходящие многочлены:

$$f_1(x) = x^2 + 1,$$
$$f_2(x) = x^2 + x + 2,$$
$$f_3(x) = x^2 + 2x + 2.$$

Задача 2.15. *Найти все нормированные многочлены 3-й третьей степени, неприводимые над полем вычетов по модулю* 3.

Решение. Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

$$f_1(x) = x^3 + 2x + 1,$$
$$f_2(x) = x^3 + 2x + 2,$$
$$f_3(x) = x^3 + x^2 + 2,$$
$$f_4(x) = x^3 + 2x^2 + 1,$$
$$f_5(x) = x^3 + x^2 + x + 2,$$
$$f_6(x) = x^3 + x^2 + 2x + 1,$$
$$f_7(x) = x^3 + 2x^2 + x + 1,$$
$$f_8(x) = x^3 + 2x^2 + 2x + 2.$$

Задача 2.16. *1. Проверить, что*

$$F = \mathbb{F}_7[x]/\big(x^2+x-1\big)$$

является полем.

2. В F найти обратный элемент к $1-x$.

Решение. 1. $a(x) = x^2+x-1$, $a(0)=6$, $a(1)=1$, $a(2)=5$, $a(3)=4$, $a(4)=6$, $a(5)=1$, $a(6)=6$, т. е. многочлен $a(x)$ — *неприводим* в $\mathbb{F}_7$ и F — поле ($\cong \mathbb{F}_7^2$).

2. $\mathbb{F}_7^2 = \big\{\, ax+b \mid a,b \in \mathbb{F}_7,\ x^2 = 1-x = 6x+1 \,\big\}$

$$(ax+b)\cdot(6x+1) = \ldots = (2a+6b)x + (6a+b) = 1$$

$$\begin{cases} 6a+b &= 1 \\ a+3b &= 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 2 \end{cases}$$

Ответ: $(1-x)^{-1} = x+2$ в F.

Задача 2.17. *Найти порядок элемента $\beta = x+x^2$ в мультипликативной группе*

1. поля $F_1 = \mathbb{F}_2[x]/\big(x^4+x+1\big)$;

2. поля $F_2 = \mathbb{F}_2[x]/\big(x^4+x^3+1\big)$.

Решение. $\beta = x+x^2 = x(x+1)$.

Мультипликативная группа указанных полей состоит из $2^4-1=15$ элементов.

Примарное разложение 15: $15 = 3\cdot 5$, поэтому равенство $\beta^d = 1$ нужно проверить для $d = \frac{15}{5} = 3$ и $d = \frac{15}{3} = 5$.

1. $x^4 = x+1$

$$\begin{aligned}\beta^2 &= x^4 + x^2 = x^2 + x + 1,\\ \beta^3 &= x(x+1)(x^2+x+1) = x(x^3+1) = \\ &= x^4 + x = x + 1 + x = 1.\end{aligned}$$

Ответ: В поле F_1 $\operatorname{ord}\beta = 3$.

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

$$\begin{aligned}\beta^2 &= x^4 + x^2 = x^3 + x^2 + 1,\\ \beta^3 &= x(x+1)(x^3+x^2+1) = \\ &= x(x^4+x^2+x+1) = x(x^3+x^2+x) = \\ &= x^4 + x^3 + x^2 = x^2 + 1 \neq 1,\\ \beta^5 &= x^2x^3 = (x^3+x^2+1)(x^2+1) = \\ &= (x^5+x^4+x^2+x^3+x^2+1) = \ldots\\ \ldots &= (x^3+1)\,x = x^4 + x = x^3 + x + 1 \neq 1.\end{aligned}$$

Ответ: В поле F_2 $\operatorname{ord}\beta = 15$.

Задача 2.18. *Найти количество нормированных неприводимых многочленов*

1) *степени* 7 *над полем* $\mathbb{F}_2$;
2) *степени* 6 *над полем* $\mathbb{F}_5$.

Решение.

$$\sum_{d|n} d \cdot ((d)) = p^n.$$

1. $((7))$ над $\mathbb{F}_2$

$$\sum_{d|7} d((d)) = 2^7 = 1 \cdot ((1)) + 7 \cdot ((7)) = 128.$$

$((1)) = 2$: это x и $x+1$, отсюда $((7)) = \frac{128-2}{7} = 18$.

2. $\underline{((6)) \text{ над } \mathbb{F}_5}$

$$((6)) = \frac{1}{6}\sum_{d|6}\mu(d)\,5^{\frac{6}{d}} = \frac{1}{6}\left[\mu(1)5^6 + \mu(2)5^3 + \right.$$

$$\left. + \mu(3)5^2 + \mu(6)5\right] = \frac{15625 - 125 - 25 + 5}{6} = 2\,580.$$

Задача 2.19. *Для поля* $F = \mathbb{F}_3[x]/\left(-2x^2 + x + 2\right)$ *построить таблицу соответствий между полиномиальным и степенным представлением его ненулевых элементов.*

С помощью данной таблицы вычислить выражение

$$S = \frac{1}{2x+1} - \frac{2(2x)^7}{(x)^9(x+2)}.$$

Решение. $\operatorname{char} F = 3$, поэтому
$-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = a(x)$.

$F = \mathbb{F}_3^2$, F^* содержит $3^2 - 1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1,8}$ примитивного элемента α.

Если элемент x окажется примитивным, то положим $\alpha = x$ и, поскольку вычисления в $\mathbb{F}_3^2$ проводятся по $\bmod a(x)$, будем иметь

$$x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 = 2x + 1.$$

Найдём порядок элемента x: т. к. $8 = 2^3$, $\frac{8}{2} = 4$, проверим равенство $x^4 = 1$:

$$x^4 = (x^2)^2 = (2x+1)^2 = x^2 + x + 1 = \cancel{2}x + 1 + \cancel{x} + 1 = \cancel{2} \neq 1,$$

т. е. x — примитивный элемент F: $\operatorname{ord} x = 8$, $x^8 = 1$.

Повезло: $a(x) = x^2 + x + 2$ оказался примитивным многочленом над $\mathbb{F}_3$, иначе примитивный элемент поля F пришлось бы искать.

Теперь вычислим значение заданного выражения. Имеем $2^8 = 256 \equiv_3 1$, $x + 2 = -x^2$, $x^4 = 2$ и далее:

$$S = \frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} + \frac{x^7}{x^9 x^2} = \frac{x^8}{x^2} + \frac{x^7 x^8}{x^{11}} =$$
$$= x^6 + x^4 = (x^2)^3 + 2 = (2x+1)^3 + 2 = 2x^3 + \cancel{1} + \cancel{2} =$$
$$= 2x(2x+1) = x^2 + 2x = 2x + 1 + 2x = x + 1.$$

Задача 2.20. *Для поля* $F = \mathbb{F}_3[x]/\left(x^2+1\right) \cong \mathbb{F}_3^2$ *построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.*

Решение. В данном 9-элементном поле $x^2 + 1 = 0 \Rightarrow x^2 = -1 \equiv_3 2$.

1. Найдём порядок элемента x, для чего проверим равенство $x^4 = 1$ (т. к. $9 - 1 = 8 = 2^3$, $\frac{8}{2} = 4$):

$$x^4 = (x^2)^2 = 4 \equiv_3 1.$$

Следовательно $\operatorname{ord} x = 4$ и элемент x не является генератором группы F^* (и $x^2 + 1$ — не есть примитивный многочлен над $\mathbb{F}_3$:

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

2. Проверим на примитивность элемент $x+1$:

$$(x+1)^4 \;=\; (x+1)(x+1)^3 \;=\; (x+1)(x^3+1) \;=$$
$$=\; (x+1)(2x+1) \;=\; 2x^2 + \not{x} + \not{2}x + 1 \;=\; 4+1 \;=\; 2 \neq 1$$

т. е. $\alpha = x+1$ оказался примитивным элементом. Его степени:

$$\begin{aligned}
\alpha^1 &= x+1, & \alpha^5 &= 2(x+1) = 2x+2,\\
\alpha^2 &= x^2+2x+1 = 2x, & \alpha^6 &= \alpha^2\cdot\alpha^4 = 4x = x,\\
\alpha^3 &= 2x(x+1) = 2x+1, & \alpha^7 &= x(x+1) = x+2,\\
\alpha^4 &= 4x^2 = x^2 = 2, & \alpha^8 &= (\alpha^4)^2 = 4 = 1.
\end{aligned}$$

Замечание: вычисление очередной степени α^{i+j} часто бывает удобным провести как $\alpha^i \cdot \alpha^j$, а не как $\alpha \cdot \alpha^{i+j-1}$.

Задача 2.21. *В факторкольце* $R = \mathbb{F}_3[x]/\big(x^4+1\big)$ *найти все элементы главного идеала* $\big(x^2+x+2\big)$.

Решение. 1. Сначала проверим, является ли многочлен $f(x) = x^2+x+2$ делителем x^4+1?

$x^4+1 \;=\; (x^2+x+2)\cdot(x^2+2x+2)$ — да, является

Поэтому искомый идеал составят многочлены из R, кратные $f(x)$:

$$\big(x^2+x+2\big) = \big\{\,(x^2+x+2)(ax+b) \mid a,b \in \mathbb{F}_3, x^4 = 1\,\big\}.$$

2. Проведём умножение:

$$(x^2+x+2)(ax+b) \;=\; ax^3+(a+b)\,x^2+(2a+b)\,x+2b.$$

Теперь, перебирая все возможные значения $a, b \in \mathbb{F}_3$, найдём все элементы идеала $\big(x^2+x+2\big)$:

a	b	$ax^3+(a+b)x^2+(2a+b)x+2b$
0	0	0
0	1	x^2+x+2
0	2	$2x^2+2x+1$
1	0	x^3+x^2+2x
1	1	x^3+2x^2+2
1	2	x^3+x+1
2	0	$2x^3+2x^2+x$
2	1	$2x^3+2x+2$
2	2	$2x^3+x^2+1$

А если бы $f(x) \not\vdots a(x)$? Тогда кратные $f(x)$ составят в R идеал $(\text{НОД}(f(x), a(x)))$.

Задача 2.22. *В поле* $F = \mathbb{F}_7[x]/\big(x^4+x^3+x^2+3\big)$ *найти элемент, обратный к* x^2+x+3.

Решение. Обратный элемент к x^2+x+3 находим, решая соотношение Безу

$$\underbrace{(x^4+x^3+x^2+3)\cdot\chi(x)}_{=0} + (x^2+x+3)\cdot y(x) \;=\; 1 \quad (*)$$

с помощью расширенного алгоритма Евклида: им будет полином $y(x)$. Вычислять полином $\chi_i(x)$ нет необходимости.

Шаг 0. // *Инициализация*

$$\begin{aligned} r_{-2}(x) &= x^4 + x^3 + x^2 + 3, \\ r_{-1}(x) &= x^2 + x + 3, \\ y_{-2}(x) &= 0, \\ y_{-1}(x) &= 1. \end{aligned}$$

Шаг 1. // *Делим* $r_{-2}(x)$ *на* $r_{-1}(x)$ *с остатком*

$$\begin{aligned} r_{-2}(x) &= r_{-1}(x)q_0(x) + r_0(x), \\ q_0(x) &= x^2 + 5, \\ r_0(x) &= 2x + 2, \\ y_0(x) &= y_{-2}(x) - y_{-1}(x)q_0(x) = \\ &= -q_0(x) = -x^2 - 5. \end{aligned}$$

Шаг 2. // *Делим* $r_{-1}(x)$ *на* $r_{=0}(x)$ *с остатком*

$$\begin{aligned} r_{-1}(x) &= r_{=0}(x)q_1(x) + r_1(x), \\ q_1(x) &= 4x, \\ r_1(x) &= 3, \\ y_1(x) &= y_{-1}(x) - y_{=0}(x)q_1(x) = \\ &= 1 + 4x(x^2 + 5) = 4x^3 + 6x + 1. \end{aligned}$$

Алгоритм заканчивает свою работу на Шаге 2, т. к. степень 0 очередного остатка $r_1(x) = 3$ равна степени многочлена в правой части $(*)$: 1 — *многочлен* 0*-й степени.*

В результате работы алгоритма получено:

$$(x^2 + x + 3)(\underbrace{4x^3 + 6x + 1}_{y_1(x)}) = r_1(x) = 3.$$

Чтобы найти $y(x)$, нужно домножить $y_1(x)$ на $3^{-1} \equiv_7 5$:

$$y(x) = 5y_1(x) = 5 \cdot (4x^3 + 6x + 1) = 6x^3 + 2x + 5.$$

Задача 2.23. *В поле* $F = \mathbb{F}_5[x]/\big(x^2+3x+3\big)$ *найти обратную к матрице*

$$M = \begin{pmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{pmatrix}.$$

Решение. Для матриц размера 2×2 обратная матрица записывается в виде

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\cdot\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

1. Сначала вычислим $\det M = ad - bc$ с учётом $x^2 = 2x+2$:

$$\begin{aligned}\det M &= (3x+4)(3x+2) - (x+2)(x+3) = \\ &= 4x^2+3x+3-x^2-1 = \\ &= 3x^2+3x+2 = 3(2x+2)+3x+2 = 4x+3.\end{aligned}$$

2. Найдём обратный к $4x+3$ элемент, решая соотношение

$$(x^2+3x+3)a(x) + (4x+3)b(x) = 1$$

с помощью расширенного алгоритма Евклида:

Шаг 0. // *Инициализация*
$$r_{-2}(x) = x^2 + 3x + 3,$$
$$r_{-1}(x) = 4x + 3,$$
$$y_{-2}(x) = 0,$$
$$y_{-1}(x) = 1.$$

Шаг 1. // *Делим* $r_{-2}(x)$ *на* $r_{-1}(x)$ *с остатком*
$$r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$$
$$q_0(x) = 4x + 4,$$
$$r_0(x) = 1, \ // \ \deg r = 0 \Rightarrow \mathit{OCTAHOB}$$
$$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) =$$
$$= -q_0(x) = -4x - 4 = x + 1.$$

3. Вычислим обратную матрицу

$$M^{-1} = (x+1)\begin{pmatrix} 3x+2 & 4x+3 \\ 4x+2 & 3x+4 \end{pmatrix} = \begin{pmatrix} x+3 & 1 \\ 4x & 3x \end{pmatrix}.$$

Задача 2.24. *Разложить на неприводимые множители многочлен*

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Решение. 1. Сначала пытаемся найти корни $f(x)$ в $\mathbb{F}_2$: получим $f(0) = f(1) = 1$, и значит $f(x)$ не имеет корней в $\mathbb{F}_2$ т. е. не имеет линейных множителей.

2. Далее ищем делители $f(x)$ среди неприводимых многочленов степени 2.

Таковых над $\mathbb{F}_2$ только один — $x^2 + x + 1$.

При делении $f(x)$ на $x^2 + x + 1$, получаем

$$f(x) = (x^2 + x + 1)\times$$

$$\times (\underbrace{x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1}_{g(x)}).$$

Делим частное $g(x)$ на $x^2 + x + 1$:

$$\begin{aligned} g(x) &= x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ &= (x^2 + x + 1) \cdot (x^7 + x^4 + x^3 + x^2 + x + 1) + x \end{aligned}$$

— не делится нацело, т. е. $x^2 + x + 1$ — делитель $f(x)$ кратности 1.

3. Неприводимых многочленов 3-й степени над $\mathbb{F}_2$ только два: $x^3 + x + 1$ и $x^3 + x^2 + 1$.
Пробуем поделить $g(x)$ на $x^3 + x + 1$:

$$\begin{aligned} x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 &= \\ = (x^3 + x + 1)(\underbrace{x^6 + x^5 + x^3 + x^2 + 1}_{h(x)}) & \end{aligned}$$

— делится!

Производя далее попытки деления $h(x)$ на неприводимые многочлены 3-й степени, получаем

$$\begin{aligned} x^6 + x^5 + x^3 + x^2 + 1 &= \\ = (x^3 + x + 1) \cdot (x^3 + x^2 + x + 1) + x^2, & \\ x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x^2 + 1) \cdot x^3 + x^2 + 1. & \end{aligned}$$

Поскольку многочлен $h(x)$ 6-ой степени не имеет делителей 3-й и меньших степеней, то он является неприводимым.

Ответ: В $\mathbb{F}_2[x]$ справедливо разложение

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 = (x^2 + x + 1)(x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1).$$

Задача 2.25. *Найти поле характеристики* 3, *в котором многочлен* $f(x) = x^3 + x + 2 \in \mathbb{F}_3[x]$ *раскладывается на линейные множители и найти в нём все корни данного многочлена.*

Решение. 1. Найдём разложение многочлена $f(x)$ на *неприводимые* множители над $\mathbb{F}_3$.

- Ищем корни: $f(0) = 2$, $f(1) = 1$, $f(2) = 0$. Поскольку $x - 2 \equiv_3 x + 1$, то $f(x) = (x + 1)(x^2 + 2x + 2)$.
- Пробуем разложить многочлен $g(x) = x^2 + 2x + 2$: он не имеет корней в $\mathbb{F}_3$, его степень $= 2 \Rightarrow$ он неприводим.
- Окончательно: $f(x) = (x + 1)(x^2 + 2x + 2) \in \mathbb{F}_3[x]$.

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над $\mathbb{F}_p$, то он:

- в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей — $$g(x) = (x-\alpha)\cdot(x - \alpha^p)\cdot\left(x - \alpha^{p^2}\right)\cdot\ldots\cdot\left(x - \alpha^{p^{n-1}}\right),$$ где α – произвольный корень $g(x)$ в F;
- не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.

3. Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2 + 2x + 2$.

В этом поле если α — корень $g(x)$, то и α^3 — тоже его корень. Вычисляем:

$$\begin{aligned}\alpha^2 &= -2\alpha - 2 = \alpha + 1,\\ \alpha^3 &= \alpha(\alpha+1) = \alpha^2 + \alpha = 2\alpha + 1\end{aligned}$$

Построенное поле $\mathbb{F}_3[x]/\big(x^2 + 2x + 2\big)$ — содержит найденный ранее корень 2, поэтому многочлен $f(x)$ в этом поле раскладывается на следующие линейные множители:

$$f(x) = x^3 + x + 2 = (x-2)(x-\alpha)(x-2\alpha-1) = (x+1)(x+2\alpha)(x+\alpha+2).$$

4. Определить корни многочлена

$$g(x) = (x-\alpha)(x-2\alpha-1)$$

в поле $\mathbb{F}_3[x]/\big(x^2 + 2x + 2\big)$ легко: всегда можно взять $\alpha = x$, откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

Ответ: многочлен $f(x) = x^3 + x + 2$ имеет корни 2, x, $2x+1$ в поле $\mathbb{F}_3[x]/\big(x^2 + 2x + 2\big) = GF(3^2)$.

Задача 2.26. *Найти м.м. для всех элементов β поля* $F = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$.

Решение. $\beta \in \{0, 1, \alpha, \ldots, \alpha^{14}\} = F, \quad x^4 = x + 1.$

$\beta = 0$: $m_{=0}(x) = x$.

$\beta = 1$: $m_1(x) = x + 1$.

$\beta = \alpha$: сопряжённые с α элементы — α^2, α^4, α^8 и
$(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) = \ldots$
$$\ldots = x^4 + x + 1 = 0.$$

Это означает, что x^4+x+1 — примитивный многочлен и $m_\alpha(x) = x^4 + x + 1$.

$\beta = \alpha^3$: сопряжённые с α^3 элементы суть α^6, α^{12}, $\alpha^{24} = \alpha^9$, их м.м. —
$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) =$$
$$= x^4 + \left(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\right)x^3 +$$
$$+ \left(\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12}\right)x^2 +$$
$$+ \left(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12}\right)x +$$
$$+ \left(\alpha^3\alpha^6\alpha^9\alpha^{12}\right) = x^4 + \left(\alpha^3 + (\alpha^3+\alpha^2) + (\alpha^3+\alpha) +\right.$$
$$\left. + (\alpha^3+\alpha^2+\alpha+1)\right)x^3 + (\ldots)\,x^2 + (\ldots)\,x + \alpha^{30} =$$
$$= x^4 + x^3 + x^2 + x + 1.$$

$\beta = \alpha^5$: единственный сопряжённый с α^5 элемент — α^{10} (т. к. $\alpha^{20} = \alpha^5$), их м.м. —
$$m_{\alpha^5}(x) = (x-\alpha^5)(x-\alpha^{10}) = x^2 + x + 1.$$

$\beta = \alpha^7$: сопряжённые с α^7 элементы — α^{14}, $\alpha^{28} = \alpha^{13}$, $\alpha^{56} = \alpha^{11}$, их м.м. —
$$m_{\alpha^7}(x) = (x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14}) =$$
$$= x^4 + x^3 + 1.$$

Задача 2.27. *Найти минимальный многочлен элемента α^3, где α — примитивный элемент поля*
$$F = \mathbb{F}_5[x]/\left(x^2+x+2\right).$$

Решение. 1. Любой многочлен в поле характеристики 5 вместе с корнем α^3 содержит все сопряжённые с ним $(\alpha^3)^5 = \alpha^{15}$, $(\alpha^3)^{5^2} = \alpha^{75}$, $(\alpha^3)^{5^3} = \alpha^{375}$ и т.д.

2. В поле F имеем $\alpha^{5^2-1} = \alpha^{24} = 1$, и сопряжённым с α^3 будет только элемент α^{15}, т. к. $\alpha^{75} = \alpha^{24\cdot 3+3} = \alpha^3$. Поэтому минимальный многочлен элемента α^3 — квадратный:

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^{15}) = x^2 - (\alpha^3+\alpha^{15})x + \alpha^{18}.$$

3. Найдём коэффициенты данного многочлена, учитывая $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
\alpha^3 &= \alpha\cdot\alpha^2 = \alpha(4\alpha+3) = 4\alpha^2+3\alpha = \\
&= 4(4\alpha+3)+3\alpha = 4\alpha+2, \\
\alpha^{15} &= (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5+2 = \\
&= 4\alpha^2\alpha^3+2 = 4(4\alpha+3)(4\alpha+2)+2 = \\
&= 4(\alpha^2+1)+2 = 4(4\alpha+4)+2 = \alpha+3, \\
\alpha^3+\alpha^{15} &= 4\alpha+2+\alpha+3 = 0, \\
\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = \\
&= 4(4\alpha+3)+4\alpha+1 = 3.
\end{aligned}$$

Ответ: $m(x) = x^2+3$.

Задание: убедитесь, что x — примитивный элемент поля F.

Задача 2.28. *Найти корни многочлена*

$$f(x) = x^3+3x^2+4x+4 \in \mathbb{F}_5[x].$$

Решение. Вычисляем значения $f(x)$ для $x \in GF(5) = \{0, 1, 2, 3, 4\}$:

$$f(0) = 4,\ f(1) = 2,\ f(2) = 1,\ f(3) = 0.$$

Таким образом, $x = 3$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x - 3$ (или на $x+2$), получим $x^3+3x^2+4x+4 = (x-3)\cdot(x^2+x+2)$.

Перебором элементов $x \in GF(5)$ убеждаемся $f_2(x) = x^2 + x + 2$ — неприводимый многочлен.

В поле $\mathbb{F}_5[x]/\big(x^2 + x + 2\big)$ корни многочлена $f_2(x) = 0$ суть $\{\, x,\, x^5 \,\}$ и $x^2 = -x - 2 = 4x + 3$.

Вычисляем:

$$x^5 = \big(x^2\big)^2 x = x(4x+3)^2 = x(x^2+4x+4) =$$
$$= x(4x+3+4x+4) = x(3x+2) = 3x^2+2x =$$
$$= 2x+4+2x = 4x+4.$$

Ответ: $\{\, 3,\, x,\, 4x+4 \,\}$.

Задача 2.29. *Является ли многочлен*

$$f(x) = x^2 + x + 2 \in \mathbb{F}_5[x]$$

примитивным?

Решение. Подстановкой в $f(x)$ всех элементов $0, \ldots, 4$ поля $\mathbb{F}_5$ убеждаемся, что данный многочлен 2-й степени не имеет линейных делителей и, следовательно, *неприводим*.

Порядок мультипликативной группы $GF(5^2)$ есть $25 - 1 = 24 = 2^3 \cdot 3$. Определим порядок элемента её x, для которого $x^2 = -x - 2 = 4x + 3$.

Поскольку простые делители 24 суть 2 и 3, проверим равенство $x^d = 1$ для $d \in \{\, \frac{24}{2} = 12,\ \frac{24}{3} = 8 \,\}$. Имеем:

$$\begin{aligned} x^4 &= (x^2)^2 = (4x+3)^2 = x^2+4x+4 = \dots \\ &\dots = 3x+2 \neq 1, \\ x^8 &= (x^4)^2 = (3x+2)^2 = -x^2+2x+4 = \dots \\ &\dots = 3x+1 \neq 1. \\ x^{12} &= x^8x^4 = (3x+1)(3x+2) = -x^2+4x+2 = \dots \\ &\dots = 4 \neq 1. \end{aligned}$$

Следовательно $\operatorname{ord} x = 24$ и рассматриваемый многочлен *примитивен* в поле $\mathbb{F}_5[x]/\big(x^2+x+2\big)$.

Задача 2.30. *Для бинома* $x^{40}-1 \in \mathbb{F}_5[x]$ *определить количество и степени неприводимых сомножителей.*

В каком минимальном поле расширения $\mathbb{F}_5[x]$ *данный бином раскладывается на линейные множители?*

Решение. Поскольку $n = 40 = 5 \times 8$, то корни бинома $x^{40}-1$ суть все[5] корни x^8-1, но 5-й кратности.

Рассмотрим разложение многочлена x^8-1 над $\mathbb{F}_5$. Относительно умножения на 5 вычеты по модулю 8 $\{\overline{0}, \overline{1}, \dots, \overline{7}\}$ разбиваются на орбиты:

$$\{\overline{0}\}, \{\overline{1}, \overline{5}\}, \{\overline{2}\}, \{\overline{3}, \overline{7}\}, \{\overline{4}\}, \{\overline{6}\}.$$

Пояснение: $5 \cdot 5 = 25 \equiv_8 1$, $2 \cdot 5 = 10 \equiv_8 2$ и т.д.

Поэтому:

- бином $x^8-1 \in \mathbb{F}_5[x]$ разлагается в произведение 4-х линейных и 2-х неприводимых квадратных многочленов;

[5] они все различны

- бином $x^{40}-1$ разлагается в произведение 20-и многочленов степени 1 (4-х линейных кратности 5 каждый) и 10-и неприводимых многочленов степени 2 (2-х квадратных кратности 5 каждый);
- максимальная степень неприводимых делителей-многочленов есть 2, следовательно полем расширения данного бинома будет $\mathbb{F}_5^2$.

Замечание. В данном случае разложение $x^8-1 \in \mathbb{F}_5[x]$ на неприводимые множители легко находится (первые 3 равенства справедливы в любом кольце):

$$
\begin{aligned}
x^8-1 &= (x^4-1)(x^4+1),\\
x^4-1 &= (x^2-1)(x^2+1),\\
x^2-1 &= (x-1)(x+1),\\
x^2+1 \equiv_5\ x^2-4 &= (x-2)(x+2),\\
x^4+1 \equiv_5\ x^4-4 &= (x^2-2)(x^2+2),\\
&\text{итого в } \mathbb{F}_5[x]:\\
x^8-1 &= (x+1)(x-1)(x+2)(x-2)(x^2+2)(x^2-2).
\end{aligned}
$$

И далее

$$x^{40}-1 = (x+1)^5(x-1)^5(x+2)^5(x-2)^5(x^2+2)^5(x^2-2)^5.$$

Задача 2.31. *Найти корни* $f(x)=x^2+x+1=0$, *если*

(1) $f(x)\in\mathbb{F}_2[x]$; (2) $f(x)\in\mathbb{F}_3[x]$; (3) $f(x)\in\mathbb{F}_5[x]$.

Решение. $\deg f(x)=2$ и поэтому $f(x)$ имеет 2 корня.

(1) Полином $f(x)$ неприводим над $\mathbb{F}_2 \Rightarrow$ его корни x и x^2.

(2) Полином $f(x)$ приводим над $\mathbb{F}_3$:

$$x^2+x+1 \;=\; x^2-2x+1 \;=\; (x-1)^2,$$

поэтому $f(x)$ над $\mathbb{F}_3$ имеет корень 1 степени 2.

(3) Полином $f(x)$ неприводим над $\mathbb{F}_5 \Rightarrow$ его корни x и x^5.

Задача 2.32. *Решить уравнение*

$$f(x) \;=\; 2x^4+x^3+4x^2+4 \;=\; 0, \;\; \textit{где} \;\; f(x)\in\mathbb{F}_5[x].$$

Решение. Вычисляем значения $f(x)$ для всех $x \in \mathbb{F}_5 = \{0,1,2,3,4\}$: $f(0)=4$, $f(1)=1$, $f(2)=0$ и т. о. $x=2$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x)=x-2=x+3$, получим $2x^4+x^3+4x^2+4 \;=\; (x+3)\cdot(2x^3+4x+3)$.

Для удобства нормируем частное $2x^3+4x+3$: т. к. $2^{-1}=3$, то вместо уравнения $2x^3+4x+3=0$ можно решать уравнение

$$f_2(x) \;=\; 3\cdot(2x^3+4x+3) \;=\; x^3+2x+4 \;=\; 0.$$

Перебором элементов $x\in\mathbb{F}_5$ —

$$f(0)=4,\;\; f(1)=2,\;\; f(2)=1,\;\; f(3)=2,\;\; f(4)=1,$$

убеждаемся, что $f_2(x) = x^3+2x+4$ — неприводимый многочлен[6].

В поле $\mathbb{F}_5[x]/\big(x^3+2x+4\big)$ корнями многочлена $f_2(x)=0$ будут x, x^5, x^{25}.

[6] а если бы это был многочлен 4-й степени?

Вычисляем — с учётом $x^3 = -2x - 4 = 3x + 1$:

$$\begin{aligned} x^5 &= x^2(3x+1) = 3x^3 + x^2 = 4x + 3 + x^2 = \\ &= x^2 + 4x + 3; \\ x^{25} &= \left(x^5\right)^5 = \left(x^2 + 4x + 3\right)^5 = x^{10} + 4^5 x^5 + 3^5 = \\ &= x^{10} + 4(x^2 + 4x + 3) + 3 = x^{10} + 4x^2 + x. \end{aligned}$$

(поскольку $4^5 = 2^{10} = 102\underline{4}$ и $3^5 = 81 \cdot 3 = 24\underline{3}$).

Найдём отдельно x^{10}:

$$\begin{aligned} x^{10} &= \left(x^5\right)^2 = \left(x^2 + 4x + 3\right)^2 = \\ &= x^4 + x^2 + 3^2 + 3x^3 + 4x + x^2 = \\ &= x^4 + 3x^3 + 2x^2 + 4x + 4 = \\ &= 3x^2 + x + 4x + 3 + 2x^2 + 4x + 4 = 4x + 2. \end{aligned}$$

Продолжаем:

$$x^{25} = x^{10} + 4x^2 + x = 4x + 2 + 4x^2 + x = 4x^2 + 2.$$

Ответ: уравнение $f(x) = 2x^4 + x^3 + 4x^2 + 4 = 0$, где $f(x) \in \mathbb{F}_5[x]$ имеет корни 2, x, x^2+4x+3, $4x^2+2$ в поле $F = \mathbb{F}_5[x]/\left(x^3 + 2x + 4\right)$ (поскольку корень $2 \in F$).

Задача 2.33. *Решить уравнение*

$$f(x) = x^8 + x^4 + x^2 + x + 1 = 0, \text{ где } f(x) \in \mathbb{F}_2[x].$$

Решение. В таблицах неприводимых многочленов данный многочлен отсутствует.

Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над $\mathbb{F}_2$ многочленов:

$$x^8+x^4+x^2+x+1 = \underbrace{(x^4+x^3+1)}_{f_1(x)} \cdot \underbrace{(x^4+x^3+x^2+x+1)}_{f_2(x)}.$$

Уравнения $f_1(x)=0$ и $f_2(x)=0$ ранее были решены: их корни соответственно суть

x, x^2, x^3+1, x^3+x^2+x в поле $F_1 = \mathbb{F}_2[x]/\big(x^4+x^3+1\big)$

и

x, x^2, x^3, x^3+x^2+x+1

в поле $F_2 = \mathbb{F}_2[x]/\big(x^4+x^3+x^2+x+1\big)$.

Степени обоих расширений поля $GF(2)$ совпадают $(=4)$ и поля F_1 и F_2 изморфны (*пока не доказано!*), т.о. все 8 корней уравнения $f(x)=0$ лежат в поле $GF(2^4)$.

Для записи данных корней выберем представление F_1 поля $GF(2^4)$. Тогда запись корней $f_1(x)=0$ останется без изменений, а корни $f_2(x)=0$ надо представить как элементы F_1.

Приравнивая многочлены, порождающие данные поля, получим

$$x^4+x^3+1 = x^4+x^3+x^2+x+1 \;\Rightarrow\; x^2+x = x(x+1) = 0.$$

Ясно, что при подстановке $x \mapsto x+1$ полученное равенство останется справедливым. Применим данную постановку для изоморфного преобразования полей $F_1 \leftrightarrow F_2$.

Находим представления корней многочлена $f_2(x)$ в поле F_1:

$$x \mapsto x+1,$$

$$x^2 \mapsto (x+1)^2 = x^2+1,$$
$$x^3 \mapsto (x+1)^3 = x^3+x^2+x+1,$$
$$x^3+x^2+x+1 \mapsto (x^3+x^2+x+1)+(x^2+1)+$$
$$+(x+1)+1 = x^3.$$

Удостоверимся, что, например, x^2+1 — корень $f(x)$:

$$f(x^2+1) = (x^2+1)^8+(x^2+1)^4+(x^2+1)^2+(x^2+1)+1 =$$
$$= (x^{16}+1)+(x^8+1)+(x^4+1)+x^2.$$

Очевидно $x^{16} = x$, $x^4 = x^3+1$ и $x^8 = (x^3+1)^2 = x^6+1$. Поскольку $x^5 = x^4+x = x^3+x+1$, то
$x^6 = x^4+x^2+x = x^3+x^2+x+1$ и $x^8 = x^3+x^2+x$.

Подставляя в выражение для $f(x^2+1)$ полученные полиномиальные представления степеней x, получим

$$f(x^2+1) = (x+1)+(x^3+x^2+x+1)+x^3+x^2 = 0.$$

Ответ: многочлен $f(x) = x^8+x^4+x^2+x+1 \in \mathbb{F}_2[x]$ имеет в поле $\mathbb{F}_2[x]/\left(x^4+x^3+1\right)$ корни x, x^2, x^2+1, x^3, x^3+1, x^3+x^2+x, $x+1$, x^3+x^2+x+1.

Задача 2.34. *Найти корень многочлена*

$$f(x) = x^4+2x+2 \in \mathbb{F}_3[x].$$

Решение. Выясним сначала разложимость $f(x)$. Поскольку $f(0) = f(1) = 2$, $f(2) = 1$, то $f(x)$ линейных делителей не имеет.

Проверим существование квадратичных делителей:

$$f(x) = x^4 + 2x + 2 = (x^2 + ax + b)(x^2 + cx + d) =$$
$$= x^4 + cx^3 + dx^2x + ax^3 + acx^2 + adx + bx^2 + bcx + bd =$$
$$= x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd.$$

Отсюда

1) $c = -a$ и коэффициент при x^2 есть $b - a^2 + d = 0$;
2) из $bd = 2$ следует, что либо $b = 1$ и $d = 2$, либо $b = 2$ и $d = 1$, т. е. в любом случае $b + d = 3 = 0$;
3) но тогда из п. (1) $a^2 = 0$, т. е. $a = c = 0$ и коэффициент при x равен $0 \Rightarrow$ противоречие.

Т.о. полином $f(x) = x^4 + 2x + 2 = 0$ над $\mathbb{F}_3$ *неприводим*.

Теперь рассмотрим поле $\mathbb{F}_3[x]/\big(x^4 + 2x + 2\big)$.

В нём $f(x) = x^4 + 2x + 2 = 0$, т. е. $x^4 = x + 1 = 0$, и корни $f(x)$ суть x, x^3, x^{3^2}, x^{3^3}.

Вычислим x^9 и x^{27}:

$$x^9 = \big(x^4\big)^2 x = (x + 1)^2 x = x^3 + 2x^2 + x;$$
$$x^{27} = \big(x^9\big)^3 = (x^3 + 2x^2 + x)^3 = x^9 + 2x^6 + x^3 =$$
$$= (x^3 + 2x^2 + x) + 2x^2x^4 + x^3 =$$
$$= x^3 + 2x^2 + x + 2x^3 + 2x^2 + x^3 =$$
$$= x^3 + x^2 + x.$$

Ответ: полином $f(x) = x^4 + 2x + 2$ имеет корни x, x^3, $x^3 + 2x^2 + x$, $x^3 + x^2 + x$ в поле $\mathbb{F}_3[x]/(f)$.

Задача 2.35. *Решить уравнение* $f(x) = x^5 + x^2 + 1 = 0$ *для* $f(x) \in \mathbb{F}_2[x]$.

Решение. Поскольку $f(0) = f(1) = 1$, полином $f(x)$ линейных делителей не имеет. Кроме того, легко устанавливается, что

$$x^5 + x^2 + 1 = (x^2 + x + 1)(x^3 + x^2) + 1,$$

т. е. полином $f(x)$ не имеет и (единственного) квадратичного неразложимого делителя и, поскольку его степень равна 5, то он *неприводим*.

Рассмотрим теперь поле $\mathbb{F}_2[x]/\big(x^5 + x^2 + 1\big)$. В нём $f(x) = x^5 + x^2 + 1 = 0$, т. е. $x^5 = x^2 + 1 = 0$ и корни $f(x)$ суть x, x^2, x^{2^2}, x^{2^3}, x^{2^4}.

Вычислим x^8 и x^{16}:

$$\begin{aligned} x^8 &= x^5x^3 = (x^2+1)x^3 = x^5 + x^3 = x^3 + x^2 + 1; \\ x^{16} &= \big(x^8\big)^2 = (x^3 + x^2 + 1)^2 = x^6 + x^4 + 1 = \\ &= x^5x + x^4 + 1 = (x^3 + x) + x^4 + 1 = \\ &= x^4 + x^3 + x + 1. \end{aligned}$$

Ответ: в поле $\mathbb{F}_2[x]/\big(x^5 + x^2 + 1\big)$ уравнение

$$f(x) = x^5 + x^2 + 1 = 0$$

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

Глава 3

Коды, исправляющие ошибки

3.1 Блоковое кодирование. Коды Хэмминга

Задача помехоустойчивого кодирования. По каналу с шумом проходит поток *битовой* информации (или хранимая информация искажается), вследствие чего возникают ошибки.

- *Модель ошибок*: биты случайно, независимо и с равными вероятностями могут оказаться инвертированными (*двоичный симметричный канал*), вставки/выпадения битов нет.
- *Задача*: обеспечить автоматическое исправление ошибок.

Подход к решению (один из возможных!):

1) входной поток информации разбить на *сообщения* — непересекающиеся блоки фиксированной длины k;
2) каждый блок *кодировать* (модифицировать) —
   а) независимо от других — *блоковое кодирование*;
   б) в зависимости от предыдущих — *свёрточное* или *потоковое кодирование* (турбо-коды).

Далее рассматривается исключительно *блоковое кодирование*:

- есть набор всех *сообщений* $S_1, \ldots, S_t$, длины k каждое ($t = 2^k$), которые нужно передать по каналу связи с шумом;
- для обеспечения помехозащишённости вместо этих сообщений передают *кодовые слова*, каждое длины $n > k$, т. е. вводят *избыточность* при передаче информации: дополнительные m бит, $n = k + m$.
- *код* — инъективное отображение $\varphi : \{0,1\}^k \to \{0,1\}^n,\ k < n$;
- *кодовые слова* — область значений $C = Im\,\varphi \subset \{0,1\}^n$ кода.
- $R = k/n$ — *скорость*, $m/n = 1 - R$ — *избыточность кода*.

Чем меньше избыточность и чем больше число ошибок, которые может исправить код, тем он лучше. Ясно, что эти требования противоречат друг другу и одно достигается за счёт другого.

Кодовое расстояние. Понятия, связанные с единичным (булевым) кубом B^n.

- *Норма* или *вес* $\|\widetilde{\gamma}\|$ = число единичных координат в наборе $\widetilde{\gamma} \in B^n$.

- *Метрика* на множестве бинарных наборов — *хэммингово расстояние* (HD) ($+-$ сумма по $\mathrm{mod}\ 2$):

$$\rho(\widetilde{\alpha},\, \widetilde{\beta}) \;=\; \left\| \widetilde{\alpha} + \widetilde{\beta} \right\|.$$

- *Шар Хэмминга с центром в* $\widetilde{\alpha}$ *и радиусом* $r > 0$:

$$S_r(\widetilde{\alpha}) \;=\; \left\{ \widetilde{\beta} \in B^n \;\mid\; \rho(\widetilde{\alpha}, \widetilde{\beta}) \leqslant r \right\}.$$

Определение 3.1. Минимальное расстояние между парами слова кода C называется его *кодовым расстоянием*, символически $d(C)$ или просто d.

Утверждение 3.1. *Множество* C *образует код с исправлением не менее* r *ошибок, если*

$$\forall\, \widetilde{\alpha}, \widetilde{\beta} \in C : \; \widetilde{\alpha} \neq \widetilde{\beta} \;\Rightarrow\; S_r(\widetilde{\alpha}) \cap S_r(\widetilde{\beta}) = \varnothing.$$

Доказательство. Если в векторе $\widetilde{\alpha}$ искажено не более r бит, то набор останется в шаре $S_r(\widetilde{\alpha})$. Если шары не пересекаются, то искомое кодовое слово — ближайший к полученному набору центр шара. □

Следствие. *У кода, исправляющего* r *ошибок, кодовое расстояние* d *должно быть не менее* $2r + 1$.

Определение кодового расстояния произвольного кода C — *трудоёмкая задача*: показано, что эта задача NP-тудна. В общем случае для нахождения $d(C)$ требуется перебрать все $\frac{2^k(2^k-1)}{2}$ пар кодовых слов, что практически невозможно уже начиная с $k = 50$.

Поэтому важной задачей является построение *кодов с заданным кодовым расстоянием*. Она решается при использовании, например, БЧХ-кодов, которые будут рассмотрены далее.

Блоковое кодирование и декодирование

Блоковое кодирование — взаимно-однозначное преобразование сообщений длины k в кодовые слова длины $n > k$.

Декодирование — определение сообщения по принятому слову.

Пример 3.1 (тривиальный код-повторение). Информация разбивается на блоки по $k = 1$ бит, т. е. передаются 2 сообщения: $S_0 = 0$ и $S_1 = 1$.

Кодирование ($n = 3$): $0 \mapsto 000, \quad 1 \mapsto 111$ *исправляет одну ошибку*. Однако такое кодирование крайне неэффективно: длина сообщения *утраивается*.

Код-повторение $a \mapsto \underbrace{a \ldots a}_{2r+1}$, очевидно, исправит r ошибок. Этот и другие *тривиальные* n*-коды* — с 2^n кодовыми словами и сообщениями нулевой длины не рассматриваем.

Кодирование. Обозначения:

- сообщение — вектор-столбец $\boldsymbol{u} \in \{0,1\}^k$:
$$\boldsymbol{u} = \begin{bmatrix} u_1 \\ \cdots \\ u_k \end{bmatrix};$$
- кодовое слово — вектор-столбец[1] $\boldsymbol{v} \in \{0,1\}^n$;
- множество всех кодовых слов — (n,k)-*код*, или, с кодовым расстоянием — (n,k,d)-*код*.

[1] некоторые авторы используют векторы-строки: будьте внимательны!

Блоковое кодирование всегда можно осуществить с использованием таблицы размера $2^k \times n$. Однако такое «табличное» кодирование весьма неэффективно: значения n и k могут достигать *десятков и сотен тысяч*.

При передаче по каналу с шумом кодовое слово $\boldsymbol{v}$ превращается в *принятое слово* $\boldsymbol{w}$ той же длины n,

$$\boldsymbol{v} \;\to\; \boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e},$$

где $\boldsymbol{e} \in \{0,1\}^n$ — *вектор ошибок*:

$$e_i = \begin{cases} 1, & \text{если в } i\text{-ом бите произошла ошибка.} \\ 0, & \text{если ошибки нет.} \end{cases}$$

Декодирование (n,k,d)-кода *обычно значительно сложнее* кодирования. Оно основано на разбиении единичного куба B^n на k областей, содержащих шары радиуса $r = \lfloor (d-1)/2 \rfloor$ с центрами в кодовых словах и предположении, что произошло $\leqslant r$ ошибок.

Схема кодирования/декодирования блокового кода:

$$\boldsymbol{u} \xrightarrow[\text{избыточность}]{\text{кодирование}} \boldsymbol{v} \xrightarrow[+\boldsymbol{e}]{\text{ошибка}} \boldsymbol{w} \xrightarrow[\text{ближ. код. слово}]{\text{декод.-1}} \widehat{\boldsymbol{v}} \xrightarrow[\text{удаление избыт.}]{\text{декод.-2}} \widehat{\boldsymbol{u}}$$

Декодирование блокового разделимого (n,k,d) кода проводится в два этапа:

1-й этап: Определение кодового слова $\widehat{\boldsymbol{v}}$ как ближайшего в метрике Хэмминга слову к $\boldsymbol{w}$, т. е. нахождение центра соответствующего шара (*декодирование в ближайшее кодовое слово*). Если произошло до $\lfloor (d-1)/2 \rfloor$ ошибок, то $\widehat{\boldsymbol{v}} = \boldsymbol{v}$.

2-й этап: Удаление избыточности и восстановление исходного сообщения по кодовому слову $\widehat{\boldsymbol{v}}$.

Ясно, что в общем случае при выполнении 1-го этапа надо перебрать все 2^n строк в $2^n \times k$-таблице кодовых слов. Поэтому декодирование блокового (n,k)-кода *общего вида* является крайне ресурсоёмким процессом, и использование таких кодов возможно лишь при небольших значениях n и k.

Однако, приняв дополнительные ограничения на множество кодовых слов, можно перейти от *экспоненциальных* требований по памяти и по сложности алгоритмов кодирования/декодирования к *линейным* по n и k. Эти ограничения приводят к использованию блоковых кодов специального вида: *групповых*, а из групповых — *циклических*.

Плотная упаковка шаров в единичный куб. Чтобы построить код минимальной избыточности исправляющий данное количество r ошибок, нужно вложить в единичный куб B^n максимально возможное число непересекающихся шаров радиуса r — это *задача плотной упаковки*.

Вопрос: При каких n и r в куб B^n можно уложить непересекающиеся шары радиуса r «плотно», «без зазоров»?

Ответ: Такое удаётся только в двух нетривиальных случаях:

1) $n = 2^q - 1$, $r = 1$ — *коды Хэмминга*, у них $m = q$ и $k = 2^m - 1 - m$;

2) $n = 23$, $r = 3$ — *код Голея*, к него $m = 11$ и $k = 12$.

Это *совершенные* или *экстремальные коды*.

Теорема 3.1 (Хэмминга). *При* $2r < n$ *максимальное число* t *кодовых слов находится в пределах*

$$\frac{2^n}{C_n^0 + C_n^1 + \ldots + C_n^{2r}} \leqslant t \leqslant \underbrace{\frac{2^n}{C_n^0 + C_n^1 + \ldots + C_n^r}}_{\text{граница Хэмминга}}.$$

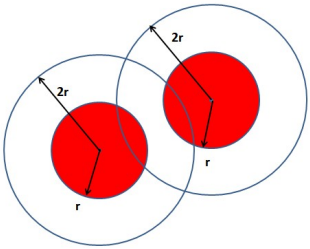
Доказательство. Для получения *верхней оценки* числа непересекающихся шаров радиуса r разделим объём булева куба на объём шара. Шар радиуса r содержит: центр + все точки с одной, двумя, ..., r измененными координатами.

Для *оценки снизу* построим негрупповой код:

1) берем произвольную точку B^n и строим вокруг неё шар радиуса $2r$;
2) берем произвольную точку вне построенного шара и строим вокруг неё шар радиуса $2r$;
3) и т.д., каждая новая точка выбирается вне построенных шаров.

В результате:

- шары, возможно, пересекаются, но каждый шар занимает $C_n^0 + C_n^1 + \ldots + C_n^{2r}$ точек $\Rightarrow$ шаров не менее $2^n / \left(C_n^0 + C_n^1 + \ldots + C_n^{2r}\right)$;
- шары радиуса r с центрами в выбранных точках не пересекаются.



□

Построим конкретный код Хэмминга длины $2^m - 1$ и покажем, что для него граница Хэмминга достигается.

Рассмотрим таблицу:

$$
\left.
\begin{array}{cc}
100\ldots000 & 1100\ldots000 \\
010\ldots000 & 1010\ldots000 \\
001\ldots000 & 1001\ldots000 \\
\ldots & \ldots \\
000\ldots100 & 1111\ldots101 \\
000\ldots010 & 1111\ldots110 \\
000\ldots001 & 1111\ldots111
\end{array}
\right\} k = 2^m - (m+1)
$$

$$
\underbrace{\qquad\qquad}_{k = 2^m - (m+1)} \quad \underbrace{\qquad\qquad}_{m}
$$

Слева — единичная матрица порядка $2^m - 1 - m$, справа — все бинарные наборы длины m, содержащие *не менее двух* единиц.

Просуммировав всевозможные совокупности строк таблицы, получим $t = 2^k = 2^{2^m-(m+1)}$ различных кодовых слов, но

$$
t = 2^{2^m-(m+1)} = \frac{2^{2^m-1}}{2^m} = \frac{2^n}{1+n}.
$$

Найдём кодовое расстояние построенного кода:

- в каждой строке таблицы — не менее 3 единиц;
- если сложить

  две строки — в левой части будет 2 единицы, а в правой — хотя бы одна,

  не менее трёх строк — в левой части будет не менее 3 единиц.

  Т. е. всегда $\rho(\widetilde{\alpha}, \widetilde{\beta}) \geqslant 3 \Rightarrow$ шары единичного радиуса с центрами в полученных наборах не пересекаются.

Заметим, что при таком кодировании исходное сообщение окажется в первых k позициях кодового слова.

Пример 3.2 (код Хэмминга $(7, 4)$).

Для $m = 3$ $(2^3 - 1 = 7)$ составим таблицу

1	0	0	0	1	1	0
0	1	0	0	1	0	1
0	0	1	0	0	1	1
0	0	0	1	1	1	1

Складывая по $\bmod 2$ все, включая пустую, совокупности строк полученной таблицы, получаем $2^4 = 16$ различных бинарных слов длины 7, которыми можно закодировать 16 сообщений.

Этот код содержит по одному слову веса 0 и 7, по семь слов веса 3 и 4.

Код Голея — (23, 12, 7)-код. М. Голей обнаружил, что

$$\underbrace{C_{23}^0 + C_{23}^1 + C_{23}^2 + C_{23}^3}_{\text{объём шара радиуса 3}} = 2^{11}.$$

Это позволило предположить, что существует содержащий

$$t = 2^{23}/2^{11} = 2^{12} = 4096$$

кодовых слов совершенный $(23, 12, 7)$-код, исправляющий до 3-х ошибок, и М. Голей в своей статье указал такой код.

Доказано, что других пар (n, r), удовлетворяющих условию

$$\frac{2^n}{C_n^0 + \ldots + C_n^r} \quad \text{— целое,}$$

кроме кодов Хэмминга и тривиальных — не существует.

3.2 Линейные коды

Линейные коды: определение, свойства

Бóльшая часть теории блокового кодирования построена на *линейных* кодах, позволяющих реализовывать эффективные алгоритмы кодирования/декодирования. В двоичном случае их называют *групповыми*, т. к. они образуют *группу относительно операции «сумма по* $\bmod 2$*»*.

Утверждение 3.2. *Устойчивая относительно операции суммы по* $\bmod 2$ *(+) совокупность кодовых слов* C *образует группу.*

Доказательство.

Устойчивость (*предполагается*): для любых кодовых слов $\widetilde{\alpha},\, \widetilde{\beta} \in C$ выполняется $\widetilde{\alpha} + \widetilde{\beta} = \widetilde{\gamma} \in C$;

Ассоциативность: свойство операции $+$;

Существование 0: $\widetilde{\alpha} + \widetilde{\alpha} = (0, \ldots, 0) = \widetilde{0} \in C$;

Противоположные элементы: $-\widetilde{\alpha} = \widetilde{\alpha}$.

□

Теорема 3.2 (кодовое расстояния группового кода). *Кодовое расстояние d группового кода равно*

$$d = \min_{\widetilde{\alpha} \neq \widetilde{\beta}} \rho(\widetilde{\alpha}, \widetilde{\beta}) = \min_{\widetilde{\gamma} \neq \widetilde{0}} \|\widetilde{\gamma}\|,$$

где $\widetilde{\alpha}$, $\widetilde{\beta}$ и $\widetilde{\gamma}$ — кодовые слова из C.

Доказательство. Для произвольных кодовых слов $\widetilde{\alpha}$ и $\widetilde{\beta}$ всегда существует их сумма — кодовое слово γ:

$$\rho(\widetilde{\alpha}, \widetilde{\beta}) = \left\| \widetilde{\alpha} + \widetilde{\beta} \right\| = \|\widetilde{\gamma}\|,$$

причем $\widetilde{\gamma} \neq \widetilde{0}$ при $\widetilde{\alpha} \neq \widetilde{\beta}$.

Отсюда получаем оценку $\min\limits_{\widetilde{\alpha} \neq \widetilde{\beta}} \rho(\widetilde{\alpha}, \widetilde{\beta}) \geqslant \min\limits_{\widetilde{\gamma} \neq \widetilde{0}} \|\widetilde{\gamma}\|$, которая достигается, например, при $\widetilde{\beta} = \widetilde{0}$. □

Следствие. Для вычисления кодового расстояния группового кода достаточно перебрать $2^k - 1$ кодовых слов.

Единичный куб $B^n = \{0,1\}^n$ можно рассматривать как n-мерное координатное векторное пространство над конечным полем $\mathbb{F}_2 = \{0,1\}$.

Определение 3.2. Блоковый (n, k)-код называется *линейным*, если он образует *векторное подпространство* размерности k координатного пространства B^n.

Это означает, что в *линейном* коде C —

1) сумма любых кодовых слов — кодовое слово, т. е. это *групповой* код;
2) кодовое расстояние $d(C) = \min\limits_{\widetilde{\gamma} \in C} \|\widetilde{\gamma}\|$;
3) существует базис $\{\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{k-1}\}$ из k векторов-столбцов $\boldsymbol{g}_i \in B^n$, $i = 0, \ldots, k-1$, и любой вектор $\boldsymbol{v} \in C$ может быть представлен как
$$\boldsymbol{v} = \sum_{i=0}^{k-1} u_i \boldsymbol{g}_i, \quad u_i \in \{0, 1\}.$$

Порождающая матрица. Систематическое кодирование

$$\boldsymbol{v} = \sum_{i=0}^{k-1} u_i \boldsymbol{g}_i = G\boldsymbol{u}\,, \text{ где } G_{n\times k} = [\,\boldsymbol{g}_0\, \boldsymbol{g}_1\, \ldots\, \boldsymbol{g}_{k-1}\,]$$

— *порождающая матрица* линейного кода.

Матрица G определена с точностью до *элементарных преобразований столбцов* — их перестановкам и сложению по $\bmod 2$ данного столбца с любым другим. Данные преобразования эквивалентны переходу к другому базису *этого же* кода[2].

[2] Элементарные преобразования *строк* G приведут к *другому блоковому линейному коду* в B^n.

Пусть линейный код задан порождающей матрицей $G_{n,k}$. Из неё с помощью элементарных преобразований столбцов может быть получена матрица $\widetilde{G}$, у которой *первые* k строк образуют единичную подматрицу I_k. Тогда при кодировании $\boldsymbol{v} = \widetilde{G}\boldsymbol{u}$ первые k бит сообщения перейдут в первые биты кодового слова.

Кодирование, при котором информационные биты переходят в фиксированные позиции сообщения, называют *систематическим* или *разделимым*. Остальные (избыточные) биты сообщения называют *проверочными*. Систематическое кодирование делает тривиальным 2-й этап декодирования: исходное сообщение есть результат удаления из кодового слова проверочных бит.

Ясно, что любой линейный код можно преобразовать в эквивалентный ему систематический.

Пример 3.2 (продолжение — (7, 4)-код Хэмминга).

Ранее была получена таблица, сложением различных групп строк которой получаются все кодовые слова данного кода Хэмминга. Порождающая матрица кода получается транспонированием этой таблицы:

$$G_{7\times4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

— порождающая матрица в систематической форме: при кодировании исходные сообщения помещаются в первые 4 бита кодового слова

Историческая справка. Первой ЭВМ, в которой использовался код Хэмминга, была IBM 7030, построенная в

1960 г., через 10 лет после появления кода Хэмминга. До этого использовался лишь простейший способ повышения надежности — *проверка на чётность*.

Ортогональное дополнение к коду и проверочная матрица

Итак, линейный код C есть k-мерное подпространство n-мерного линейного пространства $\{0,1\}^n = B^n$.

Элементы B^n, ортогональные ко всем элементам кода C образуют *ортогональное подпространство* $C^\perp$:

$$\underset{C}{\forall}\boldsymbol{v}\ \underset{C^\perp}{\forall}\boldsymbol{w}:\ \boldsymbol{v}^T\times\boldsymbol{w}\ =\ 0.$$

Замечания:

- $\dim B^n\ =\ n\ =\ \underbrace{\dim C}_{k}+\underbrace{\dim C^\perp}_{m=n-k}$;
- $C\cup C^\perp\ \neq\ B^n$, т. е. B^n — *не есть прямая сумма* подпространств C и $C^\perp$;
- произвольный вектор из B^n может либо не разлагаться, либо разлагаться неоднозначно в сумму векторов из C и $C^\perp$.

Пусть $\{\boldsymbol{h}_0,\ \ldots,\ \boldsymbol{h}_{m-1}\}$ — базис $C^\perp$, $\boldsymbol{h}_i$ — векторы-столбцы из B^n, $i\ =\ 0,\ \ldots,\ m-1$. Тогда матрица

$$H_{m\times n}\ =\ \begin{bmatrix}\boldsymbol{h}_0^T\\ \boldsymbol{h}_1^T\\ \vdots\\ \boldsymbol{h}_{m-1}^T\end{bmatrix}$$

называется *проверочной матрицей* линейного кода C.

Ясно, что

- $\forall\, \boldsymbol{v} \in C\colon\ H\boldsymbol{v} = \mathbf{0}$ — нулевой m-мерный вектор;
- $HG = O_{m\times k}$ — нулевая матрица;
- проверочная матрица определена с точностью до элементарных преобразований *строк*.

Пусть I_k и I_m — единичные матрицы порядков k и m соответственно. Тогда если порождающая матрица имеет вид

$$G = \begin{bmatrix} I_k \\ P_{m\times k} \end{bmatrix},$$

то матрица $H = \begin{bmatrix} P_{m\times k} & I_m \end{bmatrix}$ будет проверочной. Действительно, в этом случае

$$H\boldsymbol{v} = HG\boldsymbol{u} = \begin{bmatrix} P & I \end{bmatrix} \times \begin{bmatrix} I \\ P \end{bmatrix} \boldsymbol{u} = (P+P)\boldsymbol{u} = \mathbf{0}.$$

Проверочную матрицу называют также *матрицей проверки на чётность*, а строки — *правилами проверки на чётность*.

Пример 3.2 (продолжение — $(7,4)$-код Хэмминга). Для построенной порождающей матрицы $G_{7\times 4}$ проверочной будет

$$H_{3\times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Легко видеть, что столбцами проверочной матрицы кода кода Хэмминга являются все ненулевые векторы длины m.

Задание линейного кода. Пример кодирования

Резюмируем: линейный код C для сообщений длины k имеет длину $n = k + m$, m — число избыточных (при систематическом кодировании — проверочных) символов, и задаётся

либо порождающей матрицей $H_{n\times k}$,

либо проверочной матрицей $G_{m\times n}$.

Эти матрицы определены с точностью до элементарных преобразований столбцов и строк соответственно, что соответствует выбору различных базисов кода в пространствах C и $C^{\perp}$. Однако *фиксирование позиций информационных бит при систематическом кодировании* задаёт H и G *однозначно*.

Увеличение m ведёт к увеличению кодового расстояния d (как конкретно — очень трудный вопрос) и, следовательно, к увеличению количества ошибок, которые может исправить код.

Пример 3.3 (кодирования блоковым линейным кодом). Пусть дан линейный $(6, 3)$-код задан порождающей матрицей

$$G_{6\times 3} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Требуется:

1) с использованием данного кода осуществить
   (а) несистематическое и

(б) систематическое кодирование
векторов $\boldsymbol{u}_1 = [0\ 1\ 1]^T$ и $\boldsymbol{u}_2 = [1\ 0\ 1]^T$;

2) построить проверочную матрицу H;

3) определить кодовое расстояние d данного кода.

1 (а). Несистематическое кодирование находим непосредственно:

$$[\,\boldsymbol{v}_1^n\,\boldsymbol{v}_2^n\,] = G \times [\,\boldsymbol{u}_1\,\boldsymbol{u}_2\,] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

1 (б). Для систематического кодирования с помощью элементарных преобразований *столбцов* выделим в матрице G единичную подматрицу размера 3×3 (над стрелкой указано проводимое преобразование столбцов):

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{(1)+(2)\mapsto(1)} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \widetilde{G}.$$

В полученной матрице в строках 3, 5 и 1 стоит единичная подматрица — это приведёт к тому, что 1, 2 и 3-й биты исходного сообщения последовательно перейдут в 3, 5 и 1-й биты кодового слова.

Найдём систематическое кодирование $\boldsymbol{u}_1, \boldsymbol{u}_2$:

$$[\,\boldsymbol{v}_1^s\,\boldsymbol{v}_2^s\,] = \widetilde{G}\times[\,\boldsymbol{u}_1\,\boldsymbol{u}_2\,] = \begin{bmatrix}0&0&1\\1&0&1\\1&0&0\\0&1&1\\0&1&0\\1&1&1\end{bmatrix}\times\begin{bmatrix}0&1\\1&0\\1&1\end{bmatrix} = \begin{bmatrix}1&1\\1&0\\0&1\\0&1\\1&0\\0&0\end{bmatrix}.$$

2. Находим проверочную матрицу H, формируя матрицу $P_{3\times3}$ из строк $\widetilde{G}$, отличных от строк единичной подматрицы:

$$P_{3\times3} = \begin{bmatrix}1&0&1\\0&1&1\\1&1&1\end{bmatrix}.$$

Для построения проверочной матрицы H нужно

- последовательно разместить *столбцы* P в 3, 5 и 1-м её столбцах соответственно,
- остальные 2, 4 и 6-й столбцы H должны образовывать единичную подматрицу.

В итоге получим проверочную матрицу

$$H_{3\times6} = \begin{bmatrix}1&1&1&0&0&0\\1&0&0&1&1&0\\1&0&1&0&1&1\end{bmatrix}.$$

Предлагается самостоятельно проверить, что $HG = H\widetilde{G} = \mathbf{0}$ — нулевая (3×3)-матрица.

Проверим, что в результате как систематического, так и несистематического кодирований были действительно найдены кодовые слова:

$$H\times[\,\boldsymbol{v}_1^n\,\boldsymbol{v}_2^n\,\boldsymbol{v}_1^s\,\boldsymbol{v}_2^s\,]=\begin{bmatrix}1&1&1&0&0&0\\1&0&0&1&1&0\\1&0&1&0&1&1\end{bmatrix}\times\begin{bmatrix}1&1&1&1\\1&0&1&0\\0&1&0&1\\0&0&0&1\\1&1&1&0\\0&1&0&0\end{bmatrix}=$$

$$=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}.$$

3. Найдем кодовое расстояние d. Для этого закодируем все $2^3=8$ сообщений и найдем минимальный ненулевой хэммингов вес кодового слова:

$$C=[\boldsymbol{v}_1\,\ldots\,\boldsymbol{v}_8]=\widetilde{G}\times[\boldsymbol{u}_1\,\ldots\,\boldsymbol{u}_8]=$$

$$=\begin{bmatrix}0&0&1\\1&0&1\\1&0&0\\0&1&1\\0&1&0\\1&1&1\end{bmatrix}\times\begin{bmatrix}0&0&0&0&1&1&1&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\end{bmatrix}=$$

$\boldsymbol{u}_1,\ldots,\boldsymbol{u}_8$ — все 8 возможных сообщений,
$\boldsymbol{v}_1,\ldots,\boldsymbol{v}_8$ — все 8 возможных кодовых слов.
Оказалось $d=3$.

$$=\begin{bmatrix}0&1&0&1&0&1&0&1\\0&1&0&1&1&0&1&0\\0&0&0&0&1&1&1&1\\0&1&1&0&0&1&1&0\\0&0&1&1&0&0&1&1\\0&1&1&0&1&0&0&1\end{bmatrix}.$$

3.3 Декодирование линейных кодов

Наиболее эффективные методы декодирования линейных кодов, основанные на вычислении исправляющего вектора, который принято называть синдромом[3].

Синдром

Определение 3.3. *Синдромом слова* $\boldsymbol{w} \in \{0,1\}^n$, принятого при передаче сообщения, закодированного линейным (n,k)-кодом и, возможно, содержащего ошибки, назовём вектор $\boldsymbol{s} = H\boldsymbol{w} \in \{0,1\}^m$, где H — проверочная матрица, $m = n - k$.

Свойства синдрома:

- $\boldsymbol{s} = \boldsymbol{0} \Leftrightarrow \boldsymbol{w}$ — кодовое слово, ошибок нет[4];
- $\boldsymbol{s} = H\boldsymbol{w} = H(\boldsymbol{v} + \boldsymbol{e}) = \underbrace{H\boldsymbol{v}}_{=0} + H\boldsymbol{e} = H\boldsymbol{e}$.

Отсюда ясно, что вектор ошибок $\boldsymbol{e}$ удовлетворяет неоднородной недоопределенной СЛАУ

$$H\boldsymbol{e} = \boldsymbol{s}, \qquad (*)$$

а кодовые слова являются решениями соответствующей однородной системы

$$H\boldsymbol{v} = \boldsymbol{0},$$

[3] *Синдром* — совокупность явлений, вызванных отклонением от нормы.

[4] Точнее, $\boldsymbol{s} = \boldsymbol{0}$ означает отсутствие *ошибок определённого типа*, а не их отсутствие вообще; это замечание относится и к декодированию всех рассматриваемых далее кодов.

(или, иными словами — ядром линейного преобразования $H : \{0,1\}^n \to \{0,1\}^m$).

Таким образом, вектор $\boldsymbol{e}$ может быть представлен как частное решение $\widehat{\boldsymbol{e}}$ неоднородной системы $(*)$ и общее решение $\boldsymbol{v} = G\boldsymbol{u}$ соответствующей однородной —

$$\boldsymbol{e} = \widehat{\boldsymbol{e}} + G\boldsymbol{u}.$$

и среди всех возможных векторов $\widehat{\boldsymbol{e}}$ для всех сообщений $\boldsymbol{u}$ необходимо выбрать имеющий минимальный вес.

Схема декодирования по синдрому:

$$\boldsymbol{w} \longrightarrow \boldsymbol{s} = H\boldsymbol{w} \xrightarrow[H\boldsymbol{e}=\boldsymbol{s}]{} \boldsymbol{e} = \widehat{\boldsymbol{e}} + G\boldsymbol{u} \xrightarrow[\|\boldsymbol{e}\|\to\min]{} \widehat{\boldsymbol{v}} = \boldsymbol{w} + \boldsymbol{e}$$

Декодирование по синдрому

Поскольку и принятый вектор $\boldsymbol{w}$, и соответствующий ему вектор ошибок $\boldsymbol{e}$ имеют одинаковые синдромы, можно попытаться восстановить неизвестный вектор $\boldsymbol{e}$, используя тот факт, что он является решением системы $(*)$.

Для этого нужно составить *словарь синдромов* — таблицу, строки которой соответствуют всем возможным синдромам $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{2^m}$, а каждая строка содержит *наиболее вероятный вектор ошибок*, данному синдрому соответствующий. Этот вектор должен иметь наименьший вес среди возможных решений системы $(*)$ для данного $\boldsymbol{s}$ и его называют *лидером* класса векторов ошибок, имеющих общий синдром $\boldsymbol{s}$. Если таких векторов минимального веса несколько, то в качестве лидера может быть выбран любой из них.

Таким образом, данный метод потребует хранения проверочной матрицы размера $m \times n$, словаря синдромов размера $2^m \times n$, но не требует нахождения векторов ошибок минимального веса (они уже найдены на этапе проектирования декодирующего устройства).

Однако в любом случае алгоритм декодирования остаётся *экспоненциально трудоёмким* и по памяти, и по числу операций.

Пример 3.4 (декодирования линейного кода). Рассмотрим линейный $(6, 3)$-код из *Примера* 3.3.

1. Закодируем сообщения $\boldsymbol{u} = \boldsymbol{u}_1 = [0\ 1\ 1]^T$.

Систематическое кодирование для него было уже получено: $\boldsymbol{v} = [1\ 1\ 0\ 0\ 1\ 0]^T$.

Пусть при передаче происходит ошибка во 2-м бите, т. е. принят вектор $\boldsymbol{w} = [1\ 0\ 0\ 0\ 1\ 0]^T$.

Найдём синдром принятого слова $\boldsymbol{w}$:

$$H\boldsymbol{w} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \boldsymbol{s}\,.$$

Заранее, при проектировании устройства декодирования, должны быть найдены лидеры классов векторов ошибок для всех возможных синдромов.

Для полученного синдрома этот класс составляют столбцы матрицы всех кодовых слов C (уже полученной в п. 3 *Примера* 3.3), сложенные, например, с вектором $\boldsymbol{w}$. В этом случае для синдрома $\boldsymbol{s} = [1\ 0\ 0]^T$ был

получен класс

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

Наименьший вес в этой матрице имеет 4-й столбец, и, таким образом, лидером интересующего нас класса является вектор $\boldsymbol{e} = [0\ 1\ 0\ 0\ 0\ 0]^T$. Он-то и помещается в словарь синдромов.

Складывая найденный по словарю синдромов данный лидер с принятым словом, получаем

$$\widehat{\boldsymbol{v}} = \boldsymbol{w} + \boldsymbol{e} = [1\ 0\ 0\ 0\ 1\ 0]^T + [0\ 1\ 0\ 0\ 0\ 0]^T = \\ = [1\ 1\ 0\ 0\ 1\ 0]^T = \boldsymbol{v},$$

и переданное кодовое слово восстановлено верно.

Пусть передаётся сообщение $\boldsymbol{u} = \boldsymbol{u}_2 = [1\ 0\ 1]^T$; оно кодируется словом $\boldsymbol{v} = [1\ 0\ 1\ 1\ 0\ 0]^T$. Пусть также ошибка опять возникла во втором разряде.

Вычисляем синдром принятого слова $\boldsymbol{w} = [1\ 1\ 1\ 1\ 0\ 0]^T$:

$$H\boldsymbol{w} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \boldsymbol{s},$$

т. е. синдром остаётся прежним. Ему соответствует тот же лидер $\boldsymbol{e} = [0\ 1\ 0\ 0\ 0\ 0]^T$ и кодовое слово также верно восстанавливается.

Декодирование кода Хэмминга

В случае кода Хэмминга декодирование можно существенно упростить.

Особенностью проверочной матрицы $H_{m\times n}$ кода Хэмминга является то, что её столбцы представляют собой двоичные коды чисел от 1 до $n = 2^m - 1$.

Например, в *Примере* 3.2 получена матрица

$$H_{3\times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$
$$\begin{matrix} 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{matrix}$$

Хэмминг предложил использовать коды, у которых расположение столбцов проверочной матрицы H было такое, чтобы *синдром являлся двоичным представлением позиции ошибки в принятом сообщении.*

Для этого столбцы H должны быть двоичными представлениями чисел от 1 до $2^m - 1$ *последовательно.* Тогда любой синдром есть соответствующий столбец H, т. е. двоичное представление своего номера = позиция ошибки.

Заметим, что единичную подматрицу такой матрицы будут образовывать столбцы с номерами, являющимися степенью 2: 1, 2, ..., 2^{m-1}.

Пример 3.5.

Для рассматриваемого $(7,4)$-кода Хэмминга получаем матрицу

$$\widetilde{H}_{3\times 7} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$
$$\underline{1}\ \ \underline{2}\ \ 3\ \ \underline{4}\ \ 5\ \ 6\ \ 7$$

Тогда порождающая матрица есть

$$G_{7\times 4} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Она помещает сообщение последовательно в 3, 5, 6 и 7-ю позиции кодового слова, а остальные биты являются проверочными: подматрица образованная 1, 2 и 4-й строками является подматрицей H^T, оставшейся после удаления единичной подматрицы. Ясно, что G осуществляет несистематическое кодирование.

Закодируем данным кодом сообщение $\boldsymbol{u} = [0\,1\,0\,1]^T$:

$$\boldsymbol{v} = G\boldsymbol{u} = [0\,1\,0\,0\,1\,0\,1]^T.$$

Пусть при передаче ошибка произошла в 2-м бите, т. е. получено слово $\boldsymbol{w} = [0\,0\,0\,0\,1\,0\,1]^T$. Тогда синдром

$$\boldsymbol{s} = \widetilde{H}\boldsymbol{w} = [0\,1\,0]^T$$

указывает позицию ошибки.

Дуальные коды. Поскольку $HG = O = G^T H^T$, то можно использовать H^T как порождающую, а G^T — как проверочную матрицу некоторого другого кода и из линейного (n, k)-кода получить $(n, n-k)$-код. Коды, связанные таким образом, называются *дуальными* или *двойственными* друг другу.

Если исходный код был получен так, чтобы иметь минимальную избыточность при заданной исправляющей способности, то гарантировать хорошее качество дуального ему кода уже нельзя: обычно дуальный код имеет такую же исправляющую способность, как и исходный, но большую избыточность.

Код, двойственный к расширенному коду Хэмминга, называется *кодом Макдональда.*

Линейные коды (n, k): резюме

- Линейные коды могут иметь произвольные параметры n и $k < n$.
- Требование линейности производить позволяет упростить кодирование и декодирование.

  Кодирование осуществляется особенно просто — умножением вектора сообщения на порождающую матрицу.

  Но вопрос «*как найти порождающую матрицу для получения кода с хорошими характеристиками?*» остаётся открытым: общие методы синтеза оптимальных линейных кодов до сих пор не разработаны.

Декодирование возможно с помощью легко вычисляемых синдромов. Тем не менее, весь процесс декодирования остаётся трудоёмким.

3.4 Циклические коды

Определение и построение циклических кодов

Определение 3.4. Код C называется *циклическим (сдвиговым)*, если он инвариантен относительно циклических сдвигов, т. е. для любого $0 \leqslant s \leqslant n-1$ справедливо

$$(\alpha_0, \ldots, \alpha_{n-1}) \in C \Rightarrow \\ \Rightarrow (\alpha_s, \alpha_{s+1}, \ldots, \alpha_{n-1}, \alpha_0, \ldots, \alpha_{s-1}) \in C.$$

Ранее было показано:

- В кольце $R = \mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как n-мерное векторное пространство над полем $\mathbb{F}_p$, имеется базис
$$\left\{ \overline{1}, \overline{x}, \ldots, \overline{x^{n-1}} \right\}.$$
Циклический сдвиг координат в этом базисе равносилен умножению на $\overline{x}$.
- Векторное подпространство I кольца R является циклическим iff I — идеал R.
- R — КГИ, любой идеал порождается некоторым полиномом-элементом R.

Поэтому построить циклический (n, k)-код длины можно следующим образом.

1. Выбираем любой делитель $g(x)$ бинома $x^n - 1$. Многочлен $g(x)$ называют *порождающим* или *образующим*.
2. Найденный полином порождает идеал $(g(x))$ в кольце $R = \mathbb{F}_p[x]/(x^n - 1)$, а *коэффициенты многочленов из этого идеала* будут кодовыми словами. Тогда $m = \deg g(x)$ и $k = n - m$.
3. При удачном выборе порождающего полинома будут получен код с приемлемым значением d.

Однако:

- есть только несколько конструкций циклических кодов с хорошими параметрами;
- определение кодового расстояния циклического кода в общем случае является чрезвычайно трудоёмкой задачей.

Избыточный циклический код — англ. CRC, Cyclic Redundancy Code. Из всех *линейных* (n, k)-кодов будем далее рассматривать *циклические*.

Полиномиальное представление слов. Установим соответствие векторов сообщения $\boldsymbol{u} \in \{0,1\}^k$ и кодового слова $\boldsymbol{v} \in \{0,1\}^n$ с их полиномиальными представлениями $u(x)$, $v(x) \in \mathbb{F}_2[x]$:

$$\boldsymbol{u} = [\, u_0,\, u_1,\, \ldots,\, u_{k-1} \,]^T \;\leftrightarrow$$
$$\leftrightarrow\; u(x) = u_0 + u_1 x + \ldots + u_{k-1} x^{k-1},$$

$$\boldsymbol{v} = [\, v_0,\, v_1,\, \ldots,\, v_{n-1} \,]^T \;\leftrightarrow$$
$$\leftrightarrow\; v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}.$$

Любое кодовое слово $v(x)$ есть элемент

$$(g(x)) \;=\; \{\, g(x)q(x) \mid q(x) \in \mathbb{F}_2[x],\; x^n = 1 \,\}\,.$$

Замечание. Представление сообщений и кодовых слов в виде многочлена изоморфно их представлению как элементов линейного векторного пространства. При этом, операции с коэффициентами многочленов производятся по привычным правилам арифметики по $\bmod 2$, а степени переменной x используются только для обозначения места соответствующей компоненты вектора и никакой иной смысловой нагрузки не несут.

Код, представленный порождающим полиномом называется *полиномиальным*.

Коды Хэмминга могут быть циклическими. Построенная *Примере* 3.2 таблица 4×7 для кода Хэмминга *не порождает циклического кода.*

Однако если переставить 3-элементные окончания некоторых строк, то полученная таблица

1	0	0	0	1	1	0
0	1	0	0	0	1	1
0	0	1	0	1	1	1
0	0	0	1	1	0	1

уже *порождает циклический код* (проверьте!).

Пример 3.6 (построения циклического кода). Построим циклический код длины $n = 23$.

Для определения порождающего полинома кода находим разложение бинома $x^{23} - 1$ на неприводимые многочлены:

$$f(x) = (x+1)(\underbrace{x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1}_{f_1(x)}) \times \\ \times (\underbrace{x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1}_{f_2(x)}).$$

Поскольку $\deg f_1(x) = \deg f_2(x) = 11 = m$, любой из полиномов $f_1(x)$, $f_2(x)$ может быть выбран порождающим[5] для построения $(23, 12)$-кода.

Можно показать, что в обоих случаях кодовое расстояние оказывается равным 7. Например, при выборе порождающим полинома $g(x) = f_2(x)$ и несистематическом кодировании сообщения $[100000000000]^T$ получаем кодовое слово $[10101110001100000000000]^T$ веса 7.

Ясно, что построен *код Голея*.

Кодирование циклическими кодами. Пусть определён порождающий полином $g(x)$, делящий бином $x^n - 1$, $\deg g(x) = m < n$, задающий код C.

Несистематическое кодирование осуществляется путём умножения кодируемого полинома на порождаю-

[5] При выборе $g(x) = x+1$ получим код с проверкой на чётность ($m = 1$), при $g(x) = (x+1)f_1(x)$ или $g(x) = (x+1)f_2(x)$ получим *расширенный* код Голея с $m = 12$.

щий:

$$u(x) \mapsto v(x) = g(x)u(x).$$

Столбцы соответствующей порождающей матрицы — базисные векторы кода — соответствуют полиномам $x^i g(x),\ i = \overline{0, k-1}$.

Систематическое (разделимое) кодирование осуществляется приписыванием к кодовому слову *слева (в младшие разряды)* остатка $r(x)$ от деления $x^m u(x)$ на $g(x)$.

Действительно, умножение $u(x)$ на x^m помещает сообщение в старшие разряды n-битного слова. Поделим $x^m u(x)$ на $g(x)$ с остатком:.

$$x^m u(x) = g(x)q(x) + r(x), \quad \deg r(x) < m$$

откуда

$$x^m u(x) + r(x) = g(x)q(x) \in C.$$

Это означает, что кодирование

$$u(x) \mapsto v(x) = x^m u(x) + r(x).$$

будет систематическим.

Столбцы соответствующей порождающей матрицы — базисные векторы кода — соответствуют полиномам

$$x^{m+i} + r_i(x), \quad \text{где } r_i(x) \equiv_{g(x)} x^{m+i},\ i = \overline{0, k-1}.$$

Пример 3.7. 1. Построим циклический код длины $n = 7$.

Сначала нужно найти какой-либо делитель бинома $x^7 - 1$, для чего необходимо разложить его на неприводимые множители.

Заметим, что $7 = 2^3 - 1$. Но $F = \mathbb{F}_2^3$ — поле разложения бинома $x^{2^3-1} - 1$ и поэтому его корнями являются все ненулевые элементы поля F.

Делаем вывод: *выбор длины кода* $n = 2^q - 1$ *очень удобен*, т. к. легко определяются число и степени неприводимых делителей бинома $x^n - 1 = x^{2^q-1} - 1$.

Пусть α — произвольный примитивный элемент поля $F = \mathbb{F}_2^3$. Тогда с учетом $\alpha^7 = 1$ находим разбиение корней $x^7 - 1$ (= всех элементов F^*) на орбиты:

$$\{1\},\ \{\alpha, \alpha^2, \alpha^4\},\ \{\alpha^3, \alpha^6, \alpha^5\}.$$

Таким образом, многочлен x^7+1 имеет один неприводимый делитель 1-й степени и два неприводимых делителя 3-й степени (их вообще всего два).

В результате получаем разложение

$$x^7 - 1 = x^7 + 1 = (x+1) \cdot \underbrace{(x^3 + x + 1)}_{g(x)} \cdot (x^3 + x^2 + 1).$$

В качестве порождающего полинома $g(x)$ можно выбрать любой из вышеуказанных полиномов 3-й степени. Тогда $m = 3$, $k = 4$ и будет построен *циклический* $(7, 4)$-*код*[6]. Выберем конкретно $g(x) = x^3 + x + 1$.

2. Закодируем несистематическим и систематическим кодами сообщение

$$\boldsymbol{u} = [0\ 0\ 1\ 1]^T \leftrightarrow u(x) = x^3 + x^2.$$

[6] Ясно, это код Хэмминга!

Несистематическое кодирование.

$$v(x) = u(x)g(x) = (x^3+x^2)(x^3+x+1) = \\ = x^6+x^5+x^4+x^2 \leftrightarrow [0\,0\,1\,0\,1\,1\,1]^T = \boldsymbol{v}.$$

Систематическое кодирование.
Находим остаток $r(x)$ от деления многочлена $x^3u(x)$ на $g(x)$:

$$x^3(x^3+x^2) = x^6+x^5 = (x^3+x^2+x)(x^3+x+1)+x,$$

поэтому

$$v(x) = x^3u(x)+r(x) = x^6+x^5+x \leftrightarrow [0\,1\,0\,\underbrace{0\,0\,1\,1}_{\boldsymbol{u}}]^T = \boldsymbol{v}.$$

Декодирование циклических кодов

Определение 3.5. *Синдромом $s(x)$ полинома $w(x)$*, принятого при передаче сообщения закодированного циклическим кодом и, возможно, содержащего ошибки, назовём *остаток от деления $w(x)$ на порождающий код многочлен $g(x)$.*

Определение синдрома для циклического кода, очевидно, есть перефразировка в терминах полиномов определения синдрома для линейных кодов.

Свойства синдрома-полинома $w(x)$:

- $0 \leqslant \deg s(x) < m = n-k$;
- $s(x) \equiv 0 \Leftrightarrow w(x)$ — кодовое слово;
- $s(x) \equiv_{g(x)} w(x) \equiv_{g(x)} (v(x)+e(x)) \equiv_{g(x)} e(x)$.

Декодирование циклического кода проходит по общей схеме декодирования линейного кода:

1) *вычисляется синдром* $s(x)$ принятого слова $w(x)$;
2) вычисляются полиномы $e(x) = s(x) + g(x)u(x)$ для всех 2^k возможных сообщений $u(x)$.
3) определяется *полином ошибок* $e_0(x)$ как полином с минимальным числом мономов.
4) восстанавливается *переданное сообщение* $u(x) = w(x) + e_0(x)$.

Примеры декодирования циклических кодов будут даны при рассмотрении БЧХ-кодов[7].

Циклические линейные коды (n, k): резюме

- Линейный код будет циклическим, только если он *принадлежит идеалу* $(g(x))$ в кольце многочленов $\mathbb{F}_2[x]/(x^n - 1)$.

  Порождающий полином $g(x)$ циклического (n, k)-кода является делителем бинома $x^n - 1$; $\deg g(x) = m$ — число проверочных бит кода.

  Можно выбрать любой делитель, однако нахождение полинома $g(x)$, порождающего код с большим кодовым расстоянием d — *сложная задача*.

[7] Существуют и альтернативные методы декодирования циклических кодов общего вида (декодеры Меггита, Касами-Рудольфа, пороговый, мажоритарный, ...) также экспоненциальной по k трудоёмкости.

- *Циклические коды* общего вида могут иметь произвольную длину, но, в отличие от линейных кодов общего вида, его параметр k уже не произволен, что является существенным ограничением.

- *Кодирование* и *декодирование* сводится к выполнению операций умножения и деления полиномов, *легко реализуемые* на регистрах сдвига с обратными связями.

  Однако алгоритмы декодирования по-прежнему имеют *экспоненциальную сложность* по k.

3.5 Коды Боуза-Чоудхури-Хоквингема

Определение и основные свойства БЧХ-кодов. *Коды Боуза-Чоудхури-Хоквингема* (*БЧХ*, BCH) — подкласс циклических кодов, исправляющих *не менее заранее заданного* числа ошибок, предложены Р. Ч. Боузом и Д. К. Рей-Чоудхури в 1960 г. независимо от опубликованной на год ранее работы А. Хоквингема.

Основные свойства минимальных многочленов (напоминание):

1. $\forall\, \beta \in \mathbb{F}_p^n \;\; \exists !\, m_\beta(x)$, м.м. $m_\beta(x)$ неприводим и его степень $\leqslant n$;
2. если β — корень некоторого полинома $f(x) \in \mathbb{F}_p[x]$, то $m_\beta(x) \mid f(x)$;
3. м.м. примитивного элемента поля называется *примитивным многочленом*.

Циклотомический класс элемента поля

Определение 3.6 (для полей характеристики 2).
Пусть $n \mid N$. *Циклотомическим классом* (или *классом сопряжённости*) элемента α поля $\mathbb{F}_2^N$ над своим подполем $\mathbb{F}_2^n$ называется множество всех различных элементов $\mathbb{F}_2^N$, являющихся 2^n-ми степенями α: $\alpha^{2^{nt}}$, $t = 0, 1, \ldots$.

Свойства циклотомических классов.

1. Циклотомические классы различных элементов либо совпадают, либо не пересекаются $\Rightarrow$ все они образуют *разбиение* данного поля и любой элемент поля принадлежит только одному циклотомическому классу.

2. Если α — *примитивный элемент* поля $\mathbb{F}_2^{qn}$, то его циклотомический класс над $\mathbb{F}_2^n$ *содержит ровно* q *элементов*, т. е. это класс
$$\left\{ \alpha,\, \alpha^{2^n},\, \alpha^{2^{2n}},\, \ldots,\, \alpha^{2^{(q-1)\cdot n}} \right\}.$$

3. Если α — примитивный элемент $\mathbb{F}_2^{qn}$, а циклотомический класс элемента α^k над $\mathbb{F}_2^n$ содержит s элементов, то полином
$$m_\beta(x) \;=\; \prod_{t=0}^{s-1} \left(x - \alpha^{k \cdot 2^t} \right)$$
является м.м. *для всех элементов, входящих в данный циклотомический класс.*

Рассматривают разбиения на циклотомические классы мультипликативные группы полей.

Пример 3.8. Приведём примеры разложения *мультипликативных групп* полей $\mathbb{F}_2^{qn}$ на циклотомические классы над своими подполями $\mathbb{F}_2^n$.

1. $n = 1,\ q = 3$, т. е. рассматриваются поля $\mathbb{F}_2$ и $\mathbb{F}_2^3 = F$. Пусть α — примитивный элемент F.

Тогда $\alpha^7 = 1$ и разложение F^* над $\mathbb{F}_2$ есть (каждый элемент данного циклотомического класса последовательно возводим в степень $2^n = 2$)

$$\{1\},\ \{\alpha,\ \alpha^2,\ \alpha^4\},\ \{\alpha^3,\ \alpha^6,\ \alpha^5\}.$$

2. $n = 2, q = 2$, рассматриваемые поля $\mathbb{F}_2^2$ и $\mathbb{F}_2^4 = F$, и пусть α — примитивный элемент F.

Тогда $\alpha^{15} = 1$ и разложение F^* над $\mathbb{F}_2^2$ есть (каждый элемент данного циклотомического класса последовательно возводим в степень $2^n = 4$)

$$\{1\},\ \{\alpha,\ \alpha^4\},\ \{\alpha^2,\ \alpha^8\},\ \{\alpha^3,\ \alpha^{12}\},\ \{\alpha^5\},$$
$$\{\alpha^{10}\},\ \{\alpha^6,\ \alpha^9\},\ \{\alpha^7,\ \alpha^{13}\},\ \{\alpha^{11},\ \alpha^{14}\}.$$

3. $n = 1, q = 4$, рассматриваемые поля — $\mathbb{F}_2$ и $\mathbb{F}_2^4 = F$, и пусть α — примитивный элемент F.

Тогда $\alpha^{15} = 1$ и разложение F^* над $\mathbb{F}_2$ есть

$$\{1\},\ \{\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8\},\ \{\alpha^3,\ \alpha^6,\ \alpha^{12},\ \alpha^{24} = \alpha^9\},$$
$$\{\alpha^5,\ \alpha^{10}\},\ \{\alpha^7,\ \alpha^{14},\ \alpha^{28} = \alpha^{13},\ \alpha^{26} = \alpha^{11}\}.$$

БЧХ-коды: определение (простейший случай) и основное свойство

Пусть выбраны параметр q, определяющий длину кода $n = 2^q - 1$ и *конструктивное расстояние* $d_c < n$. Далее рассматривается поле $\mathbb{F}_2^q$ разложения бинома

$x^n - 1$ и некоторый примитивный элемент α этого поля.

Код БЧХ есть циклический (n, k, d)-код, в котором делящий бином $x^n - 1$ порождающий многочлен $g(x)$ является полиномом минимальной степени, имеющим корнями *нули кода* α, α^2, α^3, ..., α^{d_c-1}.

Для построенного кода $\deg g(x) = m > d_c - 1$ (т. е. кроме указанных нулей кода $g(x)$ имеет и другие корни); $k = n - m$. При этом кодовое расстояние d оказывается не менее выбранного конструктивного расстояния d_c — *важнейшее свойство построенного БЧХ-кода.*

Коды БЧХ: синдромы. Поскольку все кодовые слова циклического кода C делятся на полином $g(x)$ с корнями α, α^2, ..., α^{d-1}, то эти корни — одновременно и корни любого кодового слова:

$$v(x) \in C \;\Leftrightarrow\; v(\alpha^i) = 0, \quad i = 1, \ldots, d-1.$$

Определение 3.7. *Синдромами полинома* $w(x)$, принятого при передаче сообщения, закодированного БЧХ-кодом с нулями α^i, $i = \overline{1, d-1}$ и, возможно, содержащего ошибки, назовём набор значений $w(x)$ в нулях кода: $s_i = w(\alpha^i)$.

Ясно, что определение синдрома для БЧХ-кода, очевидно, есть *перефразировка в терминах нулей кода полиномов* синдрома для циклического кода. Далее, поскольку

$$w(x) = v(x) + e(x), \quad \text{то} \quad s_i = w(\alpha^i) = e(\alpha^i),$$

то «*все синдромы равны нулю*» $\Leftrightarrow$ $w(x)$ — кодовое слово.

3.6 Построение БЧХ-кодов

Алгоритм построения БЧХ-кода. БЧХ (n, k)-код, как и любой циклический, задаётся порождающим полиномом $g(x)$ — делителем бинома $x^n - 1$, $\deg g(x) = m$, $k = n - m$.

Для построения кода БЧХ нужно:

1) задать величину q, определяющую длину кода $n = 2^q - 1$;
2) задать величину конструктивного расстояния $d_c = 2r + 1 < n$, если предполагается исправлять до r ошибок;
3) выбрав неприводимый полином $a(x) \in \mathbb{F}_2[x]$ степени q определить поле $\mathbb{F}_2^q = \mathbb{F}_2[x]/(a(x))$ его примитивный элемент α;
4) определить циклотомические классы элемента $\alpha \in \mathbb{F}_2^q$ над полем $\mathbb{F}_2$, в которые попадают нули кода α, α^2, ..., α^{d_c-1}; пусть таких классов h;
5) найти минимальные многочлены $g_1(x)$, ..., $g_h(x)$ каждого циклотомического класса;
6) вычислить порождающий полином
$$g(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_h(x).$$

Пример 3.9 (построения кодов БЧХ). Выберем $q = 3$ и построим различные БЧХ-коды длины $n = 2^3 - 1 = 7$.

Для получения разложения бинома $x^7 - 1$ возьмём многочлен $a(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$, $\deg a(x) = q = 3$ и

образуем поле поле $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^3$. Поскольку многочлен $a(x)$ — примитивный, то элемент $\alpha = x$ примитивен и F^*, как показано ранее, разбивается на следующие циклотомические классы над $\mathbb{F}_2$:

$$\{1\},\ \{\alpha, \alpha^2, \alpha^4\},\ \{\alpha^3, \alpha^6, \alpha^5\}.$$

Для построения кодов, исправляющих заданное количество ошибок, необходимо определить соответствующий порождающий полином.

1. *Код БЧХ длины* $n = 7$, *исправляющий* $r = 1$ *ошибку* (код Хэмминга).

В этом случае $d_c - 1 = 2r = 2$ и нули кода α, α^2 попадают в *один* циклотомический класс.

Минимальный многочлен для обоих элементов этого класса — $a(x)$, поэтому порождающий полином $g(x) = a(x)$, $m = \deg g(x) = 3$ и в результате получаем уже известный $(7, 4, 3)$-код Хэмминга.

2. *Код БЧХ длины* $n = 7$, *исправляющий не менее* $r = 2$ *ошибок.*

Теперь $d_c - 1 = 2r = 4$. Нули строящегося кода α, α^2, α^3, α^4 входят в *два* циклотомических класса: $\{\alpha, \alpha^2, \alpha^4\}$ и $\{\alpha^3, \alpha^6, \alpha^5\}$, порождаемых α и α^3 соответственно, поэтому

$$g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x),$$

где $g_\alpha(x)$ и $g_{\alpha^3}(x)$ — м.м. для α и α^3.

М.м. для α известен: $g_\alpha(x) = a(x) = x^3 + x + 1$.

Найдем м.м. для $\alpha^3 = \alpha + 1$:

$$g_{\alpha^3}(x) = \left(x - \alpha^3\right)\left(x - \alpha^5\right)\left(x - \alpha^6\right) =$$

$$= x^3 + \left(\alpha^3 + \alpha^5 + \alpha^6\right) x^2 + \left(\alpha^8 + \alpha^9 + \alpha^{11}\right) x + \alpha^{14}.$$

Вычислим коэффициенты полинома $g_{\alpha^3}(x)$ с учётом $\alpha^7 = 1$ и $\alpha^3 = \alpha + 1$:

$$\begin{aligned}
\alpha^3 + \alpha^5 + \alpha^6 &= (\alpha+1) + \alpha^2(\alpha+1) + (\alpha+1)^2 = \\
&= \alpha + 1 + \alpha^3 + \alpha^2 + \alpha^2 + 1 = 1\,, \\
\alpha^8 + \alpha^9 + \alpha^{11} &= \alpha^2 + \alpha + \alpha^4 = \alpha^2 + \alpha + \alpha(\alpha+1) = 0\,, \\
\alpha^{14} &= 1\,.
\end{aligned}$$

Таким образом $g_{\alpha^3}(x) = x^3 + x^2 + 1$ (что можно было определить сразу: это второй из двух неприводимых многочленов степени 3) и

$$\begin{aligned}
g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x) &= (x^3 + x + 1)(x^3 + x^2 + 1) = \\
&= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

Получаем $\deg g(x) = m = 6$ и $k = 7 - 6 = 1$, т. е. построен тривиальный код с 7-кратным повторением, исправляющий 3 ошибки и содержащий всего два кодовых слова: $[0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ и $[1\ 1\ 1\ 1\ 1\ 1\ 1]^T$.

Хотя код и исправляет больше ошибок, чем планировалось, его скорость $R = 1/7$ чрезвычайно мала.

Пример 3.10. Попытаемся построить лучший код для исправления 2-х ошибок, взяв бóльшую его длину: выберем $q = 4$, т. е. длина кода будет $n = 2^q - 1 = 15$.

Для получения разложения бинома $x^{15} - 1$ рассмотрим поле $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^4$, $\deg a(x) = q = 4$. Тогда F^* разбивается на следующие циклотомические классы над $\mathbb{F}_2$ относительно примитивного элемента α:

$$\{1\},\ \left\{\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8\right\},\ \left\{\alpha^3,\ \alpha^6,\ \alpha^{12},\ \alpha^9\right\},$$
$$\left\{\alpha^5,\ \alpha^{10}\right\},\ \left\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\right\}.$$

Конкретно в качестве порождающего многочлена возьмём примитивный многочлен

$$a(x) = x^4 + x + 1,$$

который является м.м. для примитивного элемента $\alpha = x$ и всего класса $\left\{\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8\right\}$.

1. *Код БЧХ длины* $n = 15$, *исправляющий* $r = 2$ *ошибки.*

В этом случае $d_c - 1 = 2r = 4$ и нули α, α^2, α^3, α^4 конструируемого кода располагаются в двух циклотомических классах — для элементов α и α^3.

М.м. для (всех) элементов этих классов:

первого (α): $g_\alpha(x) = a(x)$.

второго (α^3): $g_{\alpha^3}(x) =$

$$= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = \ldots$$
$$\ldots = x^4 + x^3 + x^2 + x + 1.$$

Тогда порождающий полином кода есть

$$g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x) = x^8 + x^7 + x^6 + x^4 + 1.$$

Получено $m = 8$, $k = 7$ и, как можно показать, $d = d_c = 5$, т. е. построен БЧХ $(15, 7, 5)$-код со скоростью уже $R = 7/15 > 1/7$.

Построим теперь

2. *Код БЧХ длины* $n = 15$, *исправляющий* $r = 3$ *ошибки.*

Теперь нужно найти полином, являющийся м.м. для нулей α, α^2, ..., α^6, которые попадают в 3 циклотомических класса:

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}, \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}, \{\alpha^5, \alpha^{10}\}$$

(имеются ещё по одному 1- и 4-х элементному классу).

Пусть поле разложения бинома $x^{15}-1$ то же, тогда м.м. для α и α^3 уже найдены.

Очевидно $g_{\alpha^5}(x) = x^2+x+1$ (единственный неприводимый квадратный полином над $\mathbb{F}_2$) и порождающий полином полученного кода есть

$$g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x) \cdot g_{\alpha^5}(x) = \\ = x^{10}+x^8+x^5+x^4+x^2+x+1.$$

Получено $m = 10$, $k = 5$ и можно показать, что $d = d_c = 7$.

Этот $(15, 5, 7)$-код БЧХ при той же длине, что и предыдущий, исправляет больше ошибок, но имеет меньшую скорость $R = 1/3$.

Декодирование кодов БЧХ

Декодирование кода Хэмминга как линейного кода с помощью проверочной матрицы и вычисляемого с её помощью вектора-синдрома было уже рассмотрено в Разделе 3.3. Опишем ещё один метод декодирования кодов Хэмминга как простейших кодов БЧХ.

В этом случае $d = 3$, и поэтому нулями кода являются α и α^2, где α — примитивный элемент поля $\mathbb{F}_2^n$, $n = 2^q - 1$.

Для декодирования принятого слова $w(x)$ вычисляем синдром $s_1 = w(\alpha)$ (синдром $s_2 = w(\alpha^2)$ нам не потребуется).

- При $s = 0$ считаем, что ошибок не произошло.
- Если $s \not\equiv 0$, то определяем значение j, для которого α^j и считаем, что произошла единичная ошибка в j-м разряде для $j = 0, 1, \ldots, n-1$.

Пример 3.11 (декодирование кода Хэмминга). Рассматриваем $(7,4)$-код Хэмминга, построенный в *Примере* 3.7 для циклических кодов.

Там был выбран порождающий полином $g(x) = x^3 + x + 1$ и найдено систематическое кодирование $v(x)$ сообщения $u(x) = x^3 + x^2 \leftrightarrow [0\ 0\ 1\ 1]^T$:

$$v(x) = x^6 + x^5 + x \leftrightarrow [0\ 1\ 0\ \underline{0\ 0\ 1\ 1}]^T.$$

Пусть при передаче сообщения $u(x)$ произошла ошибка в 5-й позиции, т. е. принято слово

$$[0\ 1\ 0\ 0\ 0\ 0\ 1]^T \leftrightarrow w(x) = x^6 + x\,.$$

Для декодирования $w(x)$ найдем синдром, учитывая, что $\alpha^3 = \alpha + 1$ и $\alpha^7 = 1$:

$$s = w(\alpha) = \alpha^6 + \alpha = \left(\alpha^3\right)^2 + \alpha = (\alpha+1)^2 + \alpha = \\ = \alpha^2 + \alpha + 1 \neq 0\,.$$

Определим теперь значение $j \in \{0, \ldots, 6\}$, для которого $\alpha^j = s$:

$$\alpha^0 = 1, \qquad \alpha^3 = \alpha + 1,$$
$$\alpha^1 = \alpha, \qquad \alpha^4 = \alpha(\alpha+1) = \alpha^2 + \alpha,$$
$$\alpha^2 = \alpha^2, \qquad \alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 = s.$$

Т.о. 5-я позиция ошибки определена верно. Другой способ нахождения позиции ошибки кода Хэмминга см. в Задаче 3.3 на с. 167.

Декодирование кодов БЧХ в общем случае.

Рассмотрим (n, k, d)-код БЧХ длины $n = 2^q - 1$ при построении которого для определения порождающего полинома использовалось поле $F = \mathbb{F}_2^q = \mathbb{F}_2[x]/(a(x))$, $\deg a(x) = q$ и α — нуль кода.

Пусть при передаче кодового слова произошло $\nu \leqslant r = \lfloor (d-1)/2 \rfloor$ ошибок в позициях $j_1, \ldots, j_\nu$. Тогда

$$e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}.$$

Отметим, что ни само ν, ни значения $j_1, \ldots, j_\nu$ неизвеастны.

Вычислим синдромы принятого полинома $w(x)$: $s_i = w(\alpha^i) = e(\alpha^i)$, $i = \overline{1, 2r}$. Если не все они равны 0 (т.е. $1 \leqslant r$), запишем их значения через степени примитивного элемента α:

$$\begin{cases} s_1 = \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_\nu}, \\ s_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_\nu})^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = (\alpha^{j_1})^{2r} + \ldots + (\alpha^{j_\nu})^{2r}. \end{cases}$$

Значения $\nu, j_1, \ldots, j_\nu$, удовлетворяющие данной системе, определят число и позиции ошибок[8].

Введём обозначения $\beta_i = \alpha^{j_i}$, $i = 1, \ldots, \nu$; эти величины называют *локаторами ошибок*.

Перепишем систему:

[8] Такое решение всегда существует и единственно, т. к. код по построению способен исправлять до r ошибок.

$$\begin{cases} s_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ s_2 = \beta_1^2 + \beta_2^2 + \ldots + \beta_\nu^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = \beta_1^{2r} + \beta_2^{2r} + \ldots + \beta_\nu^{2r}. \end{cases}$$

Определим *полином локаторов ошибок*

$$\sigma(x) = \prod_{i=1}^{\nu}(1 + \beta_i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_\nu x^\nu,$$

считая формально $\sigma_0 = 1$ и $\sigma_i = 0$ при $i > \nu$. Корнями этого полинома будут величины $\beta_i^{-1} = \alpha^{-j_i},\ i = \overline{1, \nu}$.

Связь между коэффициентами полинома локаторов ошибок и самими локаторами определяет теорема Виета:

$$\begin{cases} \sigma_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ \sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3 + \ldots + \beta_{\nu-1}\beta_\nu, \\ \sigma_3 = \sum\limits_{i_1<i_2<i_3} \beta_{i_1}\beta_{i_2}\beta_{i_3}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_\nu = \beta_1\beta_2\ldots\beta_\nu. \end{cases}$$

Введённые системы задают величины синдромов и коэффициентов полинома локаторов ошибок как значения *симметрических полиномов*: первая — суммы k-х степеней и вторая — элементарных.

Соотношения между этими двумя типами симметрических полиномов задаются *тождествами Ньютона-Жирара*, которые в двоичной арифметике записываются как

$$
\begin{aligned}
&s_1 + \sigma_1 = 0,\\
&s_2 + \sigma_1 s_1 + 2\sigma_2 = 0,\\
&s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&s_\nu + \sigma_1 s_{\nu-1} + \ldots + \sigma_{\nu-1} s_1 + \nu\sigma_\nu = 0,\\
&s_{\nu+1} + \sigma_1 s_\nu + \ldots + \sigma_{\nu-1} s_2 + \sigma_\nu s_1 = 0,\\
&s_{\nu+2} + \sigma_1 s_{\nu+1} + \ldots + \sigma_{\nu-1} s_3 + \sigma_\nu s_2 = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&s_{2r} + \sigma_1 s_{2r-1} + \ldots + \sigma_{\nu-1} s_{2r-\nu+1} + \sigma_\nu s_{2r-\nu} = 0.
\end{aligned}
\qquad (*)
$$

Последние $2r - \nu$ равенств данной системы могут быть записаны как СЛАУ относительно $\sigma_1, \ldots, \sigma_\nu$. Стандартными методами эта система не может быть решена, поскольку *значение ν неизвестно.*

Алгоритмы решения системы $(*)$ называют *декодерами.* Например, *декодер PGZ (Peterson-Gorenstein-Zierler, Перерсона-Горенштейна-Цирлера)* состоит в последовательных попытках решения данных соотношений для $\nu = r, r-1, \ldots$ до тех пор, пока матрица очередной СЛАУ не окажется невырожденной.

Далее рассмотрен декодер на основе расширенного алгоритма Евклида.

В результате работы декодера находят полином локаторов ошибок $\sigma(x)$; при этом, ясно, число произошедших ошибок $\nu = \deg \sigma(x)$.

После нахождения $\sigma(x)$ можно, например, перебо-

ром[9], отыскать все ν его корней α^{-j_i}, а по ним — позиции ошибок $j_1, \ldots, j_\nu$.

Алгоритм декодирования (n, k, d)*-кода БЧХ*
Пусть $n = 2^q - 1$ и $\alpha \in \mathbb{F}_2^q = F$ — нуль кода, т. е. примитивный элемент поля $F = \mathbb{F}_2[x]/(a(x))$, $\deg a(x) = q$ и принято слово $w(x)$.

1. Найти все синдромы $s_i = w(\alpha^i)$, $i = \overline{1, d-1}$; если все они равны 0, то, считаем, что ошибок нет, в противном случае — переход к следующему пункту.
2. Найти полином локаторов ошибок $\sigma(x)$, используя тот или иной декодер; число произошедших ошибок $\nu = \deg \sigma(x)$.
3. Найти все корни $\sigma(x)$ перебором элементов F^*; пусть эти корни суть $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$.
4. Найти *позиции ошибок* $j_i \equiv_n -k_i$, $i = \overline{1, \nu}$.
5. Исправить ошибки, инвертировав позиции j_i, $i = \overline{1, \nu}$ в $w(x)$, получив кодовое слово $v(x) = w(x) + x^{j_1} + \ldots + x^{j_\nu}$.
6. По кодовому слову $v(x)$ восстановить переданное сообщение $u(x)$ (в случае систематического кодирования — тривиальная процедура).

Опишем *декодер на основе расширенного алгоритма Евклида*, который будем далее использовать.

Введём вспомогательный *синдромный полином*

[9] т.н. *процедура Ченя*

$$s(x) = 1 + s_1 x + s_2 x^2 + \ldots + s_{2r} x^{2r},$$

где s_i, $i = \overline{1, 2r}$ — синдромы и, формально, $s_0 = 1$. Заметим, что это полностью определённый полином с коэффициентами из F.

Если перемножить полиномы — синдромный и локаторов ошибок — получим *полином значений ошибок*:

$$s(x)\sigma(x) = 1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{2r+\nu} x^{2r+\nu}.$$

Коэффициенты этого полинома определяются соотношением для произведения многочленов —

$$\lambda_i = \sum_{j=0}^{i} \sigma_j s_{i-j}, \quad i = \overline{1, 2r+\nu}.$$

Замечаем, что значения λ_i по данной формуле для $i = \nu + 1, \ldots, 2r$ суть левые части соотношений $(*)$, т. е. все они равны 0.

Значит, полином значений ошибок имеет нулевую «среднюю часть». Обозначим его начальную часть $\lambda(x)$, а из заключительной части вынесем за скобку x^{2r+1}:

$$s(x)\sigma(x) = \underbrace{1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_\nu x^\nu}_{\lambda(x)} + \\ + x^{2r+1}\left(\lambda_{2r+1} + \ldots + \lambda_{2r+\nu} x^{\nu-1}\right), \quad 1 \leqslant \nu \leqslant r.$$

Это означает, что $s(x)\sigma(x)$ при делении на x^{2r+1} даст в остатке $\lambda(x)$, т. е.

$$s(x)\sigma(x) \equiv_{x^{2r+1}} \lambda(x).$$

Данное соотношение называют *ключевым уравнением*.

Очевидно, ключевое уравнение в поле $\mathbb{F}_2[x]/(a(x))$ может быть записано в виде соотношения Безу

$$s(x)\sigma(x) + x^{2r+1}a(x) \;=\; \lambda(x),$$

которое может быть решено относительно $\sigma(x)$ расширенным алгоритмом Евклида. При этом:

- не требуется знать многочлен $\lambda(x)$;
- условие остановки — степень очередного полученного остатка $\leqslant r$.

Пример 3.12 (декодирования БЧХ-кода).

Рассмотрим БЧХ $(15, 5, 7)$-код, т. е. $q = 4$ и $n = 15$, исправляющий до $r = 3$ ошибок.

Пусть при построении кода в качестве поля разложения бинома $x^{15} - 1$ использовалось поле $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/\big(x^4 + x + 1\big) = F$ и α — нуль кода.

Пусть также передаётся сообщение

$$[0\ 1\ 1\ 0\ 1]^T \;\leftrightarrow\; u(x) \;=\; x^4 + x^2 + x\,.$$

При систематическом кодировании (опустим этот этап) кодовое слово есть

$$v(x) \;=\; x^{14} + x^{12} + x^{11} + x^8 + x^4 + x^3 + x^2 + x \;\leftrightarrow$$
$$\leftrightarrow\; [0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ \underline{0\ 1\ 1\ 0\ 1}]^T.$$

Пусть ошибки произошли в 0, 6 и 12-й позициях, т. е. принятое слово —

$$w(x) \;=\; x^{14} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \;\leftrightarrow$$
$$\leftrightarrow\; [\underline{1}\ 1\ 1\ 1\ 1\ 0\ \underline{1}\ 0\ 1\ 0\ 0\ 1\ \underline{0}\ 0\ 1]^T.$$

Для дальнейших вычислений нам понадобится представление ненулевых элементов поля $\mathbb{F}_2[x]/\left(x^4+x+1\right)$ как степеней его генератора α (что уже сделано в таблице со с. 66):

α^1	α
α^2	α^2
α^3	α^3
α^4	$\alpha+1$
α^5	$\alpha^2+\alpha$
α^6	$\alpha^3+\alpha^2$
α^7	$\alpha^3+\alpha+1$
α^8	α^2+1
α^9	$\alpha^3+\alpha$
α^{10}	$\alpha^2+\alpha+1$
α^{11}	$\alpha^3+\alpha^2+\alpha$
α^{12}	$\alpha^3+\alpha^2+\alpha+1$
α^{13}	$\alpha^3+\alpha^2+1$
α^{14}	α^3+1
α^{15}	1

1. Поскольку $d-1=2r=6$, найдём все 6 синдромов для принятого слова:

$$
\begin{aligned}
s_1 &= w(\alpha) = \\
&= (\alpha^3+1)+(\alpha^3+\alpha^2+\alpha)+(\alpha^2+1)+(\alpha^3+\alpha^2)+ \\
&+(\alpha+1)+\alpha^3+\alpha^2+\alpha+1 = \alpha, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = s_1^2 = \alpha^2, \\
s_3 &= w(\alpha^3) = \underbrace{\alpha^{42}}_{\alpha^{12}}+\underbrace{\alpha^{33}}_{\alpha^3}+\underbrace{\alpha^{24}}_{\alpha^9}+\underbrace{\alpha^{18}}_{\alpha^3}+\alpha^{12}+\alpha^9+ \\
&+\alpha^6+\alpha^3+1 = \alpha^3+\alpha^6+1 = \cancel{\alpha^3}+\alpha^2+\cancel{\alpha^3}+1 =
\end{aligned}
$$

$$
\begin{aligned}
&= \alpha^2 + 1 = \alpha^8,\\
s_4 &= w(\alpha^4) = s_1^4 = \alpha^4,\\
s_5 &= w(\alpha^5) = \alpha^{70} + \alpha^{55} + \alpha^{40} + \alpha^{30} + \alpha^{20} + \alpha^{15} +\\
&+ \alpha^{10} + \alpha^5 + 1 =\\
&= \alpha^{10} + \alpha^{10} + \alpha^{10} + 1 + \alpha^5 + 1 + \alpha^{10} + \alpha^5 + 1 = 1,\\
s_6 &= w(\alpha^6) = s_3^2 = \alpha^{16} = \alpha.
\end{aligned}
$$

Таким образом, синдромный полином есть

$$s(x) = \alpha x^6 + x^5 + \alpha^4 x^4 + \alpha^8 x^3 + \alpha^2 x^2 + \alpha x + 1.$$

2. По декодеру на базе расширенного алгоритма Евклида, зная $a(x)$ и $s(x)$, решаем относительно $\sigma(x)$ соотношение Безу

$$x^7 a(x) + s(x)\sigma(x) = \lambda(x).$$

Шаг 0. // *Инициализация*

$$
\begin{aligned}
&r_{-2}(x) = x^7,\\
&r_{-1}(x) = s(x) = \alpha x^6 + x^5 + \alpha^4 x^4 + \alpha^8 x^3 +\\
&\qquad\qquad + \alpha^2 x^2 + \alpha x + 1,\\
&\sigma_{-2}(x) = 0, \quad \sigma_{-1}(x) = 1.
\end{aligned}
$$

Шаг 1. // *Делим с остатком $r_{-2}(x)$ на $r_{-1}(x)$*

$$
\begin{aligned}
&r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),\\
&q_0(x) = \alpha^{14} x + \alpha^{13},\\
&r_0(x) = \alpha^8 x^5 + \alpha^{12} x^4 + \alpha^{11} x^3 + \alpha^{13},\\
&\qquad \deg r_0(x) = 5 > 3 = r,\\
&\sigma_0(x) = \sigma_{-2}(x) + \sigma_{-1}(x)q_0(x) =\\
&\qquad = q_0(x) = \alpha^{14} x + \alpha^{13}.
\end{aligned}
$$

Шаг 2. // *Делим с остатком* $r_{-1}(x)$ *на* $r_{=0}(x)$

$$\begin{aligned} r_{-1}(x) &= r_0(x)q_1(x) + r_1(x),\\ q_1(x) &= \alpha^8 x + \alpha^2,\\ r_1(x) &= \alpha^{14}x^4 + \alpha^3 x^3 + \alpha^2 x^2 + \alpha^{11}x,\\ &\deg r_1(x) = 4 > 3 = r,\\ \sigma_1(x) &= \sigma_{-1}(x) + \sigma_0(x)q_1(x) =\\ &= \alpha^7 x^2 + \alpha^{11}x. \end{aligned}$$

Шаг 3. // *Делим с остатком* $r_{=0}(x)$ *на* $r_1(x)$

$$\begin{aligned} r_0(x) &= r_1(x)q_2(x) + r_2(x),\\ q_2(x) &= \alpha^9 x,\\ r_2(x) &= \alpha^5 x + \alpha^{13},\\ &\deg r_2(x) = 1 \leqslant 3 = r,\\ \sigma_2(x) &= \sigma_0(x) + \sigma_1(x)q_2(x) =\\ &= \alpha x^3 + \alpha^5 x^2 + \alpha^{14}x + \alpha^{13} = \sigma(x). \end{aligned}$$

Это последний шаг алгоритма Евклида, т. к. степень остатка $r_2(x)$ не превосходит r.

Таким образом, полином локаторов ошибок найден:

$$\sigma(x) = \alpha x^3 + \alpha^5 x^2 + \alpha^{14}x + \alpha^{13}.$$

и $\nu = \deg\sigma(x) = 3$.

3. Найдём корни $\sigma(x)$ перебором элементов F^*, используя построенную ранее таблицу степеней α:

$$\begin{aligned} \sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 + \alpha^{13} = \alpha^2,\\ \sigma(\alpha^2) &= \alpha^7 + \alpha^9 + \alpha + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha,\\ \sigma(\alpha^3) &= \alpha^{10} + \alpha^{11} + \alpha^2 + \alpha^{13} = \mathbf{0},\\ \sigma(\alpha^4) &= \alpha^{13} + \alpha^{13} + \alpha^3 + \alpha^{13} = \alpha^2 + 1,\\ \sigma(\alpha^5) &= \alpha + 1 + \alpha^4 + \alpha^{13} = \alpha^{13}, \end{aligned}$$

$$\sigma(\alpha^6) = \alpha^4 + \alpha^2 + \alpha^5 + \alpha^{13} = \alpha^3 + \alpha^2,$$
$$\sigma(\alpha^7) = \alpha^7 + \alpha^4 + \alpha^6 + \alpha^{13} = \alpha^3 + 1,$$
$$\sigma(\alpha^8) = \alpha^{10} + \alpha^6 + \alpha^7 + \alpha^{13} = \alpha^3 + \alpha^2 + 1,$$
$$\sigma(\alpha^9) = \alpha^{13} + \alpha^8 + \alpha^8 + \alpha^{13} = \mathbf{0},$$
$$\sigma(\alpha^{10}) = \alpha + \alpha^{10} + \alpha^9 + \alpha^{13} = \alpha,$$
$$\sigma(\alpha^{11}) = \alpha^4 + \alpha^{12} + \alpha^{10} + \alpha^{13} = \alpha^2 + \alpha,$$
$$\sigma(\alpha^{12}) = \alpha^7 + \alpha^{14} + \alpha^{11} + \alpha^{13} = 1,$$
$$\sigma(\alpha^{13}) = \alpha^{10} + \alpha + \alpha^{12} + \alpha^{13} = \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{14}) = \alpha^{13} + \alpha^3 + \alpha^{13} + \alpha^{13} = \alpha^2 + 1,$$

поскольку корней всего 3, то ясно, что $\sigma(\alpha^{15}) = 0$; действительно:

$$\sigma(\alpha^{15}) = \alpha + \alpha^5 + \alpha^{14} + \alpha^{13} = \mathbf{0}.$$

4. По найденным корням α^3, α^9, α^{15} вычисляем позиции ошибок:

$$j_1 = -3 \equiv_{15} 12,$$
$$j_2 = -9 \equiv_{15} 6,$$
$$j_3 = -15 \equiv_{15} 0.$$

5. Таким образом полином ошибок $e(x) = x^{12} + x^6 + 1$ определён и переданное кодовое слово есть

$$v(x) = w(x) + e(x) \leftrightarrow [0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ \underline{0\ 1\ 1\ 0\ 1}]^T.$$

Справка. В системах передачи данных широко используется двоичный $(255, 231, 7)$-код БЧХ, у которого

- степень порождающего код многочлена $g(x)$ — $m = n - k = 24$;
- $q = 8$ и в общем количестве слов длины 255 доля кодовых — $2^{-24} \approx 17 \cdot 10^{-6}$;
- все шары радиуса 3 с центрами в кодовых словах занимают $\approx 16,5\%$ объёма куба B^{255}.

В течении многих лет не было случая, чтобы ошибка передачи прошла незамеченной.

БЧХ (n, k, d)-коды: резюме

- БЧХ-коды являются *подклассом циклических. Самое ценное их свойство* — возможность построения кода с кодовым расстоянием не меньше заданного.
- *Кодирование* осуществляется с помощью порождающего полинома, имеющего корнями степени некоторого примитивного элемента поля.
- *Декодирование* может быть проведено с помощью эффективных алгоритмов (Берлекэмпа-Мэсси, Питерсона-Горенстейна-Цирлера, Евклидов алгоритм, ...).
- При небольших n среди кодов БЧХ существуют хорошие коды, но, как правило, не лучшие из известных.
- Теоретически коды БЧХ могут исправлять *произвольное количество ошибок*, но при этом существенно увеличивается длина кодового слова n,

что приводит к уменьшению скорости передачи данных и усложнению приёмно-передающей аппаратуры; поэтому при больших длинах приходится использовать другие коды.

Помехоустойчивое кодирование применяется:

- для получения *надежной связи*, когда мощность принимаемого сигнала близка к мощности тепловых шумов. Например, циклические коды используются в мобильной связи в стандартах GSM и CDMA.
- для *защиты против шума, намеренно организованного противником* в военных приложениях;
- при передаче данных *в вычислительных системах*, которые чрезвычайно чувствительны к ошибкам.

  Типичное значение вероятности ошибки на бит без кодирования в вычислительных сетях составляет 10^{-6}. Использование простейших кодов с небольшой избыточностью позволяет понизить эту вероятность более, чем на 3 порядка.
- для защиты данных во внутренних и внешних ЗУ: ленты, SSD диски, flash-память — коды БЧХ, Хэмминга;
- при *синтезе отказоустойчивых дискретных устройств* (например, БИС);
- для получения *устойчивых признаков из биометрических характеристик* (сетчатка глаза, отпечатки пальцев, ...).

Для выбора минимальных многочленов при построении БЧХ-кодов *составлены специальные таблицы.*

Коррекция ошибок может требоваться не всегда: многие современные каналы связи обладают хорошими характеристиками, и принимающей стороне часто достаточно лишь проверить, успешно ли прошла передача и в случае наличия ошибок повторить её. Также при синтезе сбоеустойчивых ИМС часто требуется лишь зафиксировать наличие ошибки, которая исчезает при повторном вычислении. В этих случаях применяются коды специально предназначенные для *обнаружения ошибок (ED)*, а не для их исправления.

Вся математика делится на три раздела: небесная механика, гидродинамика и теория кодирования (*В. И. Арнольд*, академик РАН, один из крупнейших математиков XX века).

3.7 Задачи с решениями

Задача 3.1. *Для линейного кода, заданного своей проверочной матрицей*

$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

требуется

1) *построить порождающую матрицу G кода для систематического кодирования, при котором биты исходного сообщения переходят в последние биты кодового слова;*

2) *найти такое кодирование для сообщений*

$$\boldsymbol{u}_1 = [1\ 1\ 0\ 1]^T,\ \boldsymbol{u}_2 = [1\ 0\ 0\ 1]^T.$$

Решение. Проверочная матрица H имеет размерность 3×7, следовательно код при длине $n = 7$ содержит $m = 3$ проверочных и $k = 7 - 3 = 4$ информационных бит.

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_4 \end{bmatrix}$.

Матрицу P можно получить, если привести проверочную матрицу H к виду $\begin{bmatrix} I_3 & P \end{bmatrix}$, преобразуя *строки*:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{(1)\leftrightarrow(3)} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \rightarrow$$

$$\xrightarrow{(1)+(3)\mapsto(1)} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\boldsymbol{u}_1 = [1101]^T$, $\boldsymbol{u}_2 = [1001]^T$:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad [\boldsymbol{v}_1, \boldsymbol{v}_2] = G \times [\boldsymbol{u}_1, \boldsymbol{u}_2] = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

Очевидно был задан $(7, 4)$-код Хэмминга.

Задача 3.2. *Циклический* $(9, 3)$*-код задан своим порождающим полиномом*

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить его кодовое расстояние d*, а также осуществить систематическое кодирование полинома*

$$u(x) = x^2 + x \leftrightarrow [0\ 1\ 1]^T.$$

Решение. Для определения кодового расстояния найдём все кодовые слова:

$$v(x) = g(x)(ax^2+bx+c) = (x^6+x^3+1)(ax^2+bx+c) =$$
$$= ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c.$$

В векторном виде все кодовые слова представляются как

$$[\,a,\ b,\ c,\ a,\ b,\ c,\ a,\ b,\ c\,].$$

Очевидно, это тривиальный код 3-кратного повторения и $d = 3$.

Проводим систематическое кодирование сообщения $u(x)$:

$$u(x) \ \mapsto \ v(x) = x^6 u(x) + r(x),$$
$$x^6 u(x) \ = \ x^6(x^2 + x) \ = \ x^8 + x^7.$$

Находим остаток $\deg r(x)$ от деления $x^6 u(x)$ на $g(x)$:

$$\begin{array}{l|l} x^8 + x^7 & x^6 + x^3 + 1 \\ \hline x^8 \quad + x^5 \quad + x^2 & x^2 + x \\ \hline \quad x^7 + x^5 \quad + x^2 & \\ \quad x^7 \quad + x^4 \quad + x & \\ \hline \quad x^5 + x^4 + x^2 + x & \end{array}$$

Т.о. $r(x) = x^5 + x^4 + x^2 + x$ и

$$v(x) \ = \ x^8 + x^7 + x^5 + x^4 + x^2 + x \ \leftrightarrow \ [0\,1\,1\,0\,1\,1\,\underline{0\,1\,1}]^T.$$

Задача 3.3. *Рассмотрим код Хэмминга систематического кодирования с порождающим примитивным полиномом* $a(x) = x^3 + x + 1$.

Требуется декодировать полиномы

1. $w_1(x) \ = \ x^6 + x^2 + x,$
2. $w_2(x) \ = \ x^6 + x^5 + x^3 + x^2 + x,$
3. $w_3(x) \ = \ x^6 + x^3 + x^2 + x.$

Решение. Декодирование систематического кода Хэмминга можно провести делением принятого полинома на порождающий: остаток от деления определяет синдром s с учётом таблицы соответствий между полиномиальным и степенным представлением элементов рассматриваемого поля (дублируем таблицу со с. 168):

$x^3 = x + 1$ степень x	1	x	x^2
x	$(0,$	$1,$	$0)$
x^2	$(0,$	$0,$	$1)$
$x^3 = x + 1$	$(1,$	$1,$	$0)$
$x^4 = x^2 + x$	$(0,$	$1,$	$1)$
$x^5 = x^2 + x + 1$	$(1,$	$1,$	$1)$
$x^6 = x^2 + 1$	$(1,$	$0,$	$1)$
$x^7 = 1$	$(1,$	$0,$	$0)$

Находим позицию ошибки j.

1. $x^6 + x^2 + x = (x^3 + x + 1)^2 + \underline{x + 1}$, $j = 3$.

   Действительно,

$$w(\alpha) = \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1.$$

2. $x^6 + x^5 + x^3 + x^2 + x = \\ = (x^3+x^2+x+1)(x^3+x+1)+\underline{x^2 + x + 1}$, $j = 5$;

   Действительно,

$$w(\alpha) = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha = \\ = \alpha^2 + 1 + \alpha^5 + \alpha + 1 + \alpha^2 + \alpha = \alpha^5.$$

3. $x^6 + x^3 + x^2 + x = (x^3 + x)(x^3 + x + 1) + \underline{0}$, т. е. ошибки не произошло.

Задача 3.4. *Пусть α — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$. Для кода БЧХ с нулями α, α^2, α^3 и α^4 и принятого слова*

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

Решение. Для удобства вычислений продублируем таблицу соответствий между степенным и полиномиальным представлением элементов данного поля со с. 66:

α^1	α	(0010)
α^2	α^2	(0100)
α^3	α^3	(1000)
α^4	$\alpha + 1$	(0011)
α^5	$\alpha^2 + \alpha$	(0110)
α^6	$\alpha^3 + \alpha^2$	(1100)
α^7	$\alpha^3 + \alpha + 1$	(1011)
α^8	$\alpha^2 + 1$	(0101)
α^9	$\alpha^3 + \alpha$	(1001)
α^{10}	$\alpha^2 + \alpha + 1$	(0111)
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	(1110)
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	(1111)
α^{13}	$\alpha^3 + \alpha^2 + 1$	(1101)
α^{14}	$\alpha^3 + 1$	(1001)
α^{15}	1	(0001)

С помощью этой таблицы вычислим синдромы:

$$\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \\
&= (\alpha^3 + 1) + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) + (\alpha + 1) = \\
&= \alpha^3 + \alpha + 1 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = \left(w(\alpha^2)\right)^2 = \alpha^{28} = \alpha^{13}.
\end{aligned}$$

Синдромный полином —

$$s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1.$$

Синдромов всего четыре, следовательно число возникших ошибок ν не более $2 = r$.

Полином локаторов ошибок $\sigma(x)$ удовлетворяет соотношению Безу

$$x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x), \quad \deg\lambda(x) \leqslant 2.$$

Решаем с данное соотношение помощью расширенного алгоритма Евклида:

$$\begin{aligned}
\text{Шаг 0.} \quad & r_{-2}(x) = x^5, \qquad \textit{// Инициализация} \\
& r_{-1}(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1, \\
& \sigma_{-2}(x) = 0, \\
& \sigma_{-1}(x) = 1.
\end{aligned}$$

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,
// *Делим* $r_{-2}(x)$ *на* $r_{-1}(x)$ *с остатком*
$q_0(x) = \alpha^2 x$,
$r_0(x) = \alpha x^3 + \alpha^9 x^2 + \alpha^2 x$,
$\sigma_0(x) = \sigma_{-2}(x) - \sigma_{-1}(x)q_0(x) =$
$= -q_0(x) = \alpha^2 x.$

Шаг 2. $r_{-1}(x) = r_{=0}(x)q_1(x) + r_1(x)$,
// *Делим* $r_{-1}(x)$ *на* $r_{=0}(x)$ *с остатком*
$q_1(x) = \alpha^{12} x + \alpha^5$,
$r_1(x) = \alpha^{14} x^2 + 1$,
$\deg r_1(x) = 2 \leqslant r$,
$\sigma_1(x) = \sigma_{-1}(x) - \sigma_{=0}(x)q_1(x) =$
$= 1 + \alpha^2 x(\alpha^{12} x + \alpha^5) =$
$= \underbrace{\alpha^{14} x^2 + \alpha^7 x + 1}_{\text{полином локаторов ошибок}} = \sigma(x).$

Задача 3.5. *Рассмотрим код БЧХ, нули которого определяются степенями* α, *где* α — *примитивный элемент поля* $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$.

Пусть для некоторого принятого слова $w(x)$ *полином локаторов ошибок есть*

$$\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1.$$

Требуется определить позиции ошибок в $w(x)$.

Решение. Найдём корни (их 2, полином квадратный) полинома локаторов ошибок полным перебором.

Для вычислений удобно пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной в предыдущей задаче.

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3,\\
\sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3,\\
\sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,\\
\sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1,\\
\sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = \mathbf{0},\\
\sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^7) &= \alpha^{16} + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1,\\
\sigma(\alpha^8) &= \alpha^{18} + \alpha^{14} + 1 = \mathbf{0}.
\end{aligned}$$

Дальше можно не вычислять: оба корня $\sigma(x)$ найдены. Итак, данный полином локаторов ошибок имеет корни α^5 и α^8.

Определяем позиции ошибок:

$$-5 \equiv_{15} 10, \qquad -8 \equiv_{15} 7.$$

Задача 3.6. *Построить 31-разрядный БЧХ-код для исправления не менее $r = 3$ ошибок.*

Решение. Имеем $n = 31 = 2^5 - 1$, $q = 5$, $d_c - 1 = 2r = 6$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни α, α^2, α^3, α^4, α^5, α^6, где α — примитивный элемент поля $F = \mathbb{F}_2^5$.

При разбиении F^* на циклотомические классы всегда[10] будет присутствовать пятиэлементный класс $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$.

[10] см. п. Циклотомический класс элемента поля на с. 143.

Остальные рассматриваемые степени α будут входить в циклотомические классы

$$\left\{\alpha^3, \alpha^6, \dots\right\} \quad \text{и} \quad \left\{\alpha^5, \dots\right\}.$$

Нетрудно установить, что эти классы также будут пятиэлементными:

$$\left\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48} = \alpha^{17}\right\}, \quad (\text{т. к. } 34 \equiv_{31} 3);$$
$$\left\{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40} = \alpha^9, \alpha^{18}\right\}, \quad (\text{т. к. } 36 \equiv_{31} 5).$$

Ранее[11] были приведены неприводимые многочлены 5-й степени над $\mathbb{F}_2$: их шесть —

1) $x^5 + x^2 + 1$,
2) $x^5 + x^3 + 1$,
3) $x^5 + x^3 + x^2 + x + 1$,
4) $x^5 + x^4 + x^2 + x + 1$,
5) $x^5 + x^4 + x^3 + x + 1$,
6) $x^5 + x^4 + x^3 + x^2 + 1$.

Во многих монографиях[12] есть соответствующие таблицы. В этих таблицах указано, что все эти многочлены являются примитивными, т. е. все они могут быть выбраны в качестве порождающего поле полинома $a(x)$.

Положим $a(x) = x^5 + x^3 + 1$ (многочлен № 2) и тогда $g_\alpha(x) = a(x)$, $\alpha^5 = \alpha^3 + 1$, $\alpha^{31} = 1$.

Определим, какие из остальных многочленов соответствуют циклотомическим классам для α^3 и α^5.

Имеем:

для многочлена № 3 —

[11] см. с. 35

[12] Например, *Лидл Р., Нидеррайтер Г.* Конечные поля, Том 1, Таблица С.

$$(x^5+x^3+x^2+x+1)\big|_{x=\alpha^3} = \alpha^{15}+\alpha^9+\alpha^6+\alpha^3+1 =$$
$$= (\alpha^3+1)^3+\alpha^4(\alpha^3+1)+\alpha(\alpha^3+1)+\alpha^3+1 = \ldots = 0,$$

для многочлена № 5 —

$$(x^5+x^4+x^3+x+1)\big|_{x=\alpha^5} = \alpha^{25}+\alpha^{20}+\alpha^{15}+\alpha^5+1 =$$
$$= (\alpha^3+1)^5+(\alpha^3+1)^4+(\alpha^3+1)^3+\alpha^5+1 = \ldots = 0.$$

Таким образом,

$g_{\alpha^3}(x) = x^5+x^3+x^2+x+1,\ g_{\alpha^5}(x) = x^5+x^4+x^3+x+1$

и порождающий многочлен для $(31,16,7)$-кода БЧХ есть

$$g(x) = g_\alpha(x)\cdot g_{\alpha^3}(x)\cdot g_{\alpha^5}(x) =$$
$$= x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1,$$
$$\deg g(x) = m = 15,\ k = n-m = 16.$$

Задача 3.7. *Рассмотрим БЧХ-код, нули которого определяются степенями примитивного элемента α поля $F = \mathbb{F}_2[x]/\big(x^4+x+1\big)$.*

Пусть для некоторого принятого слова полином локаторов ошибок есть $\sigma(x) = \alpha^6 x+\alpha^{15}$. Определить позиции ошибок в данном слове.

Решение. Для вычислений в поле F нам понадобится таблица, уже построеная в начале раздела *Существование и единственность поля $GF(p^n)$* и в Задаче 3.4.

α^1	α
α^2	α^2
α^3	α^3
α^4	$\alpha+1$
α^5	$\alpha^2+\alpha$
α^6	$\alpha^3+\alpha^2$
α^7	$\alpha^3+\alpha+1$
α^8	α^2+1
α^9	$\alpha^3+\alpha$
α^{10}	$\alpha^2+\alpha+1$
α^{11}	$\alpha^3+\alpha^2+\alpha$
α^{12}	$\alpha^3+\alpha^2+\alpha+1$
α^{13}	$\alpha^3+\alpha^2+1$
α^{14}	α^3+1
α^{15}	1

Перебором найдём корни полинома ошибок

$$\sigma(x) = \alpha^6 x + \alpha^{15} = (\alpha^3+\alpha^2)\,x + 1:$$

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4+\alpha^3+1 = \alpha+1+\alpha^3 \neq 0;\\
\sigma(\alpha^2) &= \alpha^5+\alpha^4+1 = \alpha^2+\alpha+\alpha+1+1 = \alpha^2 \neq 0;\\
&\cdots\cdots\\
\sigma(\alpha^9) &= \alpha^{12}+\alpha^{11}+1 =\\
&= (\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+\alpha)+1 = \mathbf{0}.
\end{aligned}$$

Линейный полином $\sigma(x)$ имеет один корень — α^9, и поэтому позиция единственной ошибки есть $-9 \equiv_{15} 6$.

Глава 4

Теория перечисления Пойа

4.1 Действие группы на множестве

- Группа $\langle G, \circ, e \rangle$, $|G| = n$.
- Множество T, $|T| = N > 0$.
  - $Bij(T)$ — множество всех перестановок элементов T или биекций на T.
  - S_T — симметрическая группа множества T:

$$S_T = \langle Bij(T), *, 1_T \rangle.$$

Определение 4.1 (I). $\alpha \in \mathrm{Hom}\,(G, S_T)$.

Действие α группы G на множестве T символически записывают $G \underset{\alpha}{:} T$.

Определение 4.2 (II). $\alpha = \langle G, T, \circ, \triangleright, e, 1_T \rangle$, где

$G \times G \xrightarrow{\circ} G$ — групповая операция;

$G \times T \xrightarrow{\triangleright} T$ — новая некоммутативная операция.

Аксиомы для операций:

$$1.\ e \triangleright t = t; \qquad 2.\ (g \circ h) \triangleright t = h \triangleright (g \triangleright t).$$

Запись операции $\triangleright$: $g(t) = t'$.
Тогда аксиомы: $e(t) = t$ и $(g \circ h)(t) = h(g(t))$.

Элементы g группы G порождают перестановки на T, обладающие указанными свойствами.

Для данной перестановки g:

Введём отношение эквивалентности $\sim_g$ на T —

$$t \sim_g t' \Leftrightarrow \exists\, k \in \mathbb{Z} : g^k(t) = t'$$

Рефлексивность (R), *симметричность* (S) и *транзитивность* (T) отношения $\sim_g$ легко показываются.

Смежные классы эквивалентности $\sim_g$ называются *g-циклами*: элементы этих классов образуют циклы:

$t \xrightarrow{g} t' \xrightarrow{g} \ldots \xrightarrow{g} t$, *и у каждого элемента — по единственной входящей и исходящей стрелке.*

Обозначения:

- $\langle\, \nu_1, \nu_2, \ldots, \nu_N \,\rangle = Type(g)$ — *тип перестановки* g — упорядоченная совокупность числа циклов длины $1, 2, \ldots, N$ соответственно;
- $C(g)$ — число всех g-циклов.

Понятно, что $\sum\limits_{k=1}^{N} \nu_k(g) = C(g)$ и $\sum\limits_{k=1}^{N} k \cdot \nu_k(g) = N$.

Пример 4.1. Пусть $T = \{\, 1, \ldots, 10 \,\}$ и

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 10 & 3 & 4 \end{pmatrix} =$$
$$= (1,9,3)(2,6)(4,8,10)(5)(7) = (2,6)(1,9,3)(4,8,10).$$

Тогда $Type(g) = \langle\, 2, 1, 2, 0, \ldots, 0 \,\rangle$ и

$C(g) = 2+1+2 = 5$, $\big|\, T \,\big| = 2 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 = 10$.

По всей группе G:

Отношение эквивалентности $\sim_G$ на T —

$$t \sim_G t' \Leftrightarrow \exists\, g \in G : g(t) = t'.$$

Свойства (R), (S) и (T) отношения $\sim_G$ очевидны.

- Классы этой эквивалентности называют *орбитами*; они образуют разбиение множества T.
- Класс эквивалентности, в которую попадает элемент t обозначаем $\mathrm{Orb}\,(t)$.
- Число получившихся орбит — $C(G)$.

Если $C(G) = 1$ (любой элемент T может быть переведён в любой), то действие $G \underset{\alpha}{:} T$ называют *транзитивным.*

Фиксатор перестановки и стабилизатор элемента множества. Рассмотрим равенство

$$g(t) = t.$$

При выяснении, когда оно выполняется, рассматриваем 2 случая, полагая постоянным либо t, либо g.

1. Фиксируем g, т. е. находим все элементы множества T, которые данная перестановка оставляет на месте — это *фиксатор перестановки* $g \in G$:

$$\left\{\, t \in T \mid g(t) = t \,\right\} = \mathrm{Fix}\,(g) \subseteq T.$$

2. Фиксируем t, т. е. находим все перестановки g, которые оставляют данный элемент неподвижным — это *стабилизатор элемента* $t \in T$:

$$\left\{\, g \in G \mid g(t) = t \,\right\} = \mathrm{Stab}\,(t) \subseteq G.$$

Очевидно $\forall\, t \in T : e \in \mathrm{Stab}\,(t)$, т. е. $\mathrm{Stab}\,(t) \neq \varnothing$.
Более того, стабилизатор есть подгруппа группы G:

Утверждение 4.1. $\mathrm{Stab}\,(t) \leqslant G$.

Доказательство. Для $t \in T$ рассмотрим $g,\, h \in \mathrm{Stab}\,(t)$. Тогда $g(t) = h(t) = t$ и $h^{-1}(t) = t$. Следовательно

$$(g \circ h^{-1}) \triangleright t = t \;\Rightarrow\; g \circ h^{-1} \in \mathrm{Stab}\,(t)\,.$$

□

Поэтому стабилизатор $\mathrm{Stab}\,(t)$ называют ещё *стационарной подгруппой*[1] *элемента* t и обозначают иногда G_t.

Утверждение 4.2. *При действии группы* G *на множество* T *между множеством левых смежных классов* G *по стационарной подгруппе* G_t *элемента* $t \in T$ *и его орбитой* $\mathrm{Orb}\,(t)$ *существует взаимно однозначное соответствие.*

Доказательство. Левые смежные классы G по G_t обозначаем gG_t, $g \in G$, считая при этом, что на элементы T сначала действует некоторая перестановка из G_t, а затем — фиксированная перестановка g.

Но тогда любая перестановка $h \in gG_t$ одинаково подействует на $t \in T$: $h(t) = g(t) = t' \in \mathrm{Orb}\,(t)$ (т. к. все элементы G_t оставляют t на месте). С учётом того, что смежные классы либо совпадают, либо не пересекаются, утверждение доказано. □

Из этого утверждения вытекает важное

[1] или *изотопической подгруппой*

Следствие. *Длина орбиты* $\operatorname{Orb}(t)$ *равна индексу стационарной подгруппы* $\operatorname{Stab}(t)$ *в группе* G*:*

$$\big|\operatorname{Orb}(t)\big| \;=\; \frac{\big|G\big|}{\big|\operatorname{Stab}(t)\big|} \;=\; [\,G : \operatorname{Stab}(t)\,].$$

Доказательство. По теореме Лагранжа

$$H \leqslant G \;\Rightarrow\; \big|\,G\,\big| = \big|\,H\,\big| \cdot [\,G : H\,]$$

число смежных классов группы G по её подгруппе $H \leqslant G$ равно индексу $[\,G : H\,]$. □

4.2 Лемма Бёрнсайда

Лемма 4.1 («не-Бёрнсайда», или Коши-Фробениуса). *Если группа* G *действует на множестве* T*, то*

$$C(G) \;=\; \frac{1}{|\,G\,|}\sum_{g\in G}\Big|\operatorname{Fix}(g)\Big| \;=\; \frac{1}{|\,G\,|}\sum_{t\in T}\Big|\operatorname{Stab}(t)\Big|;$$

при этом первое равенство называется леммой Бёрнсайда.

Доказательство. Пусть $|G| = n$, $|T| = N$ и действие $G \overset{\alpha}{:} T$ задаётся $n \times N$ матрицей $A = \|g_i(t_j)\|$, $i = \overline{1,n}$, $j = \overline{1,N}$.

Подсчитаем двумя различными способами мощность множества $M = \big\{\,(g,t) \in G \times T \mid g(t) = t\,\big\}$: по столбцам и по строкам матрицы A. Получим

$$\sum_{g\in G}\Big|\operatorname{Fix}(g)\Big| \;=\; \big|M\big| \;=\; \sum_{t\in T}\Big|\operatorname{Stab}(t)\Big|.$$

Если x и y принадлежат одному классу эквивалентности по $\sim_G$, то $\operatorname{Orb}(x) = \operatorname{Orb}(y)$ и их стационарные подгруппы имеют одинаковую мощность:

$$|G_x| = \frac{|G|}{|\operatorname{Orb}(x)|} = \frac{|G|}{|\operatorname{Orb}(y)|} = |G_y|.$$

Выберем по представителю $t_1, \ldots, t_{C_G}$ из всех $C(G)$ орбит. Тогда

$$|M| = \sum_{t \in T} |G_t| = \sum_{i=1}^{C(G)} |G_{t_i}| \cdot \left|\operatorname{Orb}(t_i)\right| =$$

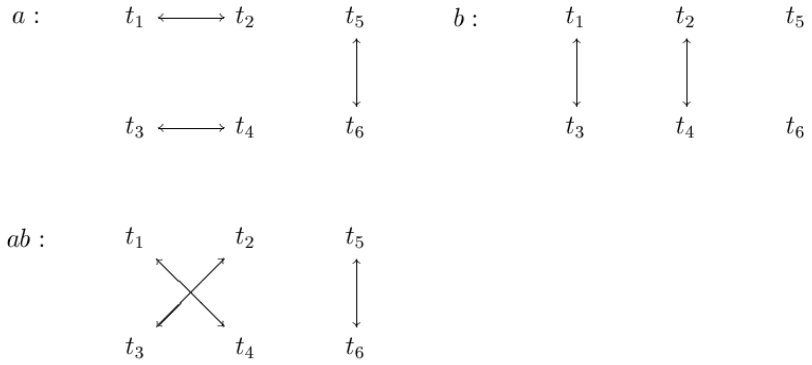
$$= \sum_{i=1}^{C(G)} \frac{|G|}{\left|\operatorname{Orb}(t_i)\right|} \cdot \left|\operatorname{Orb}(t_i)\right| = |G| \cdot C(G).$$

□

Пример 4.2. Действие четверной группы Клейна V_4 на множестве $T = \{t_1, \ldots, t_6\}$:

$\circ$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$\triangleright$	t_1	t_2	t_3	t_4	t_5	t_6
e	t_1	t_2	t_3	t_4	t_5	t_6
a	t_2	t_1	t_4	t_3	t_6	t_5
b	t_3	t_4	t_1	t_2	t_5	t_6
ab	t_4	t_3	t_2	t_1	t_6	t_5



$$Type(e) = \langle 6,0,0,0,0,0\rangle, \quad Type(a) = \langle 0,3,0,0,0,0\rangle,$$
$$Type(b) = \langle 2,2,0,0,0,0\rangle, \quad Type(ab) = \langle 0,3,0,0,0,0\rangle.$$
$$C(e) = 6,\ C(a) = C(ab) = 3,\ C(b) = 4.$$
$$\mathrm{Stab}\,(t_1) = \mathrm{Stab}\,(t_2) = \mathrm{Stab}\,(t_3) = \mathrm{Stab}\,(t_4) = e \leqslant V_4,$$
$$\mathrm{Stab}\,(t_5) = \mathrm{Stab}\,(t_6) = \langle e, b\rangle \leqslant V_4.$$
$$\mathrm{Fix}\,(a) = \mathrm{Fix}\,(ab) = \varnothing,\ \mathrm{Fix}\,(b) = \{t_5, t_6\},\ \mathrm{Fix}\,(e) = T.$$
$$\big|\,\mathrm{Orb}\,(t_1)\big| = \frac{4}{1} = 4, \quad \big|\,\mathrm{Orb}\,(t_5)\big| = \frac{4}{2} = 2.$$
$$\frac{1}{4}\sum_{g\in G}\big|\,\mathrm{Fix}\,(g)\big| = \frac{6+2}{4} = 2,$$
$$\frac{1}{4}\sum_{t\in T}\big|\,\mathrm{Stab}\,(t)\big| = \frac{4\cdot 1 + 2\cdot 2}{4} = 2.$$

Как применять лемму Бёрнсайда?

Для определения числа классов эквивалентности надо представить *отождествляемые элементы множества* T *как классы эквивалентности* действия некоторой группы G на T и по лемме Бёрнсайда определить $C(G)$.

Задача 4.1 (про слова). *Составляются слова длины* $l \geqslant 2$ *из алфавита* $A = \{ a_1, \ldots, a_q \}$.

Слова считаются эквивалентными, если они получаются одно из другого перестановкой крайних букв.

Определить число W *неэквивалентных слов.*

Решение (прямым использованием леммы Бёрнсайда). Пусть T — множество слов длины l в алфавите A, $|T| = N = q^l$.

Надо представить эквивалентности как орбиты некоторого действия подходящей группы G на T.

Очевидно, двукратная перестановка не меняет ничего, и поэтому подходит $G \cong \mathbb{Z}_2 = \{ e, f \}$. Действие f: переставляет в слове крайние буквы.

Число неэквивалентных слов = число классов эквивалентности действия $\mathbb{Z}_2 \underset{\alpha}{:} T$ —

$$\big|\operatorname{Fix}(e)\big| = \big|T\big| = q^l, \qquad \big|\operatorname{Fix}(f)\big| = q^{l-2} \cdot q = q^{l-1}.$$

$$W = C(\mathbb{Z}_2) = \frac{1}{2} \sum_{g \in G} \big|\operatorname{Fix}(g)\big| = \frac{q^l + q^{l-1}}{2} = \frac{q^{l-1}(q+1)}{2}.$$

Для $l = 3$, $q = 2$ имеем $|T| = 8$ и $W = \frac{4 \cdot 3}{2} = 6$. Пусть $A = \{a, b\}$, тогда слова и классы —

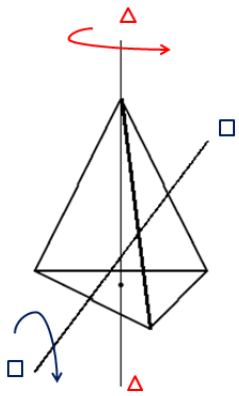
	aaa		(1)
aab		baa	(2)
	aba		(3)
abb		bba	(4)
	bab		(5)
	bbb		(6)

Платоновы тела — правильные 3-мерные многогранники. Рассматриваем их группы вращений (самосовмещений).

Платоновы тела	*Группа* вращения	*Порядок* группы
тетраэдр	T (тетраэдра)	$4 \cdot 3 = 12$
куб и октаэдр	O (октаэдра)	$8 \cdot 3 = 24$
икосаэдр и додекаэдр	Y (икосаэдра)	$12 \cdot 5 = 60$

Икосаэдр имеет 20 граней, 30 рёбер и 12 вершин.

T — группа вращения тетраэдра



$T = \langle t, f \rangle$, $t^3 = f^2 = e$, где:

t — вращение на $120°$ вокруг оси, проходящей через вершину и центр тетраэдра (△—△); таких осей 4.

f — вращение на $180°$ вокруг оси, проходящей через центры двух противоположных рёбер (□—□); таких осей 3.

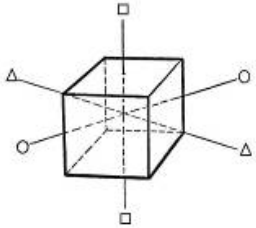
$|T| = (3-1) \cdot 4 + (2-1) \cdot 3 + 1 = 12.$

Действие T на грани (или вершины) тетраэдра: типы перестановок

$$\square: \ Type(t) = Type(t^2) = \langle 1, 0, 1, 0 \rangle;$$
$$\triangle: \ Type(f) = \langle 0, 2, 0, 0 \rangle.$$

Тетраэдр двойственен самому себе $\Rightarrow$ действие на грани $=$ действие на вершины.

O — группа вращения октаэдра (= куба)



$O = \langle t, f, r \rangle, t^4 = f^2 = r^3 = e$, где:
t — вращение на $90°$ вокруг оси, проходящей через середины двух противоположных граней (□—□), таких осей 3;
f — вращение на $180°$ вокруг оси, проходящей через середины двух противоположных рёбер (○—○), таких осей 6;
r — вращение на $120°$ вокруг оси, проходящей через две противоположные вершины (△—△) таких осей 4.

$$|O| = 3 \cdot 3 + 1 \cdot 6 + 2 \cdot 4 + 1 = 24.$$

Пример 4.3 (Действие O на вершины куба: типы перестановок).

$$\begin{aligned} \square: \ Type(t) &= Type(t^3) = \langle 0,0,0,2,0,\ldots\rangle; \\ Type(t^2) &= \langle 0,4,0,\ldots\rangle; \\ \circ: \ Type(f) &= \langle 0,4,0,\ldots\rangle; \\ \triangle: \ Type(r) &= Type(r^2) = \langle 2,0,2,0,\ldots\rangle. \end{aligned}$$

Поскольку $|G| = |G_x| \cdot [G : G_x]$, то число элементов в группе вращения правильного многогранника есть $\big|E_0\big| \cdot \big|V\big|$, где $\big|E_0\big|$ — число рёбер, выходящих из одной вершины и $\big|V\big|$ — число вершин многогранника.

Цикловой индекс. Существует универсальный способ вычисления числа $C(G)$ — количества классов эквивалентности (= орбит).

Сопоставим каждой перестановке $g \in G$ вес $w(g)$ по правилу:

$$Type(g) = \langle \nu_1, \ldots, \nu_N \rangle \;\Rightarrow\; w(g) = \underbrace{x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}}_{\text{моном}}.$$

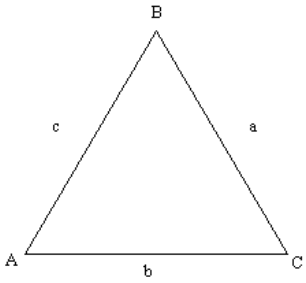
Определение 4.3. Средний вес подстановок в группе называется *цикловым индексом* действия $G \underset{\alpha}{:} T$:

$$P(G \underset{\alpha}{:} T,\, x_1,\, \ldots,\, x_N) = \frac{1}{|G|} \sum_{g \in G} w(g) = \\ = \frac{1}{|G|} \sum_{g \in G} x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}.$$

Будем также использовать обозначения $P_G(x_1,\, \ldots,\, x_N)$ и $P_G,\ P(G)$.

Пример 4.4. Вычислим цикловой индекс действия группы всех преобразований правильного треугольника в себя (т. е. оставляющих его неподвижным), на его стороны.

Решение. T — стороны треугольника, $N = 3$.
$G \cong S_3$ — все перестановки сторон, $n = 3! = 6$.



$G \underset{\alpha}{:} T$ — самодействие группы S_3

Треугольник — самодвойственная фигура $\Rightarrow$ $\Rightarrow$ действие на стороны $=$ $=$ действие на вершины

$$G \underset{\alpha}{:} T = \langle t, f \rangle =$$
$$= \{ e, \underbrace{(abc)}_{t}, \underbrace{(acb)}_{t^2}, \underbrace{((a)(bc))}_{f}, \underbrace{((b)(ac))}_{tf}, \underbrace{((c)(ab))}_{t^2 f} \}.$$

$g \in S_3$	$Type(g)$	$w(g)$	# мономов
$e = (a)(b)(c)$	$\langle 3, 0, 0 \rangle$	x_1^3	1
t, t^2	$\langle 0, 0, 1 \rangle$	x_3^1	2
f, tf, $t^2 f$	$\langle 1, 1, 0 \rangle$	$x_1^1 x_2^1$	3
Всего			6

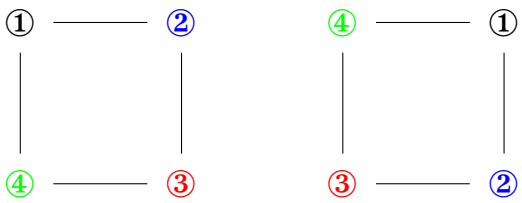
$$P(S_3) = \frac{1}{6}\left[x_1^3 + 2x_3^1 + 3x_1^1 x_2^1 \right],$$

— цикловой индекс *самодействия группы* S_3, или, что то же, *группы симметрии треугольника*.

Зачем нужен цикловой индекс?
Пусть заданы множество T, группа G и действие $G \underset{\alpha}{:} T$.

1. Припишем каждому элементу T одно из r значений (неформально: покрасим в один из r цветов). Всего, очевидно, имеется r^N раскрасок.

2. *Не будем различать раскраски*, если элементы t и $t' = g(t)$ раскрашены одинаково.
   Например, поворот на 90° вокруг центра симметрии не даёт нового раскрашивания вершин квадрата:



Вопрос: Сколько существует *неэквивалентных раскрасок = классов эквивалентности*?
Ответ: Это значение вычисляется через цикловой индекс. Имеем —

1. Каждый класс эквивалентности — это g-цикл; их $C(g) = \nu_1 + \ldots + \nu_N$ штук.
2. Каждая перестановка $g \in G$ с типом $\langle\, \nu_1, \ldots, \nu_N \,\rangle$ будет иметь $\big|\operatorname{Fix}(g)\big| = r^{C(g)}$ неподвижных точек: каждый класс эквивалентности это g-цикл, их $C(g)$ и

$$\big|\operatorname{Fix}(g)\big| \;=\; x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}\Big|_{x_1=\ldots=x_N=r} \;=\; r^{C(g)}.$$

Отсюда, по лемме Бёрнсайда, число полученных классов эквивалентности = неэквивалентных раскрасок:

Теорема 4.1.

$$C(G \underset{\alpha}{:} T) \;=\; P(G \underset{\alpha}{:} T,\, x_1,\, \ldots,\, x_N)\Big|_{x_1=\ldots=x_N=r}.$$

Например, $P_G(1, \ldots, 1) = 1$: если все элементы покрасить в один цвет, то таких раскрасок одна.

Задачи на применение циклового индекса

Задача 4.1 (про слова). *Определить число W неэквивалентных слов длины $l \geqslant 2$ в q-буквенном алфавите, если эквивалентными считаются слова, получающиеся друг из друга перестановкой крайних букв.*

Было решение: $W = \frac{q^l+q^{l-1}}{2}$.

Решение (новое, использующее цикловой индекс):

$G = \{ e, g \} \cong \mathbb{Z}_2$; T: $\underbrace{\bigcirc\overbrace{\bigcirc\ldots\bigcirc}^{l-2}\bigcirc}_{l}$.

$g \in G$	$Type(g)$	$w(g)$	# мономов
e	$\langle l, 0, \ldots, 0 \rangle$	x_1^l	1
g	$\langle l-2, 1, 0, \ldots, 0 \rangle$	$x_1^{l-2}x_2^1$	1

Цикловой индекс: $P(x_1, \ldots, x_l) = \frac{1}{2}\left[x_1^l + x_1^{l-2}x_2^1\right]$.

$$W = P(q, \ldots, q) = \frac{q^l + q^{l-1}}{2}.$$

Классическая комбинаторная задача об ожерельях

- *Ожерелье* — окружность, на которой на равных расстояниях по дуге (в вершинах правильного многоугольника) располагаются «бусины».
- *Задача об ожерельях*: сколько различных ожерелий можно составить из N бусин r цветов?
- Какие ожерелья считать неразличимыми?

  Варианты: если одно ожерелье получается из другого *самосовмещением* —

1) только *поворотом* в плоскости вокруг центра ожерелья[2] — самодействие группы $\mathbb{Z}_N$;
2) и *поворотом*, и *переворотом в пространстве* — самодействие *группы диэдра*[3] D_N.

Задача 4.2 (об ожерельях $N = 5$, $r = 3$; 1-й вариант). *Сколько разных ожерелий можно составить из* 5 *бусин* 3 *цветов?*

1. Ожерелья одинаковы, если одно получается из другого *поворотом*.

Решение. $G \cong \mathbb{Z}_5 = \langle t \rangle$, $t^5 = e$, $n = 5$.

Элемент $\mathbb{Z}_5$	$Type(g)$	$w(g)$	# мономов
e	$\langle 5, 0, 0, 0, 0 \rangle$	x_1^5	1
t, t^2, t^3, t^4	$\langle 0, 0, 0, 0, 1 \rangle$	x_5	4

Цикловой индекс: $P(x_1, \ldots, x_5) = \dfrac{1}{5}\left[x_1^5 + 4x_5\right]$.

$$\#Col(3) = P(3, \ldots, 3) = \frac{1}{5}\left(3^5 + 4 \cdot 3\right) = 51.$$

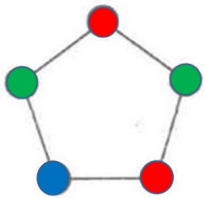
Задача 4.3 (Олимпиады «*Покори Воробьёвы горы – 2009*»). *Для* 50 *детей детского сада закуплены* 50 *одинаковых тарелок. По краю каждой тарелки равномерно расположено* 5 *белых кружочков. Воспитатели хотят закрасить какие-либо из этих кружочков в*

[2] т.н. *карусель*

[3] двойной пирамиды

другие цвета так, чтобы все тарелки стали различными.

Какое наименьшее число дополнительных цветов потребуется им для этого?



Как должны были решать школьники.

Пусть требуется r цветов. Отбросим r вариантов раскраски в один цвет. Число остальных вариантов —

без учёта возможности поворота тарелки: $r^5 - r$;

с учётом поворота: $\dfrac{r^5 - r}{5}$, т. к. каждый вариант повторяется 5 раз.

Итого: $\#Col(r) = \dfrac{r^5 - r}{5} + r = \dfrac{r^5 + 4r}{5}$
и при 2 дополнительных цветах $\#Col(3) = 51$.

Задача 4.2 (об ожерельях $N = 5$, $r = 3$; 2-й вариант).

2. Ожерелья одинаковы, если одно получается из другого *поворотом и/или переворотом.*

Решение. G — *группа диэдра* $D_5 = \langle t, f \rangle$, $t^5 = f^2 = e$, $n = |D_5| = 10$.

Элемент D_5	$Type(g)$	$w(g)$	# мономов
e	$\langle 5,\, 0,\, 0,\, 0,\, 0 \rangle$	x_1^5	1
$t,\, t^2,\, t^3,\, t^4$	$\langle 0,\, 0,\, 0,\, 0,\, 1 \rangle$	x_5	4
$f,\, tf,\, \ldots,\, t^4 f$	$\langle 1,\, 2,\, 0,\, 0,\, 0 \rangle$	$x_1 x_2^2$	5
Всего			10

Цикловой индекс: $P = \dfrac{1}{10}\left[\, x_1^5 + 4x_5 + 5x_1x_2^2 \,\right]$.

$$\#Col(3) = P(x_1, \ldots, x_5)\Big|_{x_1 = \ldots = x_5 = 3} = \\ = \frac{3^5 + 4 \cdot 3 + 5 \cdot 3^3}{10} = 39.$$

Задача 4.4 (о раскраске сторон квадрата). *Сколько существует различно окрашенных квадратов, если их стороны раскрашивают в r цветов?*

Решение. Группа самосовмещения квадрата в пространстве — группа диэдра $D_4 = \langle\, t,\, f,\, s \,\rangle$, $|D_4| = 8$, которая порождается тремя образующими:

t : вращение на 90° вокруг центра в выбранном направлении;

f : симметрия относительно оси, проходящей через середины противоположных *сторон* — 2 оси;

s : симметрия относительно оси, проходящей через середины противоположных *вершин* — 2 оси.

При самодействии группы D_4 $(N = 4)$ её элементы будут иметь следующие веса:

e : единичная перестановка оставит все стороны на месте, т. е. имеются 4 цикла длины 1, вес x_1^4 (1 перестановка);

t, t^3 : стороны циклически переходят друг в друга по и против часовой стрелке, длина цикла 4, вес x_4^1 (2 перестановки);

t^2 : стороны переходят в противоположные, что даёт два цикла длины 2, вес — x_2^2 (1 перестановка);

f : две противоположные стороны на месте, остальные две меняются местами, т. е. имеются два единичных цикла и один длины 2, вес — $x_1^2 x_2^1$ (1 перестановка, 2 оси);

s : в двух парах смежных сторон элементы меняются местами, что даёт два цикла длины 2, вес — x_2^2 (1 перестановка, 2 оси).

Итого:

Элемент D_5	$Type(g)$	$w(g)$	# мономов
e	$\langle 5, 0, 0, 0 \rangle$	x_1^4	1
t, t^3	$\langle 0, 0, 0, 1 \rangle$	x_4	2
t^2	$\langle 0, 2, 0, 0 \rangle$	x_2^2	1
f	$\langle 2, 1, 0, 0 \rangle$	$x_1^2 x_2$	$1 \times 2 = 2$
s	$\langle 0, 2, 0, 0 \rangle$	x_2^2	$1 \times 2 = 2$
Всего			8

Цикловой индекс самодействия D_4:

$$P_{D_4}(x_1, \ldots, x_4) = \frac{1}{8}\left[\, x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2 x_2 \,\right].$$

Число раскрасок квадрата в r цветов:

$$P_{D_4}(r, \ldots, r) = \frac{1}{8}\left[\, r^4 + 2r + 3r^2 + 2r^3 \,\right].$$

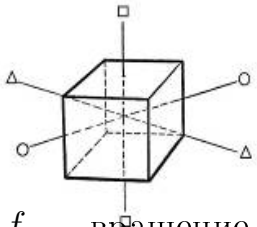
В частности, в два и три цвета:

$$\#Col(2) = \frac{2^4 + 4 \cdot 2^2 + 2^4}{2^3} = 2 + 2 + 2 = 6,$$
$$\#Col(3) = \frac{3^4 + 2 \cdot 3 + 3^4}{8} = 21.$$

Цикловой индекс действия группы октаэдра на множестве F граней куба ($|F| = N = 6$).

Задача 4.5. *Грани куба раскрашивают в 2 и 3 цвета. Сколько существует различно окрашенных кубов?*

Решение. Напоминание: $G = O = \langle\, t,\, f,\, r \,\rangle$, $|O| = 24$.



$O = \langle t, f, r\rangle, t^4 = f^2 = r^3 = e$, где:
t — вращение на $90°$ вокруг оси, проходящей через середины двух противоположных граней (□—□), таких осей 3;
f — вращение на $180°$ вокруг оси, проходящей через середины двух противоположных рёбер (○—○), таких осей 6;
r — вращение на $120°$ вокруг оси, проходящей через две противоположные вершины (△—△) таких осей 4.

Обозначим через F множество граней куба; $|F| = N = 6$. Выберем некоторую грань куба (квадрат) и обозначим её ①, а параллельную ей — ②.

Перенумеруем последовательно вершины грани ① числами $1, \ldots, 4$, а вершины грани ② — числами $5, \ldots, 8$ так, что вершина с номером i смежна с вершиной с номером $i+4$, $i = 1, 2, 3, 4$.

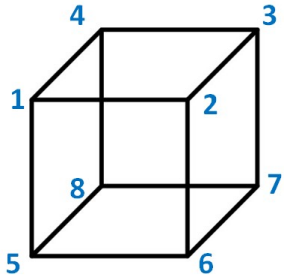
Перестановки далее указаны для случая, когда ось вращения

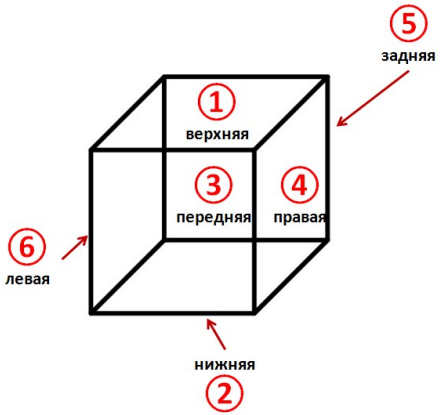
$\langle t \rangle$ проходит через середины граней ① и ②,

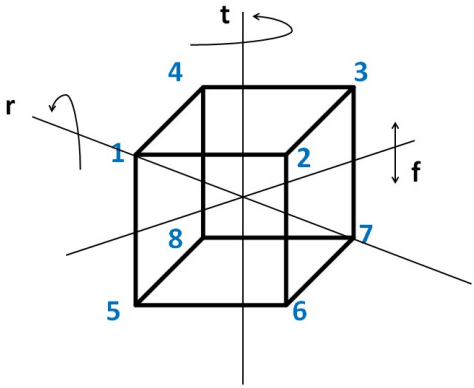
$\langle f \rangle$ проходит через середины рёбер (3-7) и (1-5),

$\langle s \rangle$ проходит через вершины (1) и (7),

а грани обозначены: (1-2-6-5) через ③, параллельная ей грань — ⑤, грань (2-3-7-6) — через ④, параллельная ей грань — ⑥.







$g \in O$	перестановка	$Type(g)$	$w(g)$	#
e	(①)…(⑥)	$\langle 6,\ 0,\ \ldots \rangle$	x_1^6	1
t, t^3	(①)(②)(③④⑤⑥)	$\langle 2,\ 0,\ 0,\ 1,\ 0,\ \rangle$	$x_1^2 x_4$	6
t^2	(①)(②)(③⑤)(④⑥)	$\langle 2,\ 2,\ 0,\ \ldots \rangle$	$x_1^2 x_2^2$	3
f	(①②)(③⑥)(④⑤)	$\langle 0,\ 3,\ 0,\ \ldots \rangle$	x_2^3	6
r, r^2	(①③⑥)(②④⑤)	$\langle 0,\ 0,\ 2,\ 0,\ \ldots \rangle$	x_3^2	8
Всего				24

$$P(x_1,\ \ldots,\ x_6) \ =\ \frac{1}{24}\left[\, x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2 \,\right].$$

$$\#Col(2) \ =\ \frac{1}{24}\left[2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 8\cdot 2^2\right] \ =\ 10,$$
$$\#Col(3) \ =\ \frac{1}{24}\left[3^6 + 12\cdot 3^3 + 3\cdot 3^4 + 8\cdot 3^2\right] \ =\ 48.$$

Цикловой индекс действия группы октаэдра на множестве R *рёбер куба* ($|R| = N = 12$):

$g \in O$	$Type(g)$	$w(g)$	#
e	$\langle 12, 0, \dots \rangle$	x_1^{12}	1
t, t^3	$\langle 0, 0, 0, 3, 0, 0 \rangle$	x_4^3	$3 \cdot 2 = 6$
t^2	$\langle 0, 6, 0, \dots \rangle$	x_2^6	3
f	$\langle 2, 5, 0, \dots \rangle$	$x_1^2 x_2^5$	6
r, r^2	$\langle 0, 0, 4, 0, \dots \rangle$	x_3^4	$4 \cdot 2 = 8$

$$P(O \underset{\alpha}{:} R) = \frac{1}{24}\left[x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4\right].$$

Цикловой индекс действия группы октаэдра на множестве V вершин куба ($|V| = N = 8$):

$g \in O$	$Type(g)$	$w(g)$	#
e	$\langle 8, 0, \dots \rangle$	x_1^8	1
t, t^3	$\langle 0, 0, 0, 2, 0, 0 \rangle$	x_4^2	$3 \cdot 2 = 6$
t^2	$\langle 0, 4, 0, \dots \rangle$	x_2^4	3
f	$\langle 0, 4, 0, \dots \rangle$	x_2^4	6
r, r^2	$\langle 2, 0, 2, 0, \dots \rangle$	$x_1^2x_3^2$	$4 \cdot 2 = 8$

$$P(O \underset{\alpha}{:} V) = \frac{1}{24}\left[x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2\right].$$

Цикловые индексы самодействия S_n, $\mathbb{Z}_n$, D_n и действия O на элементы куба.

$$P(S_n) = \sum_{\substack{(j_1,\dots,j_n)\in\mathbb{N}_0^n \\ 1j_1+2j_2+\dots+nj_n=n}} \frac{x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}}{(1^{j_1}j_1!)(2^{j_2}j_2!)\dots(n^{j_n}j_n!)},$$

$$P(\mathbb{Z}_n) = \frac{1}{n}\sum_{d|n}\varphi(d)\,x_d^{n/d}, \quad \varphi - \text{функция Эйлера},$$

$$P(D_n) = \frac{1}{2}P(\mathbb{Z}_n) + \begin{cases} \frac{1}{2}\,x_1 x_2^{(n-1)/2}, & n \text{ нечётно}, \\ \frac{1}{4}\left[\,x_2^{n/2} + x_1^2 x_2^{n/2-1}\,\right], & n \text{ чётно}, \end{cases}$$

$$P(O \underset{\alpha}{:} V) = \frac{1}{24}\left[\,x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2\,\right],$$

$$P(O \underset{\alpha}{:} E) = \frac{1}{24}\left[\,x_1^{12} + 3x_2^6 + 8x_3^4 + 6x_1^2x_2^5 + 6x_4^3\,\right],$$

$$P(O \underset{\alpha}{:} F) = \frac{1}{24}\left[\,x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2\,\right].$$

4.3 Решение комбинаторных задач с помощью теоремы Пойа

К множеству T, $|T| = N$, группе G, $|G| = n$ и действию $G \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \ldots, c_r\}$, меток («красок»), и совокупность функций $F = R^T$ — приписывания меток (*раскрашиваний*) элементам T.

G, действуя на T, действует и на R^T.

Придадим вес элементам R: $w(c_i) = y_i$, $i = \overline{1,r}$.

Теорема 4.2 (Редфилда-Пойа; 1927, 1937). *Цикловой индекс действия группы G на R^T есть*

$$P(G \underset{\alpha}{:} R^T,\, y_1,\, \ldots,\, y_r) = \\ = P(G \underset{\alpha}{:} T,\, x_1,\, \ldots,\, x_N)\Big|_{x_k = y_1^k + \ldots + y_r^k,\; k = \overline{1,N}}.$$

Следствие. *Если все веса выбраны одинаковыми, т. е.* $y_1 = \ldots = y_r = 1$, *то* $x_1 = \ldots = x_N = r$ *и число классов эквивалентности*

$$W(F) = P(G \underset{\alpha}{:} T, r, \ldots, r)$$

— *лемма Бёрнсайда.*

Что можно определить (подсчитать) с помощью:

леммы Бёрнсайда — *общее число* неэквивалентных разметок (раскрасок);

теоремы Редфилда-Пойа — число разметок *данного типа*, т. е. содержащих данное количество элементов конкретного цвета (метки).

Усложним задачу об ожерельях:

Задача 4.1 (об ожерельях $N = 5$, $r = 3$, продолжение, более сложный вариант). *Цвета — красный, синий, зелёный. Ожерелья одинаковы, если одно получается из другого поворотом и переворотом.*

Сколько имеется ожерелий, имеющих ровно 2 *красные бусины?*

Решение. Было: $G = D_5$, цикловой индекс

$$P(x_1, \ldots, x_5) = \frac{1}{10}\left[x_1^5 + 4x_5 + 5x_1x_2^2\right],$$

всего ожерелий $P(3, \ldots, 3) = 39$ («карусель» — 51). Подстановка:

$$x_1 = y_1+y_2+y_3, \quad x_2 = y_1^2+y_2^2+y_3^2, \quad \ldots, \quad x_5 = y_1^5+y_2^5+y_3^5.$$

$$\left\{\begin{array}{ll} w(\textit{красный}) & = y_1, \\ w(\textit{синий}) & = y_2, \\ w(\textit{зелёный}) & = y_3 \end{array}\right. \Rightarrow \left\{\begin{array}{l} y_1 = y, \\ y_2 = y_3 = 1 \end{array}\right. \Rightarrow$$

$$\Rightarrow \left\{\begin{array}{ll} x_1 & = y + 2, \\ x_2 & = y^2 + 2, \\ \dots & \\ x_5 & = y^5 + 2. \end{array}\right. \quad \begin{array}{l} x_k \mapsto y^k + 2,\ k = \overline{1,5}; \\ P(y) = \sum\limits_{i=1}^{5} u_i y^i; \\ \boxed{u_2 = ?} \end{array}$$

$$P(y) = \frac{1}{10}\left[\, u_0 + u_1 y + u_2 y^2 + \ldots + u_5 y^5 \,\right] =$$

$$= \frac{1}{10}\left[\, (y+2)^5 + 4(y^5+2) + 5(y+2)(y^2+2)^2 \,\right] =$$

$$= \frac{1}{10}\left[\, \ldots + C_5^2 2^3 y^2 + \ldots + 5(y+2)(y^4+4y^2+4) \,\right] =$$

$$= \frac{1}{10}\left[\, \ldots + (10 \cdot 8 + 5 \cdot 2 \cdot 4)\, y^2 + \ldots \,\right].$$

$$u_2 = 8 + 4 = 12.$$

Задача 4.6 (о раскраске куба). *Вершины куба помечают красными и синим цветами. Сколько существует*

1) *разнопомеченных кубов* — $\#Col(2)$*?*
2) *кубов, у которых половина вершины красные* — $\#Col(4,4)$*?*
3) *кубов, у которых не более* 2 *красных вершин* — $\#Col(\leqslant 2, *)$*?*

Решение.

Цикловой индекс действия O на вершины куба —

$$P(O \underset{\alpha}{:} V;\, x_1, \ldots x_8) = \frac{1}{24}\left[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2 x_3^2 \,\right].$$

1) $\#Col(2) = P(x_1,\dots,x_8)\Big|_{x_1=\dots=x_8=2} =$

$$= \frac{2^8 + 6\cdot 2^2 + 9\cdot 2^4 + 8\cdot 4\cdot 4}{3\cdot 2^3} = \frac{32+3+18+16}{3} = 23.$$

2) $w(\text{красный}) = y,\ w(\text{синий}) = 1,$
$x_k = y^k + 1,\ k = \overline{1,8}$:

$$\#Col(4,4) = \frac{1}{24}\big[\,(y+1)^8 + 9\cdot(y^2+1)^4 + 6\cdot(y^4+1)^2 + 8\cdot(y+1)^2(y^3+1)^2\,\big] =$$

$$= \frac{1}{24}\big[\,\dots + C_8^4 y^4 + \dots + 9(\dots 4y^2 + 6y^4 + \dots) + 6(\dots + 2y^4 + \dots) + 8(y^2+2y+1)(\dots + 2y^3 + \dots)\,\big].$$

$$u_4 = \frac{1}{24}\big[\,70 + 9\cdot 6 + 6\cdot 2 + 8\cdot 2\cdot 2\,\big] = \frac{168}{24} = 7.$$

3) $\#Col(\leqslant 2,*) = u_0 + u_1 + u_2$, очевидно $u_0 = u_1 = 1.$

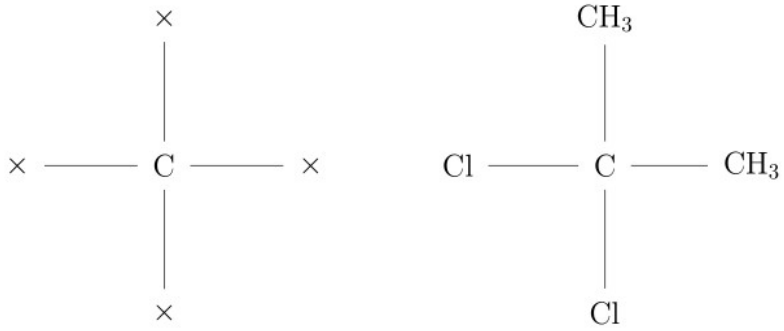
$$u_2 = \frac{1}{24}\big[\dots + 28y^2 + 9(\dots + 4y^2\dots) + 8(\dots + y^2 + \dots)\big] = \frac{28+36+8}{24} = 3.$$

$$\#Col(\leqslant 2,*) = 1 + 1 + 3 = 5.$$

Задача 4.7 (о числе молекул). *Рассмотрим молекулы 4-валентного углерода* C*: где на на месте* $\times$ *могут находится* CH_3 *(метил),* C_2H_5 *(этил),* H *(водород) или* Cl *(хлор). Например — дихлорбутан.*

Найти

1) *общее число* M *всех молекул;*



2) *число молекул с* $H = 0, 1, 2, 3, 4$ *атомами водорода.*

Решение. Какая группа действует и на каком множестве?
T на множестве вершин тетраэдра.
Находим цикловой индекс:

$g \in T$	$Type(g)$	$w(g)$	#
e	$\langle 4, 0, 0, 0 \rangle$	x_1^4	1
$t,\ t^2$	$\langle 1, 0, 1, 0 \rangle$	$x_1 x_3$	$4 \cdot 2 = 8$
f	$\langle 0, 2, 0, 0 \rangle$	x_2^2	3

$$P(T \underset{\alpha}{:} V) = \frac{1}{12}\left[x_1^4 + 8x_1x_3 + 3x_2^2 \right]$$

1. Всего M молекул (4 радикала, $x_1 = \ldots = x_4 = 4$):

$$M = P(x_1, \ldots, x_4) = \frac{4^4 + 8 \cdot 4 \cdot 4 + 3 \cdot 4^2}{3 \cdot 4} = 36.$$

2. Веса: $y_1 = \mathrm{H}$, $y_2 = y_3 = y_4 = 1$.
Подстановка в P: $x_k = \mathrm{H}^k + 3$, $k = \overline{1,4}$.

$P(H) =$

$$= \frac{1}{12}\left[(\mathrm{H}+3)^4 + 8\,(\mathrm{H}+3)\left(\mathrm{H}^3+3\right) + 3\left(\mathrm{H}^2+3\right)^2 \right] =$$
$$= \frac{1}{12}\left[\left(\mathrm{H}^4 + 4\cdot\mathrm{H}^3\cdot 3 + 6\cdot\mathrm{H}^2\cdot 9 + 4\cdot\mathrm{H}\cdot 27 + 81\right) + \right.$$
$$\left. +8\left(\mathrm{H}^4+3\mathrm{H}^3+3\mathrm{H}+9\right) + 3\left(\mathrm{H}^4+6\mathrm{H}^2+9\right) \right] =$$
$$= 1\cdot\mathrm{H}^4 + 3\cdot\mathrm{H}^3 + 6\cdot\mathrm{H}^2 + 11\cdot\mathrm{H} + 15.$$

Итого имеется молекул с числом атома водорода: с 4-мя — 1 шт., с 3-мя — 3 шт., с 2-мя — 6 шт., с 1-м — 11 шт., без атомов водорода — 15 шт., всего — $1+3+6+11+15 = 36$.

4.4 Задачи с решениями

Задача 4.8. *Найдите порядок стабилизаторов произвольной (а) вершины, (б) ребра, (в) грани куба при действии группы октаэдра O на соответствующие элементы.*
Какие перестановки в них содержатся?

Решение.

(а) Пусть O действует на вершины куба и v — некоторая вершина.
Тогда $\mathrm{Stab}\,(v) = \{\, e, s, s^2 \,\} \leqslant O$ — группа вращений на 120° (в выбранном направлении) вокруг диагонали куба, проходящей через данную вершину, $\mathrm{Stab}\,(v) \cong \mathbb{Z}_3$.

(б) Пусть O действует на рёбра куба и r — некоторое ребро.

Тогда $\mathrm{Stab}(r) = \{e, f\} \leqslant O$ — группа вращений на 180° вокруг оси, проходящей через середины рёбер (данного и ему противоположного) куба, $\mathrm{Stab}(r) \cong \mathbb{Z}_2$.

(в) Пусть O действует на грани куба и f — некоторая грань.
Тогда $\mathrm{Stab}(f) = \{e, t, t^2, t^3\} \leqslant O$ — группа вращений на 90° (в выбранном направлении) вокруг вокруг оси, проходящей через середины граней (данной и ей противоположной) куба, $\mathrm{Stab}(f) \cong \mathbb{Z}_4$.

Задача 4.9. *Найти цикловой индекс для следующим образом определённого самодействия четверной группы Клейна*
$V_4 = \{e, a, b, ab \mid a^2 = b^2 = (ab)^2 = e^2 = e,\ ab = ba\}$:

1.
$$e : \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}, \qquad a : \begin{pmatrix} e & a & b & ab \\ a & e & ab & b \end{pmatrix},$$
$$b : \begin{pmatrix} e & a & b & ab \\ b & ab & e & a \end{pmatrix}, \qquad ab : \begin{pmatrix} e & a & b & ab \\ ab & b & a & e \end{pmatrix};$$

2.
$$e : \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}, \qquad a : \begin{pmatrix} e & a & b & ab \\ a & e & b & ab \end{pmatrix},$$
$$b : \begin{pmatrix} e & a & b & ab \\ e & a & ab & b \end{pmatrix}, \qquad ab : \begin{pmatrix} e & a & b & ab \\ a & e & ab & b \end{pmatrix}.$$

Решение. Везде группа Клейна V_4 действует на свои же элементы.

1)

g	$Type(g)$	$w(g)$	#
e	$\langle\, \underline{4},\, 0,\, 0,\, 0 \,\rangle$	x_1^4	1
$a,\, b,\, ab$	$\langle\, 0,\, 2,\, 0,\, 0 \,\rangle$	x_2^2	3

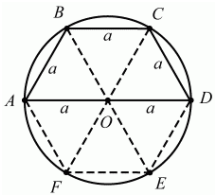
$$P_{V_4} \;=\; \frac{1}{4}\left[\, x_1^4 + 3x_2^2 \,\right].$$

2)

g	$Type(g)$	$w(g)$	#
e	$\langle\, \underline{4},\, 0,\, 0,\, 0 \,\rangle$	x_1^4	1
$a,\, b$	$\langle\, \underline{2},\, 1,\, 0,\, 0 \,\rangle$	$x_1^2 x_2$	2
ab	$\langle\, 0,\, 1,\, 0,\, 0 \,\rangle$	x_2	1

$$P'_{V_4} \;=\; \frac{1}{4}\left[\, x_1^4 + 2x_1^2 x_2 + x_2 \,\right].$$

Задача 4.10. *Найти цикловой индекс транзитивного самодействия группы* $\mathbb{Z}_6$.



Решение. Обозначим последовательно вершины правильного шестиугольника буквами $A, \ldots, F$, $\mathbb{Z}_6 = \langle t \rangle$, t — поворот на $60°$.

$g \in \mathbb{Z}_6$	$Type(g)$	$w(g)$
$e = (A)\ldots(F)$	$\langle\, 6,\, 0,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_1^6
$g = (ABCDEF)$	$\langle\, 0,\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_6
$g^2 = (ACE)(BDF)$	$\langle\, 0,\, 0,\, 2,\, 0,\, 0,\, 0 \,\rangle$	x_3^2
$g^3 = (AD)(BE)(CF)$	$\langle\, 0,\, 3,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_2^3
$g^4 = (AEC)(BFD)$	$\langle\, 0,\, 0,\, 2,\, 0,\, 0,\, 0 \,\rangle$	x_3^2
$g^5 = (AFEDCB)$	$\langle\, 0,\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_6

$$P_{\mathbb{Z}_6} = \frac{1}{6}\left[\, x_1^6 + x_2^3 + 2x_3^2 + 2x_6 \,\right] = \frac{1}{6}\sum_{d|6} \varphi(d)\, x_d^{6/d};$$

$$D(6) = \{\, 1, 2, 3, 6 \,\},\ \varphi(1) = \varphi(2) = 1,\ \varphi(3) = \varphi(6) = 2.$$

Задача 4.11. *На стеклянных пластинах рисуют одинаковые прямоугольники (не квадраты) и раскрашивают их стороны в r цветов.*

Сколько можно нарисовать таких различных прямоугольников? Конкретно, при $r = 2$?

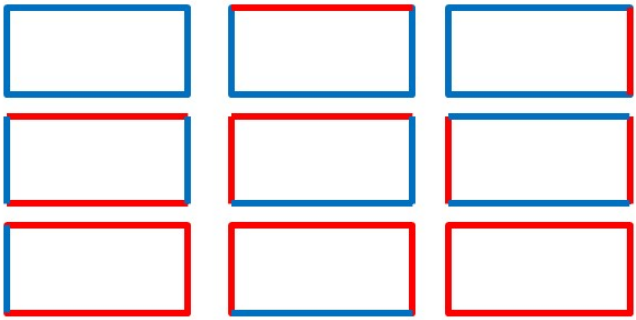
Решение. Найдём цикловой индекс $R \underset{\alpha}{:} S$ действия группы R самосовмещений прямоугольника в пространстве на его стороны. Группа $R = \langle\, t,\, f \,\rangle$ порождается образующими: t — вращение вокруг центра симметрии на $180°$, f — отражение вокруг оси, проходящей через середины противоположных сторон, 2 оси.

$g \in R$	$Type(g)$	$w(g)$	#
e	$\langle\, 4,\, 0,\, 0,\, 0 \,\rangle$	x_1^4	1
t	$\langle\, 0,\, 2,\, 0,\, 0 \,\rangle$	x_2^2	1
f	$\langle\, 2,\, 1,\, 0,\, 0 \,\rangle$	$x_1^2 x_2$	2

$$P(R \underset{\alpha}{:} S;\, x_1,\, x_2,\, x_3,\, x_4) = \frac{1}{4}\left[\, x_1^4 + x_2^2 + 2x_1^2 x_2 \,\right].$$

Число 2-цветных прямоугольников —

$$\#Col(2) = P(R \underset{\alpha}{:} S; 2, \ldots, 2) = \frac{16 + 4 + 16}{4} = 9$$



Задача 4.12. *На стеклянных пластинах рисуют одинаковые прямоугольники (не квадраты) и раскрашивают их вершины в* 3 *цвета.*

Сколько можно нарисовать таких различных прямоугольников?

Решение. Найдём цикловой индекс $P(R \underset{\alpha}{:} V)$ действия группы R самосовмещений прямоугольника в пространстве на его вершины.

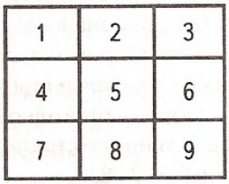
$g \in R$	$Type(g)$	$w(g)$	#
e	$\langle\, 4,\, 0,\, 0,\, 0 \,\rangle$	x_1^4	1
t	$\langle\, 0,\, 2,\, 0,\, 0 \,\rangle$	x_2^2	1
f	$\langle\, 0,\, 2,\, 0,\, 0 \,\rangle$	x_2^2	2

$$P(R \underset{\alpha}{:} V;\, x_1,\, x_2,\, x_3,\, x_4) \;=\; \frac{1}{4}\left[\, x_1^4 + 3x_2^2 \,\right]$$

Число прямоугольников:

$$\#Col(3) \;=\; P(R \underset{\alpha}{:} V; 3, \ldots, 3) \;=\; \frac{81+27}{4} \;=\; 27$$

Задача 4.13. *Квадратная стеклянная пластина разделена на 9 равных квадратов, которые раскрашиваются в один из 2 цветов.*
Сколько существует разноокрашенных пластин?



Решение. На множество T из $N = 9$ квадратов стеклянной пластики действует группа $D_4 = \langle t, f, s \rangle$, $t^4 = f^2 = s^2 = e$, где

t — вращение на 90° вокруг центра квадрата;

f — симметрия относительное прямой, проходящей через середины противоположных сторон;

s — симметрия относительное прямой, проходящей через противоположные вершин.

Определяем цикловой индекс действия D_4 на T.

$g \in D_4$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(9)$	$\langle 9, 0, \dots \rangle$	x_1^9	1
t, t^3	$(5)(1397)(2684)$	$\langle 1, 0, 0, 2, \dots \rangle$	$x_1 x_4^2$	2
t^2	$(5)(19)(37)(28)(79)$	$\langle 1, 4, 0, \dots \rangle$	$x_1 x_2^4$	1
$s, f, \dots$	$(2)(5)(8)(13)(48)(79)$	$\langle 3, 3, 0, \dots \rangle$	$x_1^3 x_2^3$	4
Всего				8

Цикловой индекс: $P = \dfrac{1}{8}\left[x_1^9 + 2x_1x_4^2 + x_1x_2^4 + 4x_1^3x_2^3\right]$.

$$\#Col(2) = \frac{2^9 + 2 \cdot 2^3 + 2^5 + 4 \cdot 2^3 \cdot 2^3}{2^3} = 102.$$

Задача 4.14 (о компостере). *Компостером назовём квадратную таблицу 4×4, в которой каждая клетка может быть либо пустой, либо содержать в центре символ* $\bullet$.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Сколько существует различных компостеров, если не различать те, которые могут быть получены один из другого самосовмещениями в пространстве?

Решение. Найдём цикловой индекс действия группы диэдра D_4 на 16 клеток компостера.
$D_4 = \langle t, f, s \rangle$, $t^4 = f^2 = s^2 = e$, $|D_4| = 8$,

$g \in D_4$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(16)$	$\langle 16, 0, \dots \rangle$	x_1^4	1
$t,\ t^3$	$(1,4,16,13)\dots(6,7,11,10)$	$\langle 0, 0, 0, 4, \dots \rangle$	x_4^4	2
t^2	$(1,16)\dots(6,11)$	$\langle 0, 8, 0 \dots \rangle$	x_2^8	1
f	$(1,4)\dots(10,11)$	$\langle 0, 8, 0, \dots \rangle$	x_2^8	2
s	$(1)\dots(16)(2,5)\dots(12,15)$	$\langle 4, 6, 0, \dots \rangle$	$x_1^4 x_2^6$	2

Цикловой индекс действия группы D_4 на элементы компостера:

$$P(x_1, \dots, x_4) = \frac{1}{8}\left[\, x_1^{16} + 2x_4^4 + 3x_2^8 + 2x_1^4 x_2^6 \,\right].$$

Наличие/отсутствие в клетке символа $\bullet$ описывается их отображением в двухэлементное множество (раскраске в два цвета), поэтому число различных компостеров есть $P(2, 2, \dots) =$

$$= \frac{1}{8}\left[\, 2^{16} + 2 \cdot 2^4 + 3 \cdot 2^8 + 2 \cdot 2^4 \cdot 2^6 \,\right] = 8548.$$

К аналогичной задаче сводится задача о числе фотошаблонов рисунков соединений для интегральных схем.

Задача 4.15. *Найти число различных вариантов раскраски граней куба в 2 и 3 цвета.*

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} F) = \frac{1}{24}\left[x_1^6 + \underline{6x_1^2x_4} + 3x_1^2x_2^2 + \underline{6x_2^3} + 8x_3^2\right].$$

$$\#Col(2) = \frac{2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 2^5}{3\cdot 2^3} = 10.$$

$$\#Col(3) = \frac{3^6 + 12\cdot 3^3 + \cdot 3^5 + 8\cdot 3^2}{3\cdot 8} = 57.$$

Задача 4.16. *Определить число различных раскрасок всех граней правильной 4-угольной пирамиды П в 3 цвета.*

Решение. Занумеруем последовательно боковые грани П числами $1, \ldots 4$, а основание — 5.
$G \cong \mathbb{Z}_4 = \langle t \rangle$, t — вращение на $90°$.

$g \in \mathbb{Z}_4$	$Type(g)$	$w(g)$	#
$e = (1)(2)(3)(4)(5)$	$\langle 5, 0, 0, 0, 0 \rangle$	x_1^5	1
$t, t^3 = (1234)(5)$	$\langle 1, 0, 0, 1, 0 \rangle$	x_1x_4	2
$t^2 = (12)(34)(5)$	$\langle 1, 2, 0, 0, 0 \rangle$	$x_1x_2^2$	1

$$P(x_1, \ldots, x_5) = \frac{1}{4}\left[x_1^5 + 2x_1x_4 + x_1x_2^2\right],$$

$$P(3, \ldots, 3) = \frac{3^5 + 2\cdot 3^2 + 3^3}{4} = \frac{9\cdot 32}{4} = 72.$$

Задача 4.17. *Найти число раскрасок всех граней усечённой правильной 4-угольной пирамиды в 3 цвета.*

Решение. Пронумеруем грани П: боковые — с 1 по 4 по часовой стрелке, основания — 5 и 6. Группа, действующая на П — $\mathbb{Z}_4 = \langle t \rangle$, t — поворот на 90° по часовой стрелке.

$g \in \mathbb{Z}_4$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(6)$	$\langle 6, 0, \dots \rangle$	x_1^6	1
t, t^3	$(1234)(5)(6)$	$\langle 2, 0, 0, 1, 0, 0 \rangle$	$x_1^2 x_4$	2
t^2	$(12)(34)(5)(6)$	$\langle 2, 2, 0, \dots \rangle$	$x_1^2 x_2^2$	1

Цикловой индекс $P = \dfrac{1}{4}\left[x_1^6 + 2x_1^2 x_4 + x_1^2 x_2^2\right]$.

$$\#Col(3) = \frac{3^6 + 2 \cdot 3^2 + 3^4}{4} = \frac{3^3(27 + 2 + 3)}{4} = 216.$$

Задача 4.18. *Найти число различных вариантов раскраски граней тетраэдра в 2 и 3 цвета.*

Решение. $P(T \underset{\alpha}{:} F, x_1, \dots, x_4) = \dfrac{1}{12}\left[x_1^4 + 8x_1x_3 + 3x_2^2\right]$.

$$\#Col(2) = \frac{2^4 + 11 \cdot 2^2}{3 \cdot 2^2} = \frac{4 + 11}{3} = 5\,.$$

$$\#Col(3) = \frac{3^4 + 11 \cdot 3^2}{3 \cdot 4} = \frac{27 + 33}{4} = \frac{60}{4} = 15.$$

Задача 4.19. *Найти число различных вариантов раскраски рёбер тетраэдра в 2 и 3 цвета.*

Решение. Группа $T = \langle t, f \rangle$, $t^3 = f^2 = e$, $|T| = 12$, где

t — вращение на $120°$ вокруг оси, проходящей через вершину и центр симметрии, 4 оси;

f — вращение на $180°$ вокруг оси, проходящей через середины противоположных рёбер, 3 оси.

Обозначим через E множество рёбер тетраэдра — $|E| = 6$ — и обозначим их цифрами от 1 до 6, считая, что рёбра 1, 2 и 3 инцидентны одной вершине, а ось вращения, задаваемого элементом f, проходит через середины рёбер 1 и 6.
Найдём цикловой индекс.

$g \in T$	$Type(g)$	$w(g)$	#
$e = (1)\dots(6)$	$\langle 6, 0, \dots \rangle$	x_1^6	1
$t, t^2 = (123)(456)$	$\langle 0, 0, 2, 0, \dots \rangle$	x_3^2	8
$f = (1)(23)(45)(6)$	$\langle 2, 2, 0, \dots \rangle$	$x_1^2 x_2^2$	3

$$P(T \underset{\alpha}{:} E, x_1, \dots, x_6) = \frac{1}{12}\left[x_1^6 + 8x_3^2 + 3x_1^2x_2^2\right].$$

$$\#Col(2) = \frac{2^6 + 8 \cdot 2^2 + 3 \cdot 2^4}{3 \cdot 2^2} = \frac{15 + 9 + 12}{3} = 12,$$

$$\#Col(3) = \frac{3^6 + 8 \cdot 3^2 + 3 \cdot 3^4}{3 \cdot 4} = 87.$$

Задача 4.20. *Найти число различных вариантов раскраски рёбер куба в 2 цвета.*

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} R) \;=\; \frac{1}{24}\left[\, x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4 \,\right].$$

$$\#Col(2) \;=\; \frac{2^{12} + 6\cdot 2^3 + 3\cdot 2^6 + 7\cdot 2^7}{3\cdot 2^3} \;=\; 218.$$

Задача 4.21. *Найти число различных вариантов раскраски вершин куба в* 2 *и* 3 *цвета.*

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} V) \;=\; \frac{1}{24}\left[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\right].$$

$$\#Col(2) \;=\; \frac{1}{3\cdot 2^3}\left[\, 2^8 + 6\cdot 2^2 + 9\cdot 2^4 + 2^7 \,\right] \;=\; 23,$$

$$\#Col(3) \;=\; \frac{1}{3\cdot 8}\left[\, 3^8 + 6\cdot 3^2 + 9\cdot 3^4 + 8\cdot 3^4 \,\right] \;=\; 333.$$

Задача 4.22. *Назовём две булевы функции* f_1 *и* f_2 *от* n *переменных подобными, если при подходящей перестановке* $(i_1, \ldots, i_n)$ *индексов* $(1, \ldots, n)$ *окажется, что*

$$f_1(x_1, \ldots, x_n) \;=\; f_1(x_{i_1}, \ldots, x_{i_n})$$

для всех $(x_1, \ldots, x_n) \in B^n$.

Определить, сколько имеется существенно различных (т. е. неподобных) таких функций.

История. Эта задача для $n = 4$ была решена численно в 1951 г. с помощью компьютерной программы, осуществившей перебор $2^{2^4} = 65\,536$ функций.

Решение. Задача, однако, допускает прямое решение. Здесь $G = S_n$, но она действует не на $\{1, \ldots, n\}$ а на B^n.

Для $n = 4$ результат действия, например, подстановки $g = (1,2)(3,4)$ на четвёрку $(a,b,c,d) \in B^4$ есть (b,a,d,c).

Очевидно, $\mathrm{Fix}\,(g)$ состоит из тех функций, которые постоянны на области действия каждого цикла из g. В нашем случае, например, для $g = (1,2)(3,4)$ получаем $|\,\mathrm{Fix}\,(g)| = 2 \cdot 2 = 4$.

Группа S_4 разбивается на следующие классы сопряжённости:

1) id;
2) шесть 2-циклов — $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$;
3) три произведения по два 2-цикла — $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$;
4) восемь 3-циклов — $(1)(2,3,4)$, $(1)(2,4,3)$, ...;
5) шесть 4-циклов — $(1,2,3,4)$, $(1,3,2,4)$, ...

Подстановка id (1) фиксирует все 16 четвёрок (a,b,c,d), $a,b,c,d \in \{0,1\}$, определяя моном x_1^{16} в цикловом индексе.

Далее, (2) даёт $6x_1^8x_2^4$, т. к., например, $(1,2)$ порождает четыре 2-цикла $(\,(0,1,c,d),(1,0,c,d)\,)$ на B^4 и фиксирует все четвёрки $(0,0,c,d)$ и $(1,1,c,d)$, порождая восемь 1-циклов, и т.д.

Многочлен цикловых индексов группы G, действующий на B^4, имеет вид

$$P(G) \;=\; \frac{1}{24}\,\left[x_1^{16} + 6x_1^8x_2^4 + 3x_1^4x_2^6 + 8x_1^4x_3^4 + 6x_1^2x_2x_4^3\right].$$

Подставляя $x_1 = \ldots = x_4 = 2$, получаем 3 984 класса подобных булевых функций от 4-х переменных.

Замечание. Если к группе G добавить взятие дополнения как новую симметрию (т. е. считать, что $f_1(x_1, \ldots, x_n) = f_2(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) \;\Rightarrow\; f_1 \sim f_2,\; \sigma_i \in \{0, 1\}$) то искомым числом (классов Шеннона-Поварова) вместо 3 984 будет 222.

Задача 4.23. *Сколькими геометрически различными способами три абсолютно одинаковые мухи могут усесться в вершинах правильного семиугольника, нарисованного на листе бумаги?*

Решение. Множество T — вершины семиугольника, на которые действует группа $\mathbb{Z}_7 = \langle\, t \,\rangle,\; t^7 = e$.

$g \in \mathbb{Z}_7$	$Type(g)$	$w(g)$	#
e	$\langle\, 7,\, 0,\, \ldots \,\rangle$	x_1^7	1
$t,\, t^2,\, \ldots,\, t^6$	$\langle\, 0,\, \ldots,\, 0,\, 1 \,\rangle$	x_7	6

Цикловой индекс самодействия $\mathbb{Z}_7$:

$$P_{\mathbb{Z}_7}(x_1,\, \ldots,\, x_7) \;=\; \frac{1}{7}\,\left[\, x_1^7 + 6x_7 \,\right] \;=\; \frac{1}{7}\sum_{d|7} \varphi(d)\, x_d^{7/d}.$$

Число различных раскрасок в 2 цвета (муха есть/нет), при условии окраски ровно 3 вершин из 7 есть коэффициент u_3 при y^3 после подстановки
$x_1 \mapsto y + 1,\; x_7 \mapsto y^7 + 1$ в $P_{\mathbb{Z}_7}$:

$$P(y) \;=\; \frac{1}{7}\,\left[\, (y+1)^7 + 6(y+1) \,\right] \;=\; \frac{1}{7}\,\left[\, \ldots + C_7^3 y^3 + \ldots \,\right].$$

$$u_3 = \frac{7!}{7 \cdot 3! \cdot 4!} = \frac{5 \cdot 6}{2 \cdot 3} = 5.$$

Задача 4.24. *Боковые грани правильной* 6*-угольной пирамиды окрашиваются в красный, синий и зелёный цвета. Определить*

(а) *число различных* 2*- и* 3*-цветных пирамид;*

(б) *число пирамид с одной красной гранью;*

(в) *число пирамид, у которых не менее трёх красных граней.*

Решение. Имеем транзитивное самодействие $\mathbb{Z}_6$.

(а) *Общее число пирамид.*

$$P(\mathbb{Z}_6) = \frac{1}{6} \sum_{d|6} \varphi(d)\, x_d^{6/d} = \frac{1}{6} \left[x_1^6 + x_2^3 + 2x_3^2 + 2x_6 \right].$$

$$\#Col(2) = \frac{1}{2 \cdot 3} \left[2^6 + 2^3 + 2 \cdot 2^2 + 2 \cdot 2 \right] = \frac{4 \cdot 21}{3} = 14.$$

$$\#Col(3) = \frac{1}{6} \left[3^6 + 3^3 + 2 \cdot 3^2 + 2 \cdot 3 \right] = \frac{780}{6} = 130.$$

(б, в) *Число пирамид с* 1 *и* $3 \leqslant$ *красными гранями.* Полагаем $y_1 = y$, $y_2 = y_3 = 1$ (следим только за красными гранями), $x_1 = y + 2$, $x_2 = y^2 + 2$, $x_3 = y^3 + 2$.

$$P(y) = \frac{1}{6} \left[(y+2)^6 + (y^2+2)^3 + 2(y^3+2)^2 + \right.$$
$$\left. + 2(y^6+2) \right] = \frac{1}{6} \left[u_0 + u_1 y + u_2 y^2 + \ldots + u_6 y^6 \right] =$$

$$= \frac{1}{6}\left[\left(2^6+2^3+2^3+4\right)+6\cdot 2^5\,y+ \right.$$
$$\left. +\left(16\cdot 15+2\cdot 3\cdot 2^2\right)\,y^2+\ldots\right].$$

$u_0 = 84/6 = 14$, $u_1 = 2^5 = 32$, $u_2 = (240{+}24)/6 = 44$.

Число пирамид с:

(б) одной красной гранью — $u_1 = 32$,

(в) не менее, чем 3 красными гранями — $\#Col(3) - (u_0+u_1+u_2) = 130-(14+32+44) = 130-90 = 40$.

Задача 4.25. *Имеются плоские бусины, окрашенные с одной стороны в красный, синий и зелёный цвета. Из них составляют ожерелья, содержащие по 8 в равноотстоящих точках окружности. Определить*

а) *число различных 3-цветных ожерелий;*

б) *число ожерелий, у которых не менее трёх красных бусин?*

Решение. Здесь везде — транзитивное самодействие циклической группы $\mathbb{Z}_8$.

$D(8) = \{1, 2, 4, 8\}$, $\varphi(1) = \varphi(2) = 1$, $\varphi(4) = 2$, $\varphi(8) = 4$,

$$P(\mathbb{Z}_8) = \frac{1}{8}\sum_{d|8}\varphi(d)\,x_d^{8/d} = \frac{1}{8}\left[\,x_1^8+x_2^4+2x_4^2+4x_8\,\right].$$

а) *Общее число ожерелий*:

$$\#Col(3) = \frac{3^8+3^4+2\cdot 9+4\cdot 3}{8} = 834.$$

б) Подсчитаем *число X ожерелий, в которых число красных бусин не более* 3 (т. е. 0, 1 и 2) и вычтем полученное количество из 834.

Полагаем $y_1 = y,\ y_2 = y_3 = 1$ (следим только за бусинами красного цвета).

Найдём коэффициенты u_0, u_1, u_2 при y_0, y_1, y_2 в производящем многочлене W при подстановке $x_k = y^k + 2,\ k = 1, \ldots, 8$.

$$P(\mathbb{Z}_8) = \frac{1}{8}\left[\, x_1^8 + x_2^4 + 2x_4^2 + 4x_8 \,\right]$$

$$W = \frac{1}{8}\left[\, (y+2)^8 + (y^2+2)^4 + 2(y^4+2)^2 + 4(y^8+2) \,\right] =$$
$$= u_0 + u_1 y + u_2 y^2 + \ldots + u_8 y^8 =$$
$$= \frac{1}{2^3}\left[\, (2^8 + 2^4 + 2\cdot 2^2 + 8) + 8\cdot 2^7 y + \right.$$
$$\left. + (C_8^2 \cdot 2^6 + 4\cdot 2^3)\, y^2 + \ldots \,\right].$$
$$u_0 = 2^5 + 2 + 1 + 1 = 36, \qquad u_1 = 128,$$
$$u_2 = 28\cdot 8 + 4 = 224 + 4 = 228.$$

Отсюда
$$\#Col(3 \leqslant) = 834 - (36 + 128 + 228) = 834 - 392 = 442.$$

Задача 4.26. *Грани куба раскрашивают в два цвета — красный и синий. Сколько существует кубов*

1) *различно окрашенных?*
2) *у которых не менее 4 граней красные* – $\#Col(\geqslant 4)$*?*

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} F) = \frac{1}{3\cdot 2^3}\left[\, x_1^6 + \underline{6x_1^2 x_4} + 3x_1^2 x_2^2 + \underline{6x_2^3} + 8x_3^2 \right].$$

$$1)\ \#Col(2) = \frac{2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 2^5}{3\cdot 2^3} = \frac{30}{3} = 10.$$

2) Полагаем
$w(1) = y,\ w(2) = 1,\ x_k = y^k + 1,\ k = \overline{1,6}.$

$$W = \frac{1}{24}\left[\,(y+1)^6 + 6(y+1)^2(y^4+1) + \right.$$
$$\left. + 3(y+1)^2(y^2+1)^2 + 6(y^2+1)^3 + 8(y^3+1)^2\,\right].$$

$\#Col(\geqslant 4) = u_4 + u_5 + u_6$ — число кубов с 4, 5 и 6 красными гранями соответственно. Очевидно $u_5 = u_6 = 1$.

Раскрывая W, находим:

$$W = \frac{1}{24}\left[\,\ldots + C_6^4 y^4 + \ldots + 6(y^2+2y+1)(\underline{y^4}+1) + \right.$$
$$+3(\underline{y^2}+2y+1)(\underline{y^4}+2\underline{y^2}+1) +$$
$$\left. +6(y^6+3\underline{y^4}+3y^2+1) + 8(y^6+2y^3+1)\,\right].$$

$$u_4 = \frac{15+6+9+18}{3\cdot 8} = \frac{5+2+3+6}{8} = \frac{16}{8} = 2.$$

Итого $\#Col(\geqslant 4) = 1+1+2 = 4$.

Задача 4.27. *Для раскраски сторон квадрата на стеклянной пластинке используют 3 цвета — красный, синий и зелёный. Сколько можно получить*

1) *разнораскрашенных квадратов?*
2) *квадратов с 1 красным ребром и не более 2 синих?*

Решение. Цикловой индекс:

$$P(D_4) = \frac{1}{8}\left[\,x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2x_2\,\right]$$

1) $\#Col(3) = \frac{1}{8}\left[3^4 + 2\cdot 3 + 3\cdot 3^2 + 2\cdot 3^2\cdot 3\right] = 21.$

2) При раскраске в 3 цвета: $x_k = y_1^k + y_2^k + y_3^k$, $k = \overline{1,4}$. Следим только за красным (y_1) и синим (y_2) цветами: $x_k = y_1^k + y_2^k + 1$, $k = \overline{1,4}$. Находим $u_{10} + u_{11} + u_{12}$.

$$W = \frac{1}{8}\left[(y_1 + (y_2+1))^4 + 2(y_1^4 + y_2^4 + 1) + \right.$$
$$\left. + 3(y_1^2 + (y_2^2+1))^2 + 2(y_1 + (y_2+1))^2(y_1^2 + y_2^2 + 1)\right] =$$

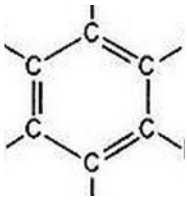
нас интересуют только члены с y_1^1 (одно красное ребро)

$$\frac{1}{8}\left[y_1^4 + 4y_1^3(y_2+1) + 6y_1^2(y_2+1)^2 + \underline{4y_1(y_2+1)^3} + \right.$$
$$+ (y_2+1) + \ldots$$
$$\left. + 2(y_1^2 + \underline{2y_1(y_2+1)} + (y_2+1)^2)(y_1^2 + y_2^2 + 1)\right] =$$
$$= \frac{1}{8}\left[\ldots + 4y_1(y_2+1)^3 + 4y_1(y_2+1)(y_2^2+1))\right] =$$
$$= \frac{1}{8}\left[\ldots + 4y_1(y_2^3 + \underline{3y_2^2 + 3y_2^1 + 1}) + \right.$$
$$\left. + 4y_1(y_2^3 + \underline{y_2 + y_2^2 + 1})\right] =$$

нас интересуют только члены с y_2^0, y_2^1 и y_2^2 при y_1 (синих рёбер — 0, 1, 2)

$$= \frac{1}{8}\left[4\cdot 7 + 4\cdot 3\right] = \frac{4\cdot 10}{8} = 5.$$

Задача 4.28. *Присоединяя к свободным связям углерода бензольного кольца атомы водорода* H *или метил* CH_3, *можно получить молекулы разных веществ (ксилол, бензол и др.).*



1) *Сколько химически разных молекул можно получить таким путём?*

2) *Сколько из них молекул с присоединёнными* $0, \ldots, 6$ *атомами водорода?*

Решение. Самодействие группы диэдра D_6.
1) Имеем $D_6 = \langle t, f, s \rangle$, $t^4 = f^2 = s^2 = e$, $|D_6| = 12$ — группа диэдра порядка 6, где

t — вращение на 60° вокруг центра квадрата;

f — симметрия относительное прямой, проходящей через середины противоположных сторон (3 оси);

s — симметрия относительное прямой, проходящей через противоположные вершин (3 оси).

Пронумеруем последовательно вершины правильного 6-угольника $1, \ldots, 6$.

Перестановки ниже указаны для случая, когда ось f проходит через середины сторон (2-3) и (5-6), а ось s — через вершины 1 и 4.

$g \in D_6$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(6)$	$\langle\, 6,\, 0,\, \dots\, 0 \,\rangle$	x_1^6	1
t, t^5	(123456)	$\langle\, 0,\, \dots,\, 0,\, 1 \,\rangle$	x_6^1	2
t^2, t^4	$(135)(246)$	$\langle\, 0,\, 0,\, 2, \dots\, 0 \,\rangle$	x_3^2	2
t^3	$(14)(25)(36)$	$\langle\, 0,\, 3,\, 0, \dots\, 0 \,\rangle$	x_2^3	1
f	$(14)(23)(56)$	$\langle\, 0,\, 3,\, 0,\, \dots\, 0 \,\rangle$	x_3^2	3
s	$(1)(4)(26)(35)$	$\langle\, 2,\, 2,\, 0,\, \dots \,\rangle$	$x_1^2 x_2^2$	3
Всего				12

$$P(D_6) \,=\, \frac{1}{12}\left[\, x_1^6 + 2x_6 + 2x_3^2 + 4x_2^3 + 3x_1^2 x_2^2 \,\right].$$

Всего молекул — подстановка $x_1 = \dots = x_6 = 2$ (водород H и метил CH_3):

$$M \,=\, \frac{64 + 4 + 8 + 32 + 3 \cdot 16}{3 \cdot 4} \,=\, \frac{39}{3} \,=\, 13.$$

2) *Число молекул с* $0, \dots, 6$ *атомами водорода* — обозначение $y_1 = \mathrm{H}$, $y_2 = 1$ и подстановка $x_k = \mathrm{H}^k + 1$, $k = \overline{1,6}$ в P.

$$\begin{aligned} W \,=\, \frac{1}{12}\big[\, &(\mathrm{H}+1)^6 + 3(\mathrm{H}+1)^2(\mathrm{H}^2+1)^2 + 4(\mathrm{H}^2+1)^3 + \\ &+ 2(\mathrm{H}^3+1)^2 + 2(\mathrm{H}^6+1)\,\big] \,= \\ &= \mathrm{H}^6 + \mathrm{H}^5 + 3\cdot\mathrm{H}^4 + 3\cdot\mathrm{H}^3 + 3\cdot\mathrm{H}^2 + \mathrm{H} + 1\,. \end{aligned}$$

Итого: молекул с числом атомов водорода (как радикала) — $\mathrm{H} = 0,\, 1,\, 5$ и 6 — по 1 шт., $\mathrm{H} = 2,\, 3$ и 4 — по 3 шт., всего — 13.

Задача 4.29. *Сколько существует ожерелий из 6 красных и 12 синих бусин?*

Решение. Цикловой индекс самодействия группы диэдра (было ранее)

$$P(D_n) = \frac{1}{2n}\sum_{d|n}\varphi(d)\,x_d^{n/d} + \\ + \begin{cases} \frac{1}{2}x_1 x_2^{(n-1)/2}, & n \text{ нечётно}, \\ \frac{1}{4}\left[x_2^{n/2} + x_1^2 x_2^{n/2-1}\right], & n \text{ чётно}, \end{cases}$$

$n = 6 + 12 = 18,\ D(18) = \{1, 2, 3, 6, 9, 18\},$

$$\varphi(1) = 1, \qquad \varphi(3) = 2, \qquad \varphi(9) = 6,$$
$$\varphi(2) = 1, \qquad \varphi(6) = 2, \qquad \varphi(18) = 6.$$

По формуле: $P(D_{18}) =$

$$= \frac{1}{36}\left[x_1^{18} + x_2^9 + 2x_3^6 + 2x_6^3 + 6x_9^2 + 6x_{18}^1\right] + \\ + \frac{1}{4}\left[x_2^9 + x_1^2 x_2^8\right] = \\ = \frac{1}{36}\left[x_1^{18} + 10x_2^9 + 2x_3^6 + 2x_6^3 + 6x_9^2 + 6x_{18}^1 + 9x_1^2 x_2^8\right].$$

$x_k = y^k + 1, \quad W = \frac{1}{36}\left[(y+1)^{18} + \right.$

$$+ 10(y^2+1)^9 + 2(y^3+1)^6 + 2(y^6+1)^3 + \\ \left. + 6(y^9+1)^2 + 6(y^{18}+1) + 9(y+1)^2(y^8+1)^8\right] =$$

$$= \frac{1}{36}\left[\ldots + \left(C_{18}^6 + 10C_9^3 + 2C_3^1 + 2C_6^2 + 0 + 0 + \right.\right.$$
$$\left.\left. + 9(C_8^2 + C_8^3)\right) y^6\right] =$$
$$= \frac{1}{36}\left[\ldots + (18654 + 840 + 6 + 30 + 756)\, y^6\right] =$$
$$= 561\, y^6. \qquad \textit{Ответ.}\ 561.$$

Задача 4.30. *Найти число раскрасок куба в красный и синий цвета с 5 красными рёбрами.*

Решение. Ранее был найден цикловой индекс действия группы O на рёбра куба:

$$P(O \underset{\alpha}{:} R) = \frac{1}{24}\left[x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4\right].$$

$y_k = x^k + 1$,

$$W = \frac{1}{24}\left[(y+1)^{12} + 6(y^4+1)^3 + 3(y^2+1)^6 + \right.$$
$$\left. + 6(y+1)^2(y^2+1)^5 + 8(y^3+1)^4\right] =$$
$$= \frac{1}{24}\left[\ldots + \left(C_{12}^5 + 6C_2^1C_5^2\right) y^5\right] =$$
$$= \frac{1}{24}\left[\ldots + (792 + 6\cdot 2\cdot 10)\, y^5\right] = \ldots + \frac{792+120}{24} y^5 =$$
$$= \ldots + (33+5)\, y^5 = \ldots + 38\, y^5.$$

Ответ: 38.