Конспект лекций по курсу

ПРИКЛАДНАЯ АЛГЕБРА

группы 320–328 (III поток)
осенний семестр 2016/17 уч. года

Лектор *С. И. Гуров*

ассистент *Д. А. Кропотов*

(кафедра *Математических методов прогнозирования*)

2017

Предисловие

... а иногда потому так пространно писали, что если тебе не разъяснить, то от тебя и ответа не получишь.

Иван Грозный. Из послания шведскому королю Юхану III.

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 содержит, в основном, лишь формулировки определений и теорем (возможно, с доказательствами), которые в учебнике претворяются пояснениями, часто включающие фактический материал 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:

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

Пример 1.2.

1. *Числовые группы* — все они абелевы:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно *сложения*.
- *Ненулевые* элементы $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно *умножения*; 1 — нуль группы.

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 $\{t_1, t_2, \ldots, t_k\}$.

Например, для предыдущей композиции перестановок:

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

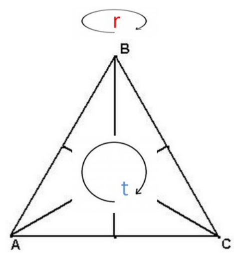
4. *Группы симметрии (самосовмещений) объекта — совокупность преобразований, совмещающих объект с самим собой.*

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

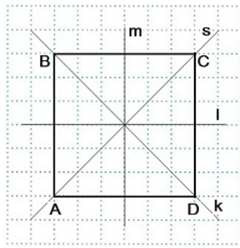
$$D_3 = \langle t, r \rangle = \{ e, (ABC), (ACB), (A)(BC), (B)(AC), (C)(AB) \} = S_3.$$



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

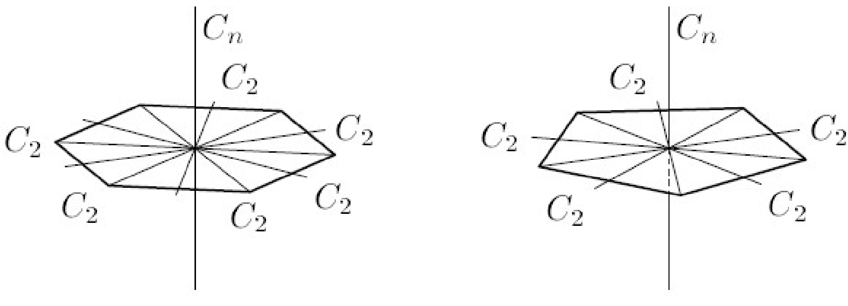


$$D_4 = \langle t, r, f \rangle = \{ e, (ABCD), (AC)(BD), (ADCB), (AD)(BC), (AB)(CD), (BD), (AC) \}.$$

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 $t^m r^n f^k$.

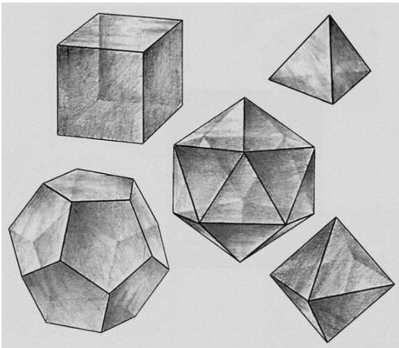
Пример: группы диэдра D_6 и D_5.



$|D_n| = 2n$: 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 —

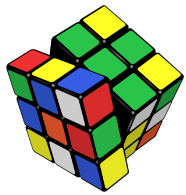


T — группа тетраэдра,

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

$$(aH) \circ (bH) = abH.$$

называется *факторгруппой*, символически G/H[1].

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 операцию:

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

[1] Легко видеть, что, поскольку H — нормальная, введённое умножение не зависит от выбора элементов в классах смежности и именно поэтому G/H оказывается группой.

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 $\left\langle \frac{2\pi}{n} \right\rangle$ вращений в плоскости вокруг центра правильного n-угольника, совмещающих его с собой.

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

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

   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 нетривиальная 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* $\mathbb{Z}$.

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

<u>Определение</u> 1.4. Значение *функции Эйлера* $\varphi(n)$ — количество чисел из интервала $[\,1, \ldots, n-1\,]$, взаимно простых с n.

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

При $n > 2$ значения функция Эйлера чётные.

Свойства (p — 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 $\varphi(\cdot)$

- $\sum_{d|n}\varphi(d) = n$, $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + {}$ $+\varphi(12) = 12$;

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

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 определено умножение $\cdot$, связанное со сложением *дистрибутивными законами*

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

Тривиальное кольцо — $\{0\}$[2].

[2] в нём и только в нём $0 = 1$

Обычно рассматривают *ассоциативные кольца* с ассоциативной операцией умножения:

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

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 $\langle\, R, +, \cdot, 0, 1 \,\rangle$.

Если операция умножения кольца коммутативна, то и кольцо называется *коммутативным*.

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

$$\underset{R}{\forall}\, r_1, r_2 : (r_1 \cdot r_2 = 0) \Rightarrow (r_1 = 0) \vee (r_2 = 0).$$

Важное для нас

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

Пример 1.4. 1. Кольцо целых чисел $\mathbb{Z}$ с обычными операциями сложение и умножение на нём целостно; обратимые элементы в нём — $+1$ и -1.

2. Пример кольца без единицы — кольцо чисел $2\mathbb{Z}$.

3. $\mathbb{Z}_n = \{\, 0, 1, \ldots, n-1 \,\}$ — *кольцо классов вычетов по модулю* n (*вычет = остаток*), результаты операции — по $\mod n$.

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

Определение 1.7. 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 $R \cong R'$.

Определение 1.8. Непустое подмножество S кольца $\langle\, R, +, \cdot, 0 \,\rangle$ называется его *подкольцом*, если оно устойчиво относительно вычитания (ясно, что тогда и $0 \in S$) и произведения своих элементов.

Подкольцо *собственное*[3], если $S \neq R$.

При $n < m$ кольцо $\mathbb{Z}_n$ не есть подкольцо $\mathbb{Z}_m$: например, в $\mathbb{Z}_5$ — $3 \cdot 3 = 4$, $3 + 3 = 1$, а в $\mathbb{Z}_8$ — $3 \cdot 3 = 1$, $3 + 3 = 6$[4].

Идеалы колец и факторко́льца

Определение 1.9. Непустая подгруппа I коммутативного кольца[5] R называется его *идеалом*, символически $I \lhd R$, если она устойчива относительно умножения на элементы R.

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

[4] Образно говоря, элементы 3 в этих кольцах суть *омонимы* — одинаково звучащие слова с разным смыслом.

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

Само кольцо и его нуль 0 — *тривиальные идеалы* кольца. Идеалы, не совпадающие со всем кольцом — *собственные.*

Любой идеал кольца — его подкольцо, поскольку он устойчив относительно сложения и умножения.

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

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

Целостные кольца, в которых все идеалы главные[6], называются *кольцами главных идеалов* (*КГИ*).

Пример 1.5. $(n) = n\mathbb{Z} \lhd \mathbb{Z}$, $\mathbb{Z}$ — КГИ.

Свойства идеалов колец

- Бинарное отношение $\lhd$ на множестве идеалов кольца является *частичным порядком.*
- Если R — произвольное кольцо и $n \in \mathbb{Z}$, то
$$nR = \{ na \mid a \in R \} \lhd R.$$
- Если $I_1, I_2 \lhd R$, то
  пересечение идеалов $(I_1 \cap I_2) \lhd R$,

  сумма идеалов
  $$I_1 + I_2 = \{ x + y \mid x \in I_1,\ y \in I_2 \} \lhd R,$$
  произведение идеалов
  $$I_1 \cdot I_2 = \{ x_1 \cdot y_1 + \ldots + x_n \cdot y_n \mid x_1 \in I_1,\ y_1 \in I_2, \\ i = \overline{1, n},\ n \in \mathbb{N} \} \lhd R.$$

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

Классом вычетов по модулю идеала I *кольца* $\langle\, R,\, +,\, \cdot,\, 0\,\rangle$ называется смежный класс по нормальной подгруппе $\langle\, I,\, +,\, 0\,\rangle$ аддитивной группы кольца с некоторым фиксированным представителем $r \in R$:

$$\{\, r + i \mid i \in I\,\}, \qquad \text{символически } [r]_I.$$

Классы вычетов разных представителей по модулю данного идеала либо совпадают, либо не пересекаются и в объединении дают R, т. е. образуют *разбиение* R.

Множество классов вычетов — *факторкольцо кольца* R *по модулю идеала* I, символически R/I.

Пример 1.6.

- $I = 2\mathbb{Z} = (2) \lhd \mathbb{Z}$;
- $\mathbb{Z}/2\mathbb{Z} = \{\, [0]_I,\, [1]_I\,\}$, при этом $[0]_I = I,\ [1]_I = 2\mathbb{Z} + 1$.

Определение 1.11. Идеал I называется *максимальным* в кольце R, если не существует такого идеала $I\,'$, что $I \subset I\,' \subset R$.

Пример 1.7. В $\mathbb{Z}$

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 $\mathbb{Z}$ максимальный 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, в котором каждый ненулевой элемент x либо обратим, либо однозначно с точностью до перестановки сомножителей и умножения на обратимый элемент представляется в виде произведения неразложимых элементов, называется *факториальным*.

- $\mathbb{Z}$ — факториальное кольцо.
- Все КГИ — факториальны.
- Кольцо $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ является факториальным (и, следовательно, областью целостности), если и только если n — простое число.
- Множество всех чисел вида $a \pm i\sqrt{5}$, $a \in \mathbb{R}$ является, как нетрудно проверить, кольцом, но не факториальным, поскольку, например, число 9 имеет два представления:

$$9 = 3 \cdot 3 = \left(2 + i\sqrt{5}\right) \cdot \left(2 - i\sqrt{5}\right).$$

Определение 1.13. 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

$$a = q \cdot b + r \quad \text{и либо } r = 0, \ \text{ либо } N(r) < N(b);$$

2) $N(a \cdot b) \geqslant N(a)$ и $N(a \cdot b) \geqslant N(b)$.

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

Пример 1.8.
- Классический пример евклидова кольца — *кольцо целых чисел* $\mathbb{Z}$; норма — абсолютная величина числа.
- *Кольцо многочленов* $\Bbbk[x]$ от формальной переменной x над полем $\Bbbk$:

$$\Bbbk[x] = \left\{ f(x) = a_n x^n + \ldots + a_1 x + a_0 \mid a_n, \ldots, a_0 \in \Bbbk,\ n \in \mathbb{N}_0 \right\}$$

— важный для нас пример евклидова кольца; здесь норма — степень n многочлена $f(x)$.

Евклидовы кольца — КГИ.

Поле

Определение 1.14. Целостное кольцо $\langle\, R,\ +,\ \cdot,\ 0,\ 1\,\rangle$, в котором каждый, кроме 0, элемент обратим, называется *полем*.

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*.

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

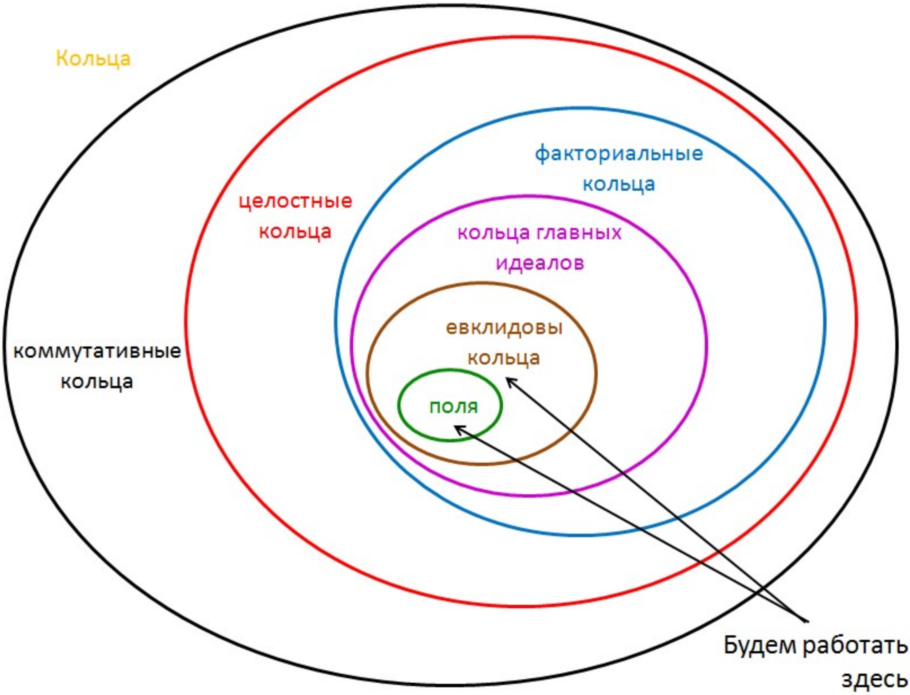


Рис. 1.2. От колец к полям

1.3 Задачи с решениями

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

1. Целые числа относительно сложения? *Да.*

2. Четные числа относительно сложения? *Да.*
3. Целые числа, кратные данному натуральному числу n, относительно сложения? *Да.*
4. Степени данного действительного числа a, $a \neq 0, \pm 1$, с целыми показателями относительно умножения? *Да.*
5. Неотрицательные целые числа относительно сложения? *Нет* (противоположного элемента)
6. Нечетные целые числа относительно сложения? *Нет* (устойчивости)
7. Целые числа относительно вычитания? *Нет* (ассоциативности).
8. Рациональные числа относительно сложения? *Да.*
9. Рациональные числа относительно умножения? *Нет* (обратного у 0).
10. Рациональные числа, отличные от нуля, относительно умножения? *Да.*
11. Положительные рациональные числа относительно умножения? *Да.*
12. Положительные рациональные числа относительно деления? *Нет* (ассоциативности).
13. Корни n-й степени из единицы (как действительные, так и комплексные) относительно умножения? *Да.*

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

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

16. Матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения? *Да.*

17. Матрицы порядка n с целыми элементами и определителем, равным ± 1 относительно умножения? *Да.*

18. Матрицы порядка n с действительными элементами относительно сложения? *Да.*

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

20. Взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t, затем s)? *Да.*

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

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

23. Параллельные переносы трехмерного пространства $\mathbb{R}^3$ относительно композиции движений? *Да.*
24. Повороты трехмерного пространства $\mathbb{R}^n$ вокруг прямых, проходящих через данную точку O относительно композиции движений? *Да.*
25. Все движения трехмерного пространства $\mathbb{R}^n$ относительно композиции движений? *Да.*
26. Действительные многочлены степени не выше n от неизвестного x и нулевой многочлен относительно сложения? *Да.*
27. Действительные многочлены любых степеней (включая 0) от переменной x относительно сложения? *Да.*

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

Решение. $\mathbb{Z}_6 = \{0, 1 \ldots, 6\}$, 0 — единица группы.

$$\operatorname{ord} 0 = 1 \mid 6;$$

$$1 = 1,\ 1+1 = 2,\ \ldots = 6 \cdot 1 = 6 \equiv_6 = 0 \Rightarrow$$

$$\Rightarrow \operatorname{ord} 1 = 6 \mid 6;$$

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

$$3 = 3,\ 3+3 = 0 \Rightarrow \operatorname{ord} 3 = 2 \mid 6;$$

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

$$5 = 5,\ 5+5 = 4,\ 5+5+5 = 3,\ \ldots,\ 6 \cdot 5 = 0 \Rightarrow$$

$$\Rightarrow \ \operatorname{ord} 5 = 6.$$

Порождающие элементы — 1 и 5.

Задача 1.3. *Показать, что*

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

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 1.4. *Найти все подгруппы циклической группы порядка* 24.

Решение. Циклическая 24-элементная группа $C = \{a^0 = 1, a^1, a^2, \ldots, a^{23}\}$ имеет (циклические) подгруппы, генераторами которых будут элементы a^m, где $m \mid n$, т.е. $m = 1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 22$.
Порядок соответствующей подгруппы — n/m.

$m = 1\ : \{1, a^1, a^2, \ldots, a^{24}\} = \langle a^1 \rangle = C \cong \mathbb{Z}_{24};$

$m = 2\ : \{1, a^2, a^4, a^6, \ldots, a^{22}\} = \langle a^2 \rangle \cong \mathbb{Z}_{12};$

$m = 3 \ : \{\, 1,\, a^3,\, a^6,\, a^9,\, \ldots,\, a^{21} \,\} \ = \ \langle a^3 \rangle \ \cong \ \mathbb{Z}_8;$

$m = 4 \ : \{\, 1,\, a^4,\, a^8,\, a^{12},\, \ldots,\, a^{20} \,\} \ = \ \langle a^4 \rangle \ \cong \ \mathbb{Z}_6;$

$m = 6 \ : \{\, 1,\, a^6,\, a^{12},\, a^{18} \,\} \ = \ \langle a^6 \rangle \ \cong \ \mathbb{Z}_4;$

$m = 8 \ : \{\, 1,\, a^8,\, a^{16} \,\} \ = \ \langle a^8 \rangle \ \cong \ \mathbb{Z}_3;$

$m = 12 \ : \{\, 1,\, a^{12} \,\} \ = \ \langle a^{12} \rangle \ \cong \ \mathbb{Z}_2;$

$m = 24 \ : \{\, 1 \,\} \ = \ \langle 1 \rangle \ \cong \ E$ — единичная.

Задача 1.5. *Выяснить, какие из следующих множеств являются кольцами, но не полями, и какие полями относительно указанных операций.*

Если операции не указаны, то подразумеваются сложение и умножение чисел.

1. Целые числа $\mathbb{Z}$? Кольцо.
2. Чётные целые числа? Кольцо.
3. Целые $n\mathbb{Z}$, $n > 0$? Кольцо.
4. Рациональные числа $\mathbb{Q}$? Поле.
5. Действительные числа $\mathbb{R}$? Поле.
6. Комплексные числа $\mathbb{C}$? Поле.
7. Квадратные матрицы порядка n с *целыми* элементами относительно сложения и умножения матриц?
   Кольцо (обратной матрицы может не быть).

8. Квадратные матрицы порядка n с *действительными* элементами относительно сложения и умножения матриц?
   Кольцо (обратной матрицы может не быть).
9. 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).
10. 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. *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 евклидово, возможно *деление с остатком*.
- 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:

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

Черту над символами классов вычетов часто не ставят.

Поскольку p — простое, то $\mathbb{Z}/(p)$ — не просто кольцо, а *поле*, и в нём возможно деление без остатка на любой ненулевой элемент.

Это *конечное поле*, точнее *простое поле Галуа*, обозначение — $\mathbb{F}_p$ или $GF(p)$; все операции в нём — по $\bmod\ p$.

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 $\mathbb{Z}/(4)$ дважды два равно нулю!
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 $\operatorname{char}\Bbbk$.

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.
$\{0, 1, 2, \ldots, \operatorname{char}\Bbbk - 1\}$ — минимальное *подполе* любого поля $\Bbbk$ характеристики $\operatorname{char}\Bbbk > 0$.

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

1. $\Bbbk[x]$ — *кольцо многочленов* (от *формальной* переменной x) над полем $\Bbbk$:
$$\{\, P(x) = a_0 + a_1x + \ldots + a_nx^n \mid a_0, \ldots, a_n \in \Bbbk \,\};$$
$$\Bbbk[x] \leftrightarrow \{\, (a_0, \ldots, a_n) \in \Bbbk^n \mid n \in \mathbb{N}_0 \,\}.$$

2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$; в нём:

   элементы — "дроби" P/Q (если $Q \neq 0$), где $P, Q \in \Bbbk[x]$;

   умножение — $(P/Q) \cdot (U/V) = (PU)/(QV)$;

   эквивалентность — $P_1/Q_1 = P_2/Q_2$, если $P_1Q_2 = P_2Q_1$;

   сложение — дроби можно приводить к общему знаменателю и складывать: $P/Q + U/V = (PV + QU)/(QV)$;

   включение — поскольку $\Bbbk[x] \subset \Bbbk(x)$, то каждый многочлен P отождествляется с $P/1$.

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

Лемма 2.1 (тождество Фробениуса, сильное упрощение вычислений в конечном поле). *В поле характеристики* $p > 0$ *выполнено тождество*

$$(a + b)^p = a^p + b^p.$$

Доказательство. В любом коммутативном кольце верна формула для степени бинома

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

а при $i = 1, \ldots, p-1$ числитель коэффициента

$$C_p^i = \tfrac{p!}{i!(p-i)!}$$

делится на p, а знаменатель — нет, откуда $C_p^i \equiv_p 0$. □

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

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

Мультипликативная группа и примитивный элемент конечного поля. Вспомним, что $\mathbb{R} \setminus \{0\}$ — группа по умножению.
$\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ — *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение 2.1. $\mathbb{F}_p^*$ — *циклическая по умножению группа порядка* $p-1$.

Как любая конечная циклическая группа, $\mathbb{F}_p^*$ содержит генератор = примитивный элемент α:

- любой элемент $\beta \in \mathbb{F}_p^*$ является некоторой его натуральной степенью: $\beta = \alpha^i$, $i \in \{1, \ldots, p-1\}$;
- причём $1 = \alpha^{p-1}$ и $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.
- $\mathbb{F}_p^*$ имеет $\varphi(p-1)$ примитивных элементов.

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

Поскольку 1 — не генератор, проверяем 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 $\mathbb{F}_{11}^*$, $\operatorname{ord} 2 = 10$.

Проверяем 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 $p-1$

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

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

(т.к. $\alpha^{k \operatorname{ord} \alpha} = 1$, $k \in \mathbb{N}$).

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

$2^2 = 4 \neq 1$, $2^5 = 32 \equiv_{11} 10 \neq 1 \Rightarrow 2$ — *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 $\alpha \in \mathbb{F}_p^*$ генератором, нужно проверить не более двух равенств: $\alpha^{12} = 1$ и $\alpha^{18} = 1$.

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

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

$$2^1 = 2, \qquad\qquad 2^3 = 8,$$
$$2^7 = 128 \equiv_{11} 7, \qquad\qquad 2^9 = 512 \equiv_{11} 6,$$

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

Заметим, что

$$0 \neq \alpha \in \mathbb{F}_p \;\Rightarrow\; \alpha^{p-1} = 1 \;\Rightarrow\; \alpha^{p-2} = \alpha^{-1}.$$

Например, найдём обратный элемент к 4 в поле $\mathbb{F}_{11}$:

$$4^{-1} = 4^{11-2} = 4^9 = 262144 = 23831 \cdot 11 + 3 \equiv_{11} 3\,.$$

Действительно, $3 \cdot 4 \equiv_{11} 1$.

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

Например, поделим «уголком» x^4 на x^2+1 в кольце $\mathbb{Z}_2[x]$:

$$\begin{array}{l|l}
x^4 & x^2+1 \\ \cline{2-2}
\underline{x^4+x^2} & x^2+1 \\
\quad\; x^2 & \\
\quad\; \underline{x^2+1} & \\
\qquad\quad 1 &
\end{array}$$

т.е. $x^4 = (x^2+1)^2 + 1$.

Самостоятельно: делением многочленов «уголком» 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 — $2x + 2$.

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

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

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

Неприводимые многочлены. Кольцо многочленов $\Bbbk[x]$ над полем $\Bbbk$ — евклидово $\Leftrightarrow$ оно факториального $\Leftrightarrow$ каждый его элемент однозначно с точностью до перестановок разлагается в произведение простых (неразложимых).

Простые (неразложимые) элементы колец $\Bbbk[x]$ называют *неприводимыми многочленами*, они не имеют нетривиальных делителей[1].

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

Вопросы для кольца многочленов над данным полем:

1) какие многочлены неприводимы?
2) как их находить?

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$:

в кольце над $\mathbb{C}$ — только многочлены 1-й степени;

[1] тривиальные делители — это $+1$ и -1

в кольце над $\mathbb{R}$ — 1) многочлены 1-й степени,

— 2) многочлены 2-й степени с отрицательным дискриминантом;

в кольце над $\mathbb{Q}$ — существуют неприводимые многочлены произвольной степени.

$\boxed{\text{Далее нас будут интересовать неприводимые (и чаще — нормированные) многочлены в конечных полях.}}$

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

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \;\; a_i \in \mathbb{F}_p, \; i = \overline{0, n-1},$$

равно p^n.

<u>*Неприводимые многочлены кольца* $\mathbb{F}_2[x]$</u>. Найдём в $\mathbb{F}_2[x]$ все неприводимые многочлены 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 $\mathbb{F}_2$: $\qquad x^2 + x + 1$.

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

Исключая, как сделано ранее, делимость на $x+1$, получаем условие $a + b \neq 0$, т.е.

$$\left[\begin{array}{l} a = 0, \; b = 1\,, \\ a = 1, \; b = 0\,. \end{array}\right.$$

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	$x^4 + x^2 + 1$	— *приводимый*
1	0	0	$x^4 + x^3 + 1$	
1	1	1	$x^4 + x^3 + x^2 + x + 1$	

Найдены многочлены, у которых нет *линейных* делителей. Но многочлен 4-й степени может иметь *квадратные делители*, и это имеет место:

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

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 нечётным, 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 —

$$x^5 + x^2 + 1, \qquad\qquad x^5 + x^3 + 1,$$

$$x^5+x^3+x^2+x+1, \qquad x^5+x^4+x^2+x+1,$$
$$x^5+x^4+x^3+x+1, \qquad x^5+x^4+x^3+x^2+1.$$

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

Линейные многочлены:

$$\begin{array}{ccc} x & x+1 & x+2 \\ 2x & 2x+1 & 2x+2 \end{array}$$

Какие из них неприводимы? *Все!* (шутка).

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

$$\begin{array}{ll} x^2+1 & 2x^2+2 \\ x^2+x+2 & 2x^2+x+1 \\ x^2+2x+2 & 2x^2+2x+1 \end{array}$$

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 (из таблиц, алгоритм Берлекэмпа...)

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

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 $a(x)$:
$$a(x) \in \mathbb{F}_p[x], \quad f(x) \equiv_{a(x)} g(x).$$

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

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 $\left\{\overline{r(x)}\right\} = GF\left(p^n\right) = \mathbb{F}_p^n$ 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:

$$\overline{x+1}+\overline{x+2} = \overline{2x}, \qquad \overline{x}\cdot\overline{2x} = \overline{1},$$
$$\overline{2x+1}+\overline{x} = \overline{1}, \qquad \overline{2x+1}\cdot\overline{x} = \overline{x+1},$$

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

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

Это значит, что $x+1$ — примитивный элемент поля $\mathbb{F}_3^2$ (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, $2x^2+x+1$?

Ответ: получится поле, *изоморфное построенному.*

Пример 2.4 (вычисления в конечном поле). 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 $a(x)$ — неприводимый многочлен[2].

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

Как найти примитивные элементы поля $\mathbb{F}_p^n$?
α — примитивный элемент поля $F = \mathbb{F}_p^n$, если при изменении $k = 1, 2, \ldots, p^n - 1$ значение α^k пробегает значения всех элементов F^*. Как следствие:

- $\alpha^{p^n - 1} = 1$;
- если m взаимно просто с $p^n - 1$, то α^m — *другой примитивный элемент* поля F.
  Так могут быть получены *все примитивные элементы* F*: их* $\varphi(p^n - 1)$ *штук = количество взаимно простых с* $p^n - 1$ *чисел.*

[2] а если бы это был многочлен 4-й степени?

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:

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

Я что-то не понимаю: неприводимые многочлены — это примитивные элементы?

Ведь было: для поиска и тех, и других нет эффективных алгоритмов...

- *Неприводимые многочлены* ищут в *кольце многочленов* $\mathbb{F}_p[x]$ над простым полем $\mathbb{F}_p$ — например, чтобы построить расширение поля.
- *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. Например, в $\mathbb{F}_3[x]/\big(x^2+1\big)$:

$$\frac{x+1}{2x+1} = x.$$

Может ли приводимый многочлен быть примитивным элементом?

1. Возьмём поле $\mathbb{F}_2 = \{\,0,\,1\,\}$.
2. Возьмём неприводимый над $\mathbb{F}_2$ многочлен $x^3 + x + 1$.

3. Построим поле $F = \mathbb{F}_2[x]/\big(x^3+x+1\big) \cong \mathbb{F}_2^3$; оно содержит все полиномы из $\mathbb{F}_2[x]$ степени $\leqslant 2$.
4. Многочлен $b(x) = x^2+x = x(x+1)$ — приводим в любом кольце, в т.ч. — в $\mathbb{F}_2[x]$, и он принадлежит F.
5. Является ли $b(x)$ — примитивным элементом поля F?

Мультипликативная группа поля F содержит $2^3-1=7$ элементов, это простое число $\Rightarrow$ в мультипликативная группе все $\varphi(7)=6$ неединичных элеметов — генераторы $\Rightarrow$ ответ на оба вопроса — *ДА*!

Удостоверимся, что $\alpha = x^2+x = x(x+1)$ — примитивный элемент поля $F = \mathbb{F}_2[x]/\big(x^3+x+1\big)$.
В F $x^3 = x+1$ и

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

Всегда ли неприводимый многочлен есть примитивный элемент?

1. Возьмём поле $\mathbb{F}_5 = \{\,0,\,1,\,2,\,3,\,4\,\}$.

2. Возьмём неприводимый над $\mathbb{F}_5$ многочлен x^2+x+1.
3. Построим поле $F = \mathbb{F}_5[x]/\big(x^2+x+1\big) \cong \mathbb{F}_5^2$; оно содержит только полиномы 0-й и 1-й степеней из $\mathbb{F}_5[x]$.
4. Все многочлены 1-й степени неприводимы, имеют вид $ax+b$ и их — 20 шт.
   Все ли они — примитивные элементы поля F?

Мультипликативная группа поля F содержит $5^2 - 1 = 24$ элемента из которых $\varphi(24) = 8$ примитивных $\Rightarrow$ не все многочлены 1-й степени — генераторы $\Rightarrow$ ответ на оба вопроса — *НЕТ*!

Удостоверимся, что $\alpha = x$ *не есть* примитивный элемент поля $F = \mathbb{F}_5[x]/\big(x^2+x+1\big)$.

В F: $x^2 = -x-1 = 4x+4$ и

$$
\begin{aligned}
\alpha &= x\\
\alpha^2 &= 4x+4,\\
\alpha^3 &= 4x^2+4x \;=\; 16x+16+4x \;=\; 1.
\end{aligned}
$$

Вопрос: когда корень x (сам неприводимый многочлен!) неприводимого над $\mathbb{F}_p$ многочлена $a(x)$ 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 $x^t-1 \not\vdots\, x^3+x+1$ ни при каком $1 \leqslant t < 7 = m$.

Поэтому

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

— 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 Вычисление в конечных полях

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

Наблюдение: общий делитель пары чисел (a,b), то остаётся им и для пары $(a-b,b)$.

Отсюда:

- пары чисел (a,b) и $(a-kb,b)$ *имеет одинаковые общие делители*;
- вместо $a-kb$ можно взять *остаток* r_0 от деления нацело a на b: $a \;=\; bq+r_0$, $q\in\mathbb{N}$, $0\leqslant r_0 < b$;

- 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, $a \geqslant b$*
>
> 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 оно 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): $r_{-1} = 105 \quad \Rightarrow (252, 105)$;

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

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

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

Ясно, что

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

Утверждение 2.3 (соотношение Безу[3]). *Для любых натуральных* a, b *и* $d = \text{НОД}\,(a, b)$ *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:

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

[3] 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, в котором на каждом шаге:

1) дополнительно вычисляются x_i и y_i по формулам
$$x_i = x_{i-2} - q_i x_{i-1},\ y_i = y_{i-2} - q_i y_{i-1},\ i = 0, 1, \ldots;$$
$$x_{-2} = y_{-1} = 1\,,\ x_{-1} = y_{-2} = 0\,;$$

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

$$4x \;=\; 1. \tag{$*$}$$

Решение.

1. $4x \;=\; 1 + k \cdot 101 \;=\; 102,\ 203,\ \mathbf{304}$
   $x \;=\; 304/4 \;=\; 76.$
   Это решение перебором.
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

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

(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 $\Bbbk = \{\,1, \alpha, \beta, \ldots\}$ называется двухосновная алгебраическая система $\mathcal{V} \;=\; \langle\, V, \Bbbk; +, \cdot\rangle$, где

- $V \;=\; \{\,0, v, \ldots\}$ — произвольное множество *векторов*,
- $+$ — бинарная операция сложения элементов V:
  $$V \times V \xrightarrow{+} V,$$
- $\cdot$ — бинарная операция умножения элемента («числа́») 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 $(+)$, 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) $1 \cdot v = v$.

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, его называют *n-мерным координатным пространством* над полем $\Bbbk$.

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

  $v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1-1) \cdot v = 0 \cdot v = 0.$

Утверждение 2.4. *Поле $GF(q)$ характеристики простого $p > 0$ 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 как векторное пространство состоит из p^n элементов: $q = p^n$.*

Представление элементов конечных полей. Поле $\mathbb{F}_p^n$ с элементами $\mathcal{M}_{p,n}(x) =$

$$= \left\{ b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} \mid b_0, b_1, \ldots, b_{n-1} \in \mathbb{F}_p \right\},$$

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: $F = \mathbb{R}[x]/\left(x^2+1\right)$;
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 $\mathbb{F}_p^n = \mathbb{F}_p[x]/\big(a(x)\big)$

- $\overline{x}$ есть совокупность всех многочленов из $\mathbb{F}_p[x]$, дающих при делении на $a(x)$ остаток x;
- $\overline{x} = (0, 1, 0, \ldots, 0) \in (\mathbb{F}_p)^n$.

В дальнейшем, 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 $\alpha^z = b$).

На сложности этой задачи (известны не более, чем субэкспоненциальные алгоритмы её решения) базируются 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.

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

а значит и $a_n^{-1} a(x)$.

С другой —

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

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 $b_0 = b_1 = \ldots = b_{n-1} = 0$.

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 (см. с. 76).

Примитивные многочлены

Пример 2.11.

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

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. □

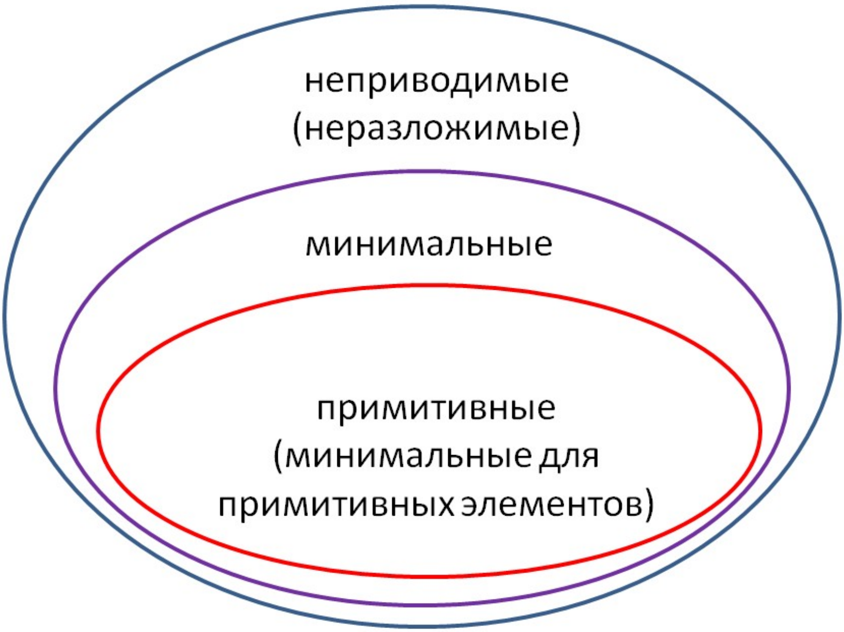


Рис. 2.1. Соотношение множеств неприводимых, минимальных и примитивных многочленов

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 $m_\beta(x)$.*

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

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

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:* $\deg m_\beta(x) \leqslant n$.

Доказательство. Рассмотрим следующие элементы поля $\mathbb{F}_p^n$: 1, β, β^2, ..., β^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, ..., 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 $f(x)$. $\square$

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

1. $m_\beta(x) \mid \left(x^{p^n} - x\right)$.
2. Многочлен $m_\beta(x)$ — минимальный для $\left\{\beta,\, \beta^p,\, \beta^{p^2},\, \ldots,\, \beta^{p^{\deg m_\beta(x)-1}}\right\}$ — *сопряжённых* с β элементов $\mathbb{F}_p^n$.

Свойства многочленов над конечным полем

Поле разложения многочлена $f(x) \in \mathbb{F}_p[x]$ — наименьшее $\mathbb{F}_p^n$, $n = \min$ расширение 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 многочлена $x^{p^n-1} - 1$:*

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

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

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

Порядок $\operatorname{ord}\alpha$ любого её элемента ($=$ 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 многочлена $x^{p^n} - x$.*

Доказательство. Вынесем x за скобку:

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

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

Иными словами, $\mathbb{F}_p^n$ — поле разложения многочлена $x^{p^n} - x$.

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

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

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

Теорема даёт возможность раскладывать многочлены $x^n - 1$ *при составных* n.

Пример 2.12. Многочлен $x^{15} + 1 \in \mathbb{F}_2[x]$ (где $-1 = +1$) должен делиться на $x^3 + 1$ и $x^5 + 1$.

Действительно,

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

Теорема 2.6. *Все неприводимые многочлены n-й степени из $\mathbb{F}_p[x]$ делят многочлен $x^{p^n} - x$.*

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 многочлену $f(x)$ степени n из $\mathbb{F}_p[n]$ (*пока не доказано!*[4]) и строим поле $\mathbb{F}_p[x]/\big(f(x)\big)$.
В нём x — корень и своего м.м. $f(x)$, и $x^{p^n-1} - 1$.
По свойствам м.м. $x^{p^n-1} - 1$ делится на $f(x)$.

□

[4] Теорема 2.1

Пример 2.13 (продолжение *Примера* 2.12). 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:

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

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: $x^2 + x + 1$.

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

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

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

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

Тогда $F \overset{\text{def}}{=} \mathbb{F}_p/(\varphi)$ — 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 $n \geqslant k$. □

Итак, *вопрос*: какие неприводимые многочлены $f(x) \in \mathbb{F}[x]$ делят $x^{p^n} - x$?
Ответ: либо (1) любой — степени n, либо (2) некоторый — степени $< n$ и (3) других нет.

Следующая теорема позволяет находить все корни многочлена, если известен какой-либо один корень: достаточно возводить его последовательно в степени p.

Теорема 2.8 (свойство корней неприводимого многочлена). *Если β — корень неприводимого многочлена $f(x)$ степени n из $\mathbb{F}_p[x]$, то элементы $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$ 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

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

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 $\beta,\ \beta^p,\ \ldots,\ \beta^{p^{n-1}}$ — корни многочлена $f(x)$.

2. Осталось доказать, что все $\beta,\ \beta^p,\ \ldots,\ \beta^{p^{n-1}}$ 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* 2.6 получаем $n - k + l \geqslant n \;\Rightarrow\; l \geqslant k$, т.е. $l = k$ и все вышеописанные корни различны. □

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

Нахождение корней неприводимого многочлена

Пример 2.14. 1. Найти корни неприводимого над $\mathbb{F}_2$ многочлена

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

Решение. Один корень получаем немедленно: это x.

По только что доказанной теореме можно выписать остальные корни в поле $\mathbb{F}_2[x]/(f(x))$:

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

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, и по доказанной теореме выписываем остальные в поле $\mathbb{F}_2[x]/(f(x))$:

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

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 $\mathbb{F}_3[x]/\big(x^2+2x+2\big)$ 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 $\mathbb{F}_3[x]/\big(x^2+2x+2\big)$.

Алгоритм нахождения всех корней многочлена $f(x) \in \mathbb{F}_p[x]$.

1. Разложить $f(x)$ на *неприводимые* произведение неприводимых многочленов:
$$f(x) = g_1(x)\cdot g_2(x)\cdot\ldots\cdot g_k(x).$$
2. Для каждого многочлена $g_i(x)$, $i = \overline{1,k}$ рассмотреть расширение $\mathbb{F}_p[x]/\big(g_i(x)\big)$, в котором он будет иметь $\deg g_i$ корней
$$\alpha,\ \alpha^p,\ \alpha^{p^2},\ \ldots,\ \alpha^{p^{\deg g_i - 1}}.$$
3. Объединить все корни в одном общем расширении $\mathbb{F}_p^n$, где $n = \text{НОК}\,(n_1, \ldots, n_k)$.

Пример 2.15. 1. Решить уравнение

$$f(x) = 2x^4 + x^3 + 4x^2 + 4 = 0, \text{ где } f(x) \in \mathbb{F}_5[x].$$

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[5].

В поле $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$ корнями многочлена $f_2(x) = 0$ будут x, x^5, x^{25}.

Вычисляем — с учётом $x^3 = -2x - 4 = 3x + 1$:

$$\begin{aligned} x^5 &= x^2(3x+1) = 3x^3 + x^2 = 4x + 3 + x^2 = \\ &= x^2 + 4x + 3; \\ x^{25} &= \big(x^5\big)^5 = \big(x^2 + 4x + 3\big)^5 = x^{10} + 4^5x^5 + 3^5 = \\ &= x^{10} + 4(x^2 + 4x + 3) + 3 = x^{10} + 4x^2 + x. \end{aligned}$$

(поскольку $4^5 = 2^{10} = 102\underline{4}$ и $3^5 = 81 \cdot 3 = 24\underline{3}$).

Найдём отдельно x^{10}:

[5] а если бы это был многочлен 4-й степени?

$$
\begin{aligned}
x^{10} &= \left(x^5\right)^2 = \left(x^2+4x+3\right)^2 = \\
&= x^4+x^2+3^2+3x^3+4x+x^2 = \\
&= x^4+3x^3+2x^2+4x+4 = \\
&= \cancel{3}x^2+\cancel{x}+\cancel{4}x+3+\cancel{2}x^2+4x+4 = 4x+2.
\end{aligned}
$$

Продолжаем:

$$x^{25} = x^{10}+4x^2+x = \cancel{4}x+2+4x^2+\cancel{x} = 4x^2+2.$$

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 $2 \in F$).

2. 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:

$$x^8{+}x^4{+}x^2{+}x{+}1 = \underbrace{\left(x^4+x^3+1\right)}_{f_1(x)} \cdot \underbrace{\left(x^4+x^3+x^2+x+1\right)}_{f_2(x)}.$$

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 $F_1 = \mathbb{F}_2[x]/\left(x^4+x^3+1\right)$

и

x, x^2, x^3, x^3+x^2+x+1

в поле $F_2 = \mathbb{F}_2[x]/\left(x^4+x^3+x^2+x+1\right)$.

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:

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

Удостоверимся, что, например, x^2+1 — корень $f(x)$:

$$\begin{aligned} f(x^2+1) &= (x^2+1)^8+(x^2+1)^4+(x^2+1)^2+(x^2+1)+1 =\\ &= (x^{16}+1)+(x^8+1)+(x^4+1)+x^2. \end{aligned}$$

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 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 в поле $\mathbb{F}_2[x]/\big(x^4+x^3+1\big)$.

3. Найти корень многочлена

$$f(x)=x^4+2x+2=0\in\mathbb{F}_3[x].$$

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:

$$\begin{aligned} f(x)\ =\ x^4+2x+2\ =\ (x^2+ax+b)(x^2+cx+d)\ =\\ =\ x^4+cx^3+dx^2x+ax^3+acx^2+adx+bx^2+bcx+bd\ =\\ =\ x^4+(a+c)x^3+(b+ac+d)x^2+(ad+bc)x+bd.\end{aligned}$$

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}:

$$\begin{aligned} x^9 &= \big(x^4\big)^2 x = (x+1)^2 x = x^3 + 2x^2 + x; \\ x^{27} &= \big(x^9\big)^3 = (x^3 + 2x^2 + x)^3 = x^9 + 2x^6 + x^3 = \\ &= (x^3 + 2x^2 + x) + 2x^2x^4 + x^3 = \\ &= x^3 + 2x^2 + x + 2x^3 + 2x^2 + x^3 = \\ &= x^3 + x^2 + x. \end{aligned}$$

Ответ: в поле $\mathbb{F}_3[x]/\big(x^4 + 2x + 2\big)$ уравнение

$$f(x) = x^4 + 2x + 2 = 0$$

имеет корни x, x^3, $x^3 + 2x^2 + x$, $x^3 + x^2 + x$.

4. Решить уравнение $f(x) = x^5 + x^2 + 1 = 0$, где $f(x) \in \mathbb{F}_2[x]$.

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}:

$$x^8 = x^5x^3 = (x^2+1)x^3 = x^5+x^3 = x^3+x^2+1;$$

$$\begin{aligned} x^{16} &= \left(x^8\right)^2 = (x^3+x^2+1)^2 = x^6+x^4+1 = \\ &= x^5x+x^4+1 = (x^3+x)+x^4+1 = \\ &= x^4+x^3+x+1. \end{aligned}$$

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

5. Решить уравнение $f(x) = x^2+x+1 = 0$, 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.

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 $\mathbb{F}_2/\big(a(x)\big)$ 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 2.16. 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:
   $$P = \alpha^7\alpha^{10} = \alpha^{17} = \alpha^2 = x^2.$$

Нахождение минимальных многочленов. Для нахождения м.м. $m_\beta(x)$ элемента β 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
$$m_\beta(x) = (x-\beta)\cdot(x-\beta^p)\cdot\ldots\cdot\left(x-\beta^{p^{d-1}}\right),$$
случай $m_\beta(x) \equiv 0$ эквивалентен 2).

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

Пример 2.17. Найдём минимальные многочлены для элементов x^2+x, x^2 поля
$$F = \mathbb{F}_2[x]/\left(x^4+x+1\right).$$

В этом поле $x^4 = x+1$.

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

Т.о. м.м. $m_\beta(x)$ имеет 2 корня β, β^2, его степень равна 2 и
$$m_\beta(x) = (x-\beta)(x-\beta^2) = x^2+(\beta^2+\beta)\,x+\beta^3.$$
Вычисляем коэффициенты полинома:
$$\begin{aligned}\beta^2+\beta &= (x^2+x+1)+(x^2+x) = 1,\\ \beta^3 &= (x^2+x+1)(x^2+x) = \\ &= x^4+\cancel{x^3}+\cancel{x^3}+\cancel{x^2}+\cancel{x^2}+x = \\ &= (x+1)+x = 1,\end{aligned}$$

т.е. $m_\beta(x) = x^2+x+1$.

Заметим, что

- коэффициенты перед степенями x могут оказаться только константы 0 или 1, иначе — ошибка в вычислениях;
- 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:

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

Заметим, что многочлен $a(x) = x^4+x+1$ примитивен, т.е. является м.м. для x. Поэтому $a(x)$ будет м.м. и для элемента $\beta = x+1$: $m_\beta(x) = a(x) = x^4+x+1$.

Ясно, что $a(x)$ является м.м. также и для сопряжённых с x элементов x^2, x^4, x^8 (выразите их через β самостоятельно).

Существование поля $GF(p^n)$ для всех n. Мы уже показали, что любое конечное поле имеет p^n элементов (p — простое, n — натуральное).

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

Для таких многочленов над конечным полем справедлив аналог основной теоремы арифметики: *каждый нормированный многочлен разлагается на произведение неприводимых многочленов однозначно* с точностью до порядка сомножителей.

Доказательство. Действительно:

- разложение на множители в евклидовом кольце однозначно;
- в случае кольца многочленов над полем обратимые элементы — ненулевые константы;
- выбор старшего коэффициента 1 однозначно определяет сомножители.

$\square$

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

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

Доказательство. Занумеруем $i = 1, \ldots, ((n))$ все неприводимые нормированные многочлены степени n и сопоставим им формальную переменную $f_{i,n}$ $\Rightarrow$ произвольному многочлену однозначно сопоставлен моном (многочлен степени n_j берётся в степени s_j):

$$f_{i_1,n_1}^{s_1} \cdot \ldots \cdot f_{i_r,n_r}^{s_r}, \text{ причем } \sum_{j=1}^{r} n_j s_j = n.$$

Поэтому все нормированные многочлены перечисляются формальным бесконечным произведением

$$\prod_{i,n} \left(\sum_{k=0}^{\infty} f_{i,n}^k \right) = \sum f_{i_1,n_1}^{s_1} \cdot \ldots \cdot f_{i_r,n_r}^{s_r} \qquad (*)$$

(раскрыты скобки и бесконечное произведение записано в виде формального ряда).

Сделаем замену переменных $f_{i,n} = t^n$, которая делает *все многочлены одной степени неразличимыми.*

Приведение подобных приведёт к тому, что:

в правой части $(*)$ будет ряд от переменной t.

Коэффициент при t^n в этом ряде равен числу нормированных многочленов степени n, т.е. p^n:

$$\sum_{n=0}^{\infty} p^n t^n.$$

в левой части все неприводимые многочлены степени n дадут одинаковый множитель (сумму бесконечной геометрической прогрессии со знаменателем t^n) и $(*)$ превращается в

$$\prod_n \left(\sum_{k=0}^{\infty} t^{nk}\right)^{((n))} = \sum_{n=0}^{\infty} p^n t^n.$$

По формуле суммы бесконечной геометрической прогрессии:

$$\prod_n \frac{1}{(1-t^n)^{((n))}} = \frac{1}{1-pt}.$$

Прологарифмируем («$-$» в обеих частях равенства сокращаются, $n \mapsto d$):

$$\sum_d ((d)) \ln(1-t^d) = \ln(1-pt).$$

Продифференцируем по t («$-$» в обеих частях равенства сокращаются):

$$\sum_d ((d)) \frac{dt^{d-1}}{1-t^d} = \frac{p}{1-pt}.$$

Снова воспользуемся формулой суммой геометрической прогрессии:

$$\sum_{d,k} ((d)) dt^{d-1} t^{dk} = \sum_n p^{n+1} t^n.$$

Умножаем на t обе части равенства:

$$\sum_{d,k} d((d)) t^{d(k+1)} = \sum_n p^n t^n.$$

Равенство коэффициентов при одинаковых степенях t и есть утверждение леммы. □

Следствия.

1. Существование неприводимых многочленов.

Доказательство. Простая оценка

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

доказывает, что $((n)) > 0 \Rightarrow$ существует *хотя бы один* неприводимый (и нормированный) многочлен степени n; более точная оценка — $\frac{p^n}{2n} \leqslant ((n))$. □

2. Среднее число неприводимых нормированных многочленов: $((n)) \sim p^n/n$.

Доказательство. Переход к пределу при $n \to \infty$ в полученной формуле. □

Т.о. *неприводимые нормированные* многочлены составляют приблизительно $1/n$-ю часть всех многочленов степени n над полем $\mathbb{F}_p$.

Ещё одна формула для числа $((n))$ *неприводимых нормированных многочленах степени* n *над* $\mathbb{F}_p$.

Функция Мёбиуса $\mu(n)$ определена для всех $n \in \mathbb{N}$:

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

Например:

$$\begin{aligned} &\mu(1) = 1 \text{ (по определению)}, && \mu(6) = 1, \\ &\mu(2) = -1, && \mu(7) = -1, \\ &\mu(3) = -1, && \mu(8) = 0, \\ &\mu(4) = 0, && \mu(9) = 0, \\ &\mu(5) = -1, && \mu(10) = 1. \end{aligned}$$

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:

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

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

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

Докажем теперь, что *любые два поля с одинаковым числом элементов изоморфны.*

Теорема 2.10. *Пусть $m_\alpha(x)$ — минимальный многочлен элемента $\alpha \in \mathbb{F}_p^n$ и d — его степень.*

Тогда поле $\mathbb{F}_p[x]/\big(m_\alpha(x)\big)$ изоморфно подполю $\mathbb{F}_p^d$, порожденному степенями α.

Доказательство. Степени α принадлежат d-мерному пространству с базисом $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, которое является подполем поля $\mathbb{F}_p^n$, поскольку замкнуто относительно сложения и умножения и содержит 0 и 1. $\square$

2.6 Циклические пространства

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

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

$$\begin{aligned} (f) &= \{\, t\cdot f \,\},\ t\in\mathbb{F}_p[x]; \\ \mathbb{F}_p[x]/(f) &= \{\, (f), \overline{g}, \overline{h}, \ldots \,\}, \quad \deg\overline{g}, \ldots < \deg f. \\ \overline{g} &= (f)+g, \ldots . \end{aligned}$$

Нормированный делитель порождающего элемента идеала

Теорема 2.11. *Пусть φ — неприводимый нормированный многочлен, который делит f. Тогда*

1) *совокупность всех вычетов, кратных φ, образует идеал в кольце классов вычетов по модулю f:*

$$I_\varphi \overset{\text{def}}{=} \{\, t\cdot\varphi \,\} \lhd \mathbb{F}_p[x]/(f)\,.$$

2) *φ — единственный в I_φ нормированный многочлен минимальной степени.*

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 I_φ — идеал в кольце $\mathbb{F}_p[x]/(f)$.

1.

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

2.

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

2. Покажем, что в I_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:

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

$\square$

Теорема 2.12. *Пусть φ — неприводимый нормированный делитель многочлена $f \in \mathbb{F}_p[x]$ и* $\deg\varphi = k < \deg f = n$.

Тогда идеал (φ) — векторное пространство размерности $n-k$.

Доказательство. Без доказательства. $\square$

Циклическое пространство. Будем изучать кольцо вычетов по модулю $x^n - 1$.

- Пусть V — n-мерное векторное пространство над некоторым полем F.
- Фиксируем некоторый базис V.
- Тогда $V \cong F^n =$ $= \{\,(a_0, \ldots, a_{n-1}) \mid a_i \in F,\ i = 0, 1, \ldots, n-1\,\}$ — 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. набор $(a_{n-1}, a_0, \ldots, a_{n-2})$ (а следовательно и все циклические сдвиги на произвольное число позиций влево и вправо).

В кольце $\mathbb{F}_p[x]/(x^n-1)$, рассматриваемом как 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 $\overline{x}$:

$$\overline{a_0 + a_1x + \ldots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}} \cdot \overline{x} = \\ = \overline{a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1} + a_{n-1}x^n} = \\ = \overline{a_{n-1} + a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1}},$$

т.к. в этом кольце $x^n = 1$.

Теорема 2.13. *Пусть I — подпространство кольца $\mathbb{F}_p[x]/(x^n-1)$. Тогда*

$$I \text{ — } \textit{циклическое} \Leftrightarrow I \lhd \mathbb{F}_p[x]/(x^n-1).$$

Доказательство.

- Если подпространство I — идеал, то оно замкнуто относительно умножения на $\overline{x}$, а это умножение и есть циклический сдвиг $\Rightarrow$ I — циклическое.

- 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.

$\square$

Примитивные корни (т.е. корни из 1)

Было показано: *любой многочлен с коэффициентами из $\mathbb{F}_p$ разлагается на линейные множители в некотором поле (разложения) $GF(q) = \mathbb{F}_p^n$ характеристики p, $q = p^n$.*

Пусть $\mathbb{F}_q$ — поле характеристики p, в котором разлагается бином $x^n - 1$. Справедливо:

- Поскольку в $\mathbb{F}_q$ справедливо $x^{kp} - 1 = (x^k - 1)^p$, интересен случай, когда n взаимно просто с p: тогда у многочлена $x^n - 1$ *кратных* корней нет. Иначе корни $x^n - 1$ суть все корни $x^k - 1$, но p-й кратности.

- Равенство $x^n = 1$ означает, что $\operatorname{ord} x \mid n$ в циклической группе $\mathbb{F}_q^*$.

Вывод: корни бинома $x^n - 1 = 0$ образуют *группу корней степени n из единицы* — подгруппу в $\mathbb{F}_q^*$.

Эта подгруппа также циклическая; её порождающие элементы называются *примитивными корнями степени n*.

Подгруппа в циклической группе существует iff её порядок делит порядок циклической группы $\Rightarrow$ поле

$\mathbb{F}_q$ содержит группу корней из единицы степени n iff $n \mid (q-1)$.

Чтобы вернуться от разложения $x^n - 1$ на *линейные* множители в поле $GF(q) = \mathbb{F}_p^n$ (корни из 1) к разложению на *неприводимые* множители в поле $\mathbb{F}_p$, нужно понять, *какие корни из единицы будут входить в неприводимый делитель* $f(x)$.

Если β — корень $f(x)$, то β^p, β^{p^2} и т.д. — также его (*сопряжённые*) корни $\Rightarrow$ количество и степени многочленов-неприводимых делителей $x^n - 1$ можно найти, разбив $\mathbb{F}_p$ на *орбиты* отображения

$$\omega \mapsto p\omega \mod n.$$

Пример 2.18. 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 $\mathbb{F}_p[x]$ и конечные поля: резюме

- Любое конечное целостностное кольцо является полем.
- 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 (не имеющие несобственных делителей) многочлены.

  Кольцо $\mathbb{F}_p[x]$ — 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 β расширенного поля есть нормированный многочлен минимальной степени, для которого β является кор-

нем. 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. *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 2.2 (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

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

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

<u>Задача</u> 2.3. *Построить поле из 4-х элементов.*

Решение. Это поле $\mathbb{F}_2^2$, оно может быть построено как фактор-кольцо $\mathbb{F}_2[x]/\left(a(x)\right)$, 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[6]:

$+$	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 2.4. *В поле* $F = \mathbb{F}_2^2$ *вычислить произведение*

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

где $\beta_1,\, \beta_2,\, \beta_3$ *— все ненулевые элементы поля.*

Решение. Имеем

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

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

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

[6] операции с 0 опускаем

$$= (x+1)\left(x^2+\alpha x+x+\alpha x+\alpha^2+\alpha\right) =$$
$$= (x+1)\left(x^2+x+\alpha^2+\alpha\right) =$$
$$= \left(x^3+(\alpha+1)x^2+(\alpha+1)x^2+(\alpha^2+\alpha+1)x+ \right.$$
$$\left. +\alpha^2+\alpha\right) = x^3+1,$$

как и следует по Теореме 2.4:
$$(x-\beta_1)\cdot\ldots\cdot(x-\beta_{p^n-1}) = x^{p^n-1}-1.$$

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

Решение. Имеем:

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

Задача 2.6. *Найти*
НОД $\left(x^5+x^2+x+1,\, x^3+x^2+x+1\right)$ *над* $\mathbb{Z}_2[x]$.

Решение. Воспользуемся алгоритмом Евклида:
$$x^5+x^2+x+1 = (x^2+x)(x^3+x^2+x+1)+(x^2+1),$$
$$x^3+x^2+x+1 = (x+1)(x^2+1)+0.$$

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, …, 6 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.

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

$\underline{\beta=x:}$ $m_\beta(x) = a(x) = x^3+x+1.$

$\underline{\beta=x^2:}$ $\beta^2,\ \beta^4=\beta(\beta+1)=\beta^2+\beta,\ \beta^8=\beta^4+\beta^2=\beta,$

$$\begin{aligned} m_\beta(x) &= (x-\beta)(x-\beta^2)(x-\beta^4) = \\ &= \left(x^2+(\beta^2+\beta)x+\beta^3\right)(x+\beta^4) = \\ &= x^3+(\beta^4+\beta^2+\beta)x^2+(\beta^3+\beta^4(\beta^2+\beta))x+\beta^7; \end{aligned}$$

вычисляем коэффициенты м.м.:

$$\begin{aligned} &\beta^4+\beta^2+\beta=\beta^2+\beta+\beta^2+\beta=0,\\ &\beta^3+\beta^4(\beta^2+\beta)=\beta^3(1+\beta^3+\beta^2)=\\ &=(\beta+1)(\beta^3+\beta^2+1)=(\beta+1)(\beta+\beta^2)=\\ &=(\beta+1)\beta(\beta+1)=\beta(\beta^2+1)=\beta^3+\beta=\\ &=\beta+1+\beta=1, \end{aligned}$$

$\beta^7 = 1,$

Итого: $m_\beta(x) = x^3 + x + 1 = a(x)$.

Ясно, что, поскольку все, кроме 1, элементы F^* суть порождающие этой мультипликативной группы, то и их м.м. будут совпадать с $a(x)$.

$\underline{\beta = x^7 = 1:}$ $m_\beta(x) = x - 1$.

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 $GF(2)$, $GF\left(2^2\right)$, $GF\left(2^5\right)$, $GF\left(2^6\right)$, $GF\left(2^{10}\right)$, $GF\left(2^{15}\right)$ и само поле $GF\left(2^{30}\right)$.

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. $$\begin{array}{rrrr|r}
x^3 & +\,2x^2 & +\,4x & +\,1 & x+3 \\ \cline{5-5}
x^3 & +\,3x^2 & & & x^2+4x+2 \\ \cline{1-2}
 & 4x^2 & +\,4x & & \\
 & 4x^2 & +\,2x & & \\ \cline{2-3}
 & & 2x & +\,1 & \\
 & & 2x & +\,1 & \\ \cline{3-4}
 & & & 0 &
\end{array}$$
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 ($\cong \mathbb{F}_7^2$).

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

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

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

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. $\underline{x^4 = x + 1}$

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

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

2. $\underline{x^4 = x^3+1}$

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

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

<u>Задача</u> 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. $\underline{((7))\text{ над }\mathbb{F}_2}$

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

$((1)) = 2$: 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* $F = \mathbb{F}_3[x]/\big(-2x^2 + x + 2\big)$ *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 $x^4 = 1$:

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

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:

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

<u>Задача</u> 2.20. *Для поля* $F = \mathbb{F}_3[x]/\big(x^2+1\big) \cong \mathbb{F}_3^2$ *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 $\operatorname{ord} x = 4 \neq 8$ 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 $x+1$:

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

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

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

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?

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

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 $f(x) \nmid a(x)$? Тогда кратные $f(x)$ составят в R идеал (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.

$$
\begin{array}{ll}
\text{Шаг 0.} & \textit{// Инициализация}\\
& r_{-2}(x) \;=\; x^4 + x^3 + x^2 + 3,\\
& r_{-1}(x) \;=\; x^2 + x + 3,\\
& y_{-2}(x) \;=\; 0,\\
& y_{-1}(x) \;=\; 1.
\end{array}
$$

$$
\begin{array}{ll}
\text{Шаг 1.} & \textit{// Делим } r_{-2}(x) \textit{ на } r_{-1}(x) \textit{ с остатком}\\
& r_{-2}(x) \;=\; r_{-1}(x)q_0(x) + r_0(x),\\
& q_0(x) \;=\; x^2 + 5,\\
& r_0(x) \;=\; 2x + 2,\\
& y_0(x) \;=\; y_{-2}(x) - y_{-1}(x)q_0(x) \;=\\
& \qquad\quad \;=\; -q_0(x) \;=\; -x^2 - 5.
\end{array}
$$

$$
\begin{array}{ll}
\text{Шаг 2.} & \textit{// Делим } r_{-1}(x) \textit{ на } r_0(x) \textit{ с остатком}\\
& r_{-1}(x) \;=\; r_0(x)q_1(x) + r_1(x),\\
& q_1(x) \;=\; 4x,\\
& r_1(x) \;=\; 3,\\
& y_1(x) \;=\; y_{-1}(x) - y_0(x)q_1(x) \;=\\
& \qquad\quad \;=\; 1 + 4x(x^2 + 5) \;=\; 4x^3 + 6x + 1.
\end{array}
$$

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*

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

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

$$\begin{aligned} r_{-2}(x) &= r_{-1}(x)q_0(x) + r_0(x), \\ q_0(x) &= 4x + 4, \\ r_0(x) &= 1, \ // \ \deg r = 0 \ \Rightarrow \ \textit{ОСТАНОВ} \\ y_0(x) &= y_{-2}(x) - y_{-1}(x)q_0(x) = \\ &\quad = -q_0(x) = -4x - 4 = x + 1. \end{aligned}$$

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:

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

— делится!

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

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

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:

$$\alpha^2 = -2\alpha - 2 = \alpha + 1,$$
$$\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1$$

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. —

$$\begin{aligned} m_{\alpha^3}(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = \\ &= x^4 + \left(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\right)x^3 + \\ &+ \left(\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12}\right)x^2 + \\ &+ \left(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12}\right)x + \\ &+ \left(\alpha^3\alpha^6\alpha^9\alpha^{12}\right) = x^4 + \left(\alpha^3+(\alpha^3+\alpha^2)+(\alpha^3+\alpha)+\right. \\ &+ \left.(\alpha^3+\alpha^2+\alpha+1)\right)x^3 + (\ldots)\,x^2 + (\ldots)\,x + \alpha^{30} = \\ &= x^4+x^3+x^2+x+1. \end{aligned}$$

$\beta = \alpha^5$: 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. —

$$\begin{aligned} m_{\alpha^7}(x) &= (x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14}) = \\ &= x^4+x^3+1. \end{aligned}$$

<u>Задача</u> 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:

$$\begin{aligned} x^5 &= \big(x^2\big)^2 x = x(4x+3)^2 = x(x^2+4x+4) = \\ &= x(4x+3+4x+4) = x(3x+2) = 3x^2+2x = \\ &\qquad\qquad = 2x+4+2x = 4x+4. \end{aligned}$$

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 $d \in \left\{\frac{24}{2} = 12,\, \frac{24}{3} = 8\right\}$. Имеем:

$$\begin{aligned} x^4 =& (x^2)^2 = (4x+3)^2 = x^2+4x+4 = \ldots \\ & \ldots = 3x+2 \neq 1, \\ x^8 =& (x^4)^2 = (3x+2)^2 = -x^2+2x+4 = \ldots \\ & \ldots = 3x+1 \neq 1. \\ x^{12} =& x^8x^4 = (3x+1)(3x+2) = -x^2+4x+2 = \ldots \\ & \ldots = 4 \neq 1. \end{aligned}$$

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[7] 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 $\{\,\overline{0},\, \overline{1},\, \ldots,\, \overline{7}\,\}$ 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;

[7] 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):

$$
\begin{aligned}
& x^8 - 1 = (x^4 - 1)(x^4 + 1), \\
& x^4 - 1 = (x^2 - 1)(x^2 + 1), \\
& x^2 - 1 = (x - 1)(x + 1), \\
& x^2 + 1 \equiv_5 x^2 - 4 = (x - 2)(x + 2), \\
& x^4 + 1 \equiv_5 x^4 - 4 = (x^2 - 2)(x^2 + 2), \\
& \qquad \text{итого в } \mathbb{F}_5[x] : \\
& x^8 - 1 = (x + 1)(x - 1)(x + 2)(x - 2)(x^2 + 2)(x^2 - 2).
\end{aligned}
$$

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[1]:

1) входной поток информации разбить на *сообщения* — непересекающиеся блоки фиксированной длины k;
2) каждый блок *кодировать* (модифицировать) —
   а) независимо от других — *блоковое кодирование*;

[1] один из возможных!

б) в зависимости от предыдущих — *свёрточное* или *потоковое кодирование* (турбо-коды и др.).

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 помехозащищённости вместо этих сообщений передают *кодовые слова*, каждое длины $n > k$, т.е. вводят *избыточность* при передаче информации.

Более формально:

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.

Чем меньше избыточность $m = n - k$ 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.

Понятия, связанные с булевым кубом — напоминание из дискретной математики.

- *Норма* или *вес* $\|\widetilde{\gamma}\|$ = число единичных координат в наборе $\widetilde{\gamma} \in B^n$.

- *Метрика* (вспоминаем, что это такое) на множестве бинарных наборов — *хэммингово расстояние* ($+$ — сумма по $\mathrm{mod}\ 2$):

$$\rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) = \left\|\widetilde{\alpha} + \widetilde{\beta}\right\|.$$

- *Шар Хэмминга с центром в* $\widetilde{\alpha}$ *и радиусом* $r > 0$:

$$S_r\left(\widetilde{\alpha}\right) = \left\{ \widetilde{\beta} \in B^n \mid \rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) \leqslant r \right\}.$$

Ричард Уэсли Хэмминг
(Richard Wesley Hamming, 1915–1998) — американский математик, работы которого в сфере теории информации оказали существенное влияние на компьютерные науки и телекоммуникации.
В 1950 г. опубликовал способ построения кода, исправляющего одну ошибку и названный впоследствии его именем.

Кодовое расстояние

Определение 3.1. Минимальное расстояние между словами кода C называется его *кодовым расстоянием*, символически 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 при передаче сообщения $\widetilde{\alpha}$ сделано не более r ошибок, то набор останется в шаре $S_r(\widetilde{\alpha})$. Если шары не пересекаются, то искомое кодовое слово α — ближайшее к полученному набору. □

Следствие. *У кода, исправляющего r ошибок, кодовое расстояние d должно быть не менее $2r+1$.*

Определение кодового расстояния произвольного кода C — *трудоёмкая задача*: требуется перебрать все $\frac{2^k(2^k-1)}{2}$ пар кодовых слов, что практически невозможно уже начиная с $k = 50$: показано, что эта задача NP-тудна.

Поэтому при помехоустойчивом кодировании на первый план выходит проблема построения 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 $k = 1$, $n = 3$, $d = 3$). Информация разбивается на блоки по одному биту, т.е. передаются $t = 2$ сообщения: $S_0 = 0$ и $S_1 = 1$.

Кодирование $\qquad 0 \mapsto 000, \quad 1 \mapsto 111$
исправляет одну ошибку. Однако такое кодирование крайне неэффективно: длина сообщения *утраивается*.

Тривиальный код-повторение $a \mapsto \underbrace{a \ldots a}_{2r+1}$, очевидно, исправит r ошибок.

Кодирование. Будем обозначать каждое сообщение вектором-столбцом $\boldsymbol{u} \in \{0,1\}^k$:

$$\boldsymbol{u} = \begin{bmatrix} u_1 \\ \cdots \\ u_k \end{bmatrix}.$$

<u>Определение</u> 3.2.

- $\boldsymbol{v}$ — кодовое слово длины $n = k + m$.

  В случае *разделимого блокового кодирования* кодовое слово содержит сообщение $\boldsymbol{u}$ в своих *информационных битах* и, кроме того, ещё m *проверочных бит*.

- Множество $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_t\}$ всех $t = 2^k$ кодовых слов длины n — (n,k)-*код*, или, с кодовым расстоянием — (n,k,d)-*код*.

- $R = k/n$ — *скорость*, $m/n = 1 - R$ — *избыточность кода*.

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:

$$\boldsymbol{v} \;\rightarrow\; \boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e},$$

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 кодов *обычно значительно сложнее* кодирования[2]. Декодирование (n,k,d)-кода основано на:

- разбиении единичного куба B^n на k областей, содержащих шары радиуса $r = \lfloor (d-1)/2 \rfloor$ с центрами в кодовых словах;
- предположении, что произошло $\leqslant r$ ошибок.

Декодирование блокового разделимого (n,k) *кода* проводится в два этапа:

$$\boldsymbol{u} \xrightarrow[\text{избыточность}]{\text{кодирование}} \boldsymbol{v} \xrightarrow[+e]{\text{ошибка}} \boldsymbol{w} \xrightarrow[\text{ближ. код. слово}]{\text{декод.-1}} \widehat{\boldsymbol{v}} \xrightarrow[\text{удаление избыт.}]{\text{декод.-2}} \widehat{\boldsymbol{u}}$$

1-й этап: *Восстановление переданного кодового слова* $\widehat{\boldsymbol{v}}$ как ближайшего к $\boldsymbol{w}$ в метрике Хэмминга — нахождение центра соответствующего шара.
Для этого надо, вообще говоря, перебрать все 2^n строк в $2^n \times k$-таблице кодовых слов.

[2] Известны, однако, т.н. *экспандерные* коды с линейной сложностью декодирования, для которых неизвестны субквадратичные алгоритмы кодирования, но это — исключение. Экспандерные коды дают лучший из известных компромиссов между скоростью кода k/n, кодовым расстоянием d и быстротой декодирования.

Если расстояние до ближайшего центра шара превышает $\lfloor (d-1)/2 \rfloor$, то произошло больше ошибок, чем может исправить код и при декодировании необходимо выдать *отказ*.

2-й этап: *Восстановление исходного сообщения* $\widehat{\boldsymbol{u}}$ по кодовому слову $\widehat{\boldsymbol{v}}$ путём удаления проверочных бит — элементарная процедура.

Вывод: декодирование блокового (n, k)-кода *общего вида* — очень ресурсоёмкий процесс, поэтому его 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 максимального размера, исправляющий 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 в (нетривиальных) случаях:

1) $n = 2^q - 1$, $r = 1$ — *коды Хэмминга*, у них $m = q$ и
2) $n = 23$, $r = 3$ — *код Голея*, к него $m = 11$.

Это *совершенные* или *экстремальные коды.*

Тривиальные коды: $(n, 0, 0)$ — с 2^n кодовыми словами; $(2r+1, 1, r)$ — с повторением нечётной длины и $(n, 0, n)$.

Теорема 3.1 (Хэмминга). *При* $2r < n$ *максимальное число* t *кодовых слов находится в пределах*

$$\frac{2^n}{C_n^0 + C_n^1 + \ldots + C_n^{2r}} \leqslant t \leqslant \frac{2^n}{C_n^0 + C_n^1 + \ldots + C_n^r}.$$

Доказательство. t есть максимальное число непересекающихся шаров радиуса r, помещающихся в кубе B^n.

Верхняя оценка (граница Хэмминга) — шар радиуса r содержит точки: сам центр $+$ все точки с одной, двумя, ..., r измененными координатами, т.е. всего $C_n^0 + C_n^1 + \ldots + C_n^r$ штук и шары не пересекаются.

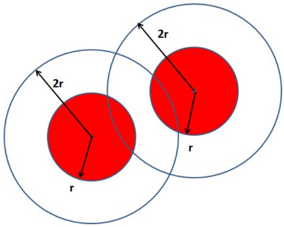
Для *оценки снизу* построим негрупповой код:

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.

$\square$



Построение кода Хэмминга $n = 2^q - 1$, $r = 1$.

Покажем, что в случае $n = 2^q - 1$ получим $t = \frac{2^n}{1+n}$, т.е. верхняя оценка теоремы Хэмминга достигается.

Построим код, а потом определим его кодовое расстояние. Рассмотрим таблицу:

$$k=2^q-(q+1)\left\{\begin{array}{cc}
100\ldots000 & 1100\ldots000\\
010\ldots000 & 1010\ldots000\\
001\ldots000 & 1001\ldots000\\
\ldots & \ldots\\
000\ldots100 & 1111\ldots101\\
000\ldots010 & 1111\ldots110\\
000\ldots001 & 1111\ldots111
\end{array}\right.$$

$$\underbrace{\hphantom{000\ldots001}}_{k=2^q-(q+1)}\quad\underbrace{\hphantom{1111\ldots111}}_{q=m}$$

Слева — единичная матрица порядка $2^q - 1 - q$, справа — все бинарные наборы длины q, содержащие *не менее двух* единиц.

Просуммировав всевозможные совокупности строк таблицы, получим $t = 2^k = 2^{2^q-(q+1)}$ различных кодовых слов, но

$$t = 2^{2^q-(q+1)} = \frac{2^{2^q-1}}{2^q} = \frac{2^n}{1+n}.$$

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 1,

  не менее трёх строк — в левой части будет не менее 3 единиц.

  Т.е. всегда $\rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) \geqslant 3 \;\Rightarrow$ шары единичного радиуса с центрами в полученных наборах не пересекаются.

Пример 3.2 (код Хэмминга длины 7). Имеем $q = 3$, $n = 2^3 - 1 = 7$, $k = 2^3 - (3+1) = 4$.
Для данного параметра $q = 3$ составим таблицу кода Хэмминга:

$$\begin{array}{|cccc|ccc|}
\hline
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
\end{array}$$

Складывая по $\bmod 2$ все совокупности (включая пустую) приведённых 4-х строк, получаем $2^4 = 16$ различных бинарных слов длины 7, которыми можно закодировать 16 сообщений.

Этот код содержит по 1 слову веса 0 и 7, по 7 слов веса 3 и 4; исправляет 1 ошибку, обнаруживает 2-, 5-, 6-кратные ошибки и 80% 3- и 4-кратных.

Число кодовых слов кода Хэмминга с различными весами есть коэффициенты *производящего полнома*

$$W(z) = \frac{1}{n+1}\left[(1+z)^n + n(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}\right].$$

Например, для $n = 7$ получим

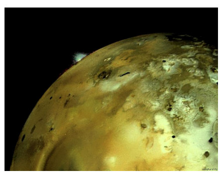
$$W(z) = \frac{1}{8}\left[(1+z)^7 + n(1+z)^3(1-z)^4\right] = \\ = 1 + 7z^3 + 7z^4 + z^7,$$

т.е. уже известные значения 1, 7, 7 и 1 для числа кодовых слов веса 0, 3, 4 и 7 соответственно.

Является ли кодом Хемминга тривиальный $(3,1)$-код?

Марсель Голей
(Marcel J. E. Golay, 1902–1989)
— швейцарский математик и физик.
В своей единственной работе по теории информации (1949) предложил совершенный двоичный код, исправляющий три ошибки.

В ходе космической программы США *Вояджер* (1979-81) для передачи цветных изображений Юпитера и Сатурна использовался код Голея.



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

$$t = \frac{2^{23}}{2^{11}} = 2^{12} = 4096$$

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 $(2^q - 1,\ 1)$ — код Хэмминга и тривиальных случаев[3] 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* $\operatorname{mod} 2$».

[3] см. с. 125

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*

$$d = \min_{\widetilde{\alpha} \neq \widetilde{\beta}} \rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) = \min_{\widetilde{\gamma} \neq \widetilde{0}} \|\widetilde{\gamma}\|,$$

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:

$$\rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) = \left\|\widetilde{\alpha} + \widetilde{\beta}\right\| = \|\widetilde{\gamma}\|,$$

причем $\widetilde{\gamma} \neq \widetilde{0}$ при $\widetilde{\alpha} \neq \widetilde{\beta}$.

Отсюда получаем оценку $\min\limits_{\widetilde{\alpha} \neq \widetilde{\beta}} \rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) \geqslant \min\limits_{\widetilde{\gamma} \neq \widetilde{0}} \|\widetilde{\gamma}\|$, которая достигается, например, при $\widetilde{\beta} = \widetilde{0}$. □

Следствие. *Для вычисления кодового расстояния группового кода достаточно перебрать $2^k - 1$ кодовых слов.*

$\{0, 1\}^n = B^n$ есть n-мерное координатное векторное пространство над конечным полем $\mathbb{F}_2 = \{0, 1\}$.

Определение 3.3. Блоковый (n, k)-код C 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 $d = \min\limits_{\widetilde{\gamma} \in C} \|\widetilde{\gamma}\|$;
3) существует базис $\{\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{k-1}\}$ из k векторов $\boldsymbol{g}_i \in B^n$, $i = 0, \ldots, k-1$, 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 и проверочная матрицы. *Линейный код: матричное представление*

$$\boldsymbol{v} = \sum_{i=0}^{k-1} u_i \boldsymbol{g}_i = G\boldsymbol{u}, \text{ где } G_{n \times k} = [\,\boldsymbol{g}_0\, \boldsymbol{g}_1 \ldots \boldsymbol{g}_{k-1}\,]$$

— *порождающая матрица* кода.

Пример 3.3 ((7, 4)-код Хэмминга). Ранее была получена таблица, сложением строк которой получаются все $2^4 = 16$ кодовых слов. Порождающая матрица получается транспонированием этой таблицы:

$$G_{7\times 4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

— порождающая матрица в *систематической форме*: при кодировании исходные сообщения помещаются в первые 4 бита кодового слова

Проверочная матрица[4] $H_{m\times n}$, $m = n - k$ для линейного (n, k)-кода обладает свойством $H\boldsymbol{v} = \mathbf{0}$ для любого *кодового слова* $\boldsymbol{v}$.

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.

Пример 3.3 (продолжение — (7, 4)-код Хэмминга). Для построенной порождающей матрицы $G_{7\times 4}$ проверочной будет

$$H_{3\times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Характеристики кода Хэмминга

- Код содержащий $q = m$ проверочных бит, длины $n = 2^m - 1$, исправляющий одну ошибку.

[4] её называют также *матрицей проверки на чётность*, а строки — *правилами проверки на чётность*

- *Совершенный код* — осуществляет плотную упаковку: куб B^{2^m-1} разбивается на $t = \frac{2^n}{n+1} = 2^{2^m-(m+1)}$ шаров единичного радиуса с центрами в кодовых словах.
- *Скорость кода* — $R = 1 - m/(2^m - 1)$.
- *Столбцы проверочной матрицы* — все ненулевые векторы из 2^m.

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.*

Часто к порождающей матрице линейного кода добавляют единичную строку, получая *расширенный код.* В результате кодовые слова пополняются битом чётности.

Расширенный кода Хемминга имеет кодовое расстояние 4 и способен либо обнаруживать ошибки, кратности не выше 3, либо исправлять все одиночные ошибки, одновременно обнаруживая все двукратные.

3.3 Кодирование линейными кодами

$$\boldsymbol{u} \xrightarrow[\text{избыточность}]{\textit{кодирование}} \boldsymbol{v} = G\boldsymbol{u}$$

Систематическое (*разделимое*) кодирование упрощает декодирование: при нём биты сообщения копируются в заранее *фиксированные позиции* кодового слова.

Возможность разделимого кодирования основана на том, что матрица G определена с точностью до эквивалентных преобразований *столбцов*, при котором осуществляется переход к другому базису того же кода.

Пример 3.4 (систематического кодирования). Пусть линейный код задан порождающей матрицей G.

С помощью эквивалентных преобразований столбцов матрица G может быть приведена к виду, в котором *первые* k строк образуют единичную матрицу I_k:

$$G_{n\times k} \longrightarrow \widetilde{G}_{n\times k} = \begin{bmatrix} I_k \\ P_{m\times k} \end{bmatrix}$$

Тогда кодирование $\boldsymbol{v} = \widetilde{G}\boldsymbol{u}$ будет систематическим: первые k бит кодового слова $\boldsymbol{v}$ являются битами исходного сообщения $\boldsymbol{u}$.

Вопрос: Что произойдёт при перестановке *строк* кодирующей матрицы? Будет задан *другой линейный код* — другие наборы из B^n будут кодовыми словами, но кодовое расстояние и, следовательно, корректирующая способность останется прежней.

То же будет и при преобразовании столбцов линейными комбинациями. Коды, полученные комбинациямитаких преобразований называют *эквивалентными*.

Любой линейный код можно преобразовать в эквивалентный ему систематический код.

Ортогональное дополнение к подпространству кода. Итак, C — k-мерное подпространство $\{0,1\}^n = B^n$. Элементы B^n, ортогональные ко всем элементам 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 $C^{\perp}$.

Определение 3.4. Пусть $\{\boldsymbol{h}_0, \ldots, \boldsymbol{h}_{m-1}\}$ — базис $C^{\perp}$, $\boldsymbol{h}_i \in B^n$, $i = 0, \ldots, m-1$. 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* кода C.

Ясно, что

- $\forall \boldsymbol{v} \in C : H\boldsymbol{v} = \boldsymbol{0}$ — нулевой m-мерный вектор;
- $HG = O$ — нулевая $(m \times k)$-матрица;
- проверочная матрица определена с точностью до эквивалентных преобразований *строк*.

Например, если линейный код C задан исходной порождающей матрицей G и построена матрица

$$\widetilde{G}_{n\times k} = \begin{bmatrix} I_k \\ P_{m\times k} \end{bmatrix},$$

то проверочной матрицей H кода C будет

$$H_{m\times n} = \begin{bmatrix} P_{m\times k} & I_m \end{bmatrix}$$

Действительно, в этом случае

$$H\boldsymbol{v} = H\widetilde{G}\boldsymbol{u} = \begin{bmatrix} P_{m\times k} & I_m \end{bmatrix} \times \begin{bmatrix} I_k \\ P_{m\times k} \end{bmatrix} = (P+P)\boldsymbol{u} = \\ = \boldsymbol{O}\boldsymbol{u} = O.$$

Таким образом, линейный код для сообщений длины k имеет длину $n = k + m$ и задаётся

либо *порождающей* матрицей H размера $n{\times}k$,
либо *проверочной* матрицей G размера $m{\times}n$.

Эти матрицы определены с точностью до эквивалентных преобразований *столбцов и строк соответственно*, что соответствует выбору *различных базисов* в пространствах C и $C^{\perp}$, однако *фиксирование позиций информационных бит при систематическом кодировании* задаёт порождающую и проверочную матрицу *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 3.5 (кодирования блоковым линейным кодом). Пусть дан линейный $(6,3)$-код C 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 (только 3-й бит сообщения перейдёт в 1-й бит кодового слова):

$$[\,\boldsymbol{v}_1^n\,\boldsymbol{v}_2^n\,] = G\times[\,\boldsymbol{u}_1\,\boldsymbol{u}_2\,] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

1 (б). Для систематического кодирования с помощью эквивалентных 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 последней 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

$$H_{3\times 6} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Базис C суть столбцы матрицы G (или $\widetilde{G}$), а базис $C^{\perp}$ — строки матрицы H:

$$G = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad \widetilde{G} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad H^T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Убедитесь, 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 $d = 3$

$$= \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

3.4 Декодирование линейных кодов

Методы декодирования линейных кодов основаны на предположении о минимальном числе произошедших ошибок.

Тривиальный метод. Пусть передано кодовое слово $\boldsymbol{v}$, а принято слово

$$\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}.$$

Хотя в этом равенстве известно только $\boldsymbol{w}$, но $\boldsymbol{v} \in C$ и, по предположению, вес вектора ошибок $\boldsymbol{e}$ минимален. Поэтому перебирая все кодовые слова можно вычислять векторы ошибок $\boldsymbol{e}_i = \boldsymbol{w} + \boldsymbol{v}_i$, $i = \overline{1, 2^k}$ и выбрав $\boldsymbol{e}_0$ минимального веса, восстановить слово $\widehat{\boldsymbol{v}} = \boldsymbol{w} + \boldsymbol{e}_0$.

Ясно, что такой метод требует хранения таблицы всех кодовых слов размера $n \times 2^k$ и реализации алгоритма нахождения вектора ошибки минимального веса.

Известны более эффективные методы декодирования линейных кодов, основанные на вычислении исправляющего вектора, который принято называть синдромом[5].

Синдром. Декодирование линейных кодов

Определение 3.5. *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[6];

[5] *Синдром* — совокупность явлений, вызванных отклонением от нормы.

[6] 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.

- $\boldsymbol{s} = H\boldsymbol{w} = H(\boldsymbol{v}+\boldsymbol{e}) = \underbrace{H\boldsymbol{v}}_{=0} + H\boldsymbol{e} = H\boldsymbol{e}.$

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

$$H\boldsymbol{v} = \boldsymbol{0},$$

(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 $G\boldsymbol{u}$ соответствующей однородной —

$$\boldsymbol{e} = \widehat{\boldsymbol{e}} + G\boldsymbol{u}.$$

и среди всех возможных векторов $\widehat{\boldsymbol{e}}$ необходимо выбрать имеющий минимальный вес.

Схема декодирования:

$$\boldsymbol{w} \xrightarrow{\qquad\qquad} \boldsymbol{s} = H\boldsymbol{w} \xrightarrow[H\boldsymbol{e}=\boldsymbol{s}]{} \boldsymbol{e} = \widehat{\boldsymbol{e}} + G\boldsymbol{u} \xrightarrow[\|\boldsymbol{e}\|\to\min]{} \widehat{\boldsymbol{v}} = \boldsymbol{w} + \boldsymbol{e}$$

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 3.6 (декодирования линейного кода). Рассмотрим линейный $(6,3)$-код из *Примера* 3.5.

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* 3.5), 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 $\boldsymbol{w} = [1\ 1\ 1\ 1\ 0\ 0]^T$:

$$Hw = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \boldsymbol{s},$$

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 $H_{m\times(2^m-1)}$ кода Хэмминга является то, что её столбцы представляют собой двоичные коды чисел от 1 до $2^m - 1$. Например, в *Примере* 3.3 получена матрица

$$H_{3\times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

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 *последовательно* быть двоичными представлениями чисел от 1 до $2^m - 1$. 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}.

Например, для $q = 3$ это матрица

$$\widetilde{H}_{3\times 7} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

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, оставшейся после удаления из неё единичной подматрицы. Тогда, как легко проверить, $HG = O$ — нулевая (3×4)-матрица.

Дуальные коды. Поскольку $HG = O$ — нулевая матрица, можно использовать H как порождающую, а G — 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 $k < n$. При заданных значениях n и k существует $2^{n(n-k)}$ линейных кодов.
- Требование линейности производить позволяет упростить кодирование и декодирование.

  1. *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.

  2. *Декодирование* осуществляется с помощью легко вычисляемых синдромов. На первом этапе:

     1) заранее определяются виды синдромов для возможных вариантов искажений кодовых комбинаций;

2) в декодере вычисляется синдром;
3) производится определение позиции ошибки, соответствующей рассчитанному синдрому;
4) производится коррекция кодовой комбинации.

Второй этап декодирования при систематическом кодировании элементарен. Однако процесс декодирования остаётся трудоёмким.

3.5 Циклические коды

Определение и построение циклических кодов

Определение 3.6. 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.

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;
- в общем случае определение кодового расстояния циклического кода, а это чрезвычайно трудоёмкая задача.

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 $u(x)$, $v(x) \in \mathbb{F}_2[x]$:

$$\begin{aligned} \boldsymbol{u} &= \left[\, u_0,\, u_1,\, \ldots,\, u_{k-1} \,\right]^T \leftrightarrow \\ &\qquad \leftrightarrow\ u(x) = u_0 + u_1 x + \ldots + u_{k-1} x^{k-1}, \\ \boldsymbol{v} &= \left[\, v_0,\, v_1,\, \ldots,\, v_{n-1} \,\right]^T \leftrightarrow \\ &\qquad \leftrightarrow\ v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}. \end{aligned}$$

Любое кодовое слово $v(x)$ представляется в виде

$$v(x) \in (g(x)) = \{\, g(x)q(x) \mid q(x) \in \mathbb{F}_2[x],\ x^n = 1 \,\}\,.$$

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.* Чтобы полиномиальный код был циклическим, порождающий полиномом должен быть делителем $x^n - 1$, n — длина кодового слова.

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 двух последних 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 3.7 (построения циклического кода). Построим *циклический код длины* $n = 23$.

Для определения порождающего полинома кода находим разложение бинома $x^{23} - 1$ на неприводимые многочлены.

Один корень находится сразу: это 1 и имеем разложение

$$x^{23} + 1 = (x+1)(\underbrace{x^{22} + x^{21} + \ldots + x^2 + x + 1}_{f(x)}).$$

Перебором неприводимых над $\mathbb{F}_2$ полиномов находим

$$f(x) = (\underbrace{x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1}_{f_1(x)})\times$$
$$\times (\underbrace{x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1}_{f_2(x)})$$

Поскольку $\deg f_1(x) = \deg f_2(x) = 11 = m$, любой из полиномов $f_1(x)$, $f_2(x)$ может быть выбран порождающим[7] 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.

[7] 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 $m = 12$.

Ясно, что построен *код Голея.*

Заметим, что делители бинома $x^{23} - 1$ пришлось искать перебором.

Кодирование циклическими кодами. Пусть определён порождающий полином $g(x)$: $g(x) \mid x^n - 1$, $\deg g(x) = m < n$, задающий код C.

Несистематическое кодирование осуществляется путём умножения кодируемого полинома на порождающий:

$$u(x) \;\mapsto\; v(x) \;=\; g(x)u(x).$$

Систематическое кодирование осуществляется приписыванием к кодовому слову *слева (в младшие разряды)* остатка $r(x)$ от деления $x^m u(x)$ на $g(x)$.

Поскольку

$$x^m u(x) \;=\; g(x)q(x) \,+\, r(x) \quad \text{и} \quad \deg r(x) < m,$$

то $x^m u(x) + r(x) = g(x)q(x) \in C$ и систематическое кодирование может быть задано как

$$u(x) \;\mapsto\; v(x) \;=\; x^m u(x) + r(x),$$

при котором полином $v(x)$ содержит k коэффициентов полинома $u(x)$ в k *крайних правых позициях* (при старших степенях x).

Пример 3.8. 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

$$x^7 - 1 = x^7 + 1 = (x+1)(x^3+x+1)(x^3+x^2+1).$$

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*[8]. Выберем конкретно $g(x) = x^3 + x + 1$.

2. Закодируем несистематическим и систематическим кодами сообщение

$$\boldsymbol{u} = [0\ 0\ 1\ 1]^T \leftrightarrow u(x) = x^3 + x^2.$$

Несистематическое кодирование.

$$v(x) = u(x)g(x) = (x^3+x^2)(x^3+x+1) =$$

[8] Ясно, это код Хэмминга!

$$= x^6 + x^5 + x^4 + x^2 \leftrightarrow [0\ 0\ 1\ 0\ 1\ 1\ 1]^T = \boldsymbol{v}.$$

Систематическое кодирование. Находим остаток $r(x)$ от деления многочлена $x^3u(x)$ на $g(x)$:

$$x^3(x^3 + x^2) = x^6 + x^5 = (x^3 + x^2 + x)(x^3 + x + 1) + \underline{x},$$

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 3.7. *Синдромом полинома* $w(x)$, принятого при передаче сообщения закодированного циклическим кодом и, возможно, содержащего ошибки, назовём остаток $s(x)$ 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 решение 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[9].

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.*

- *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. Для его обхода используют т. н. *укороченные циклические коды.*

[9] Существуют и альтернативные методы декодирования циклических кодов общего вида (декодеры Меггита, Касами-Рудольфа, пороговый, мажоритарный, ...) также экспоненциальной по k трудоёмкости.

- *Кодирование* и *декодирование* сводится к выполнению операций умножения и деления полиномов, *легко реализуемые* на регистрах сдвига с обратными связями.

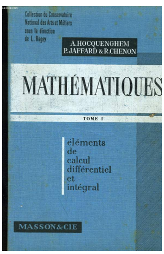
  Однако алгоритмы декодирования по-прежнему имеют *экспоненциальную сложность* по k.

3.6 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. Коды предложены Р. Ч. Боузом и Д. К. Рей-Чоудхури в 1960 г. независимо от опубликованной на год ранее работы А. Хоквингема.

Радж Чандра Боуз
(Raj Chandra Bose, 1901–1987) — индийский математик, работавший в США.

Двайджендра Камар Рей-Чоудхури
(Dwijendra Kumar Ray-Chaudhuri, 1933) — индийский математик, работающий в США. Обладатель медали Эйлера за вклад в развитие комбинаторики.



Алексис Хоквингем
(Alexis Hocquenghem[10], 1908?–1990) — французский математик. В его работе 1959 г. содержится первое описание линейных циклических кодов, исправляющих кратные ошибки.

[10] Hocquenghem является галицинизированной формой германской или фламандской фамилии, правильное её чтение — *О́кенгем*.

Основные свойства минимальных многочленов (напоминание).

1. $\forall\,\beta \in \mathbb{F}_p^n \quad \exists!\, m_\beta(x)$, м.м. $m_\beta(x)$ неприводим и $\deg m_\beta(x) \leqslant n$;
2. Если $f(x) \in \mathbb{F}_p[x]$ и $f(\beta) = 0$, то $m_\beta(x) \mid f(x)$.
3. Минимальный многочлен примитивного элемента поля называется *примитивным многочленом.*

Циклотомический класс элемента поля. Напомним, что если β — корень неприводимого многочлена $f(x) \in \mathbb{F}_p[x]$ степени n, то

$$\left\{ \beta,\ \beta^p,\ \beta^{p^2},\ \ldots,\ \beta^{p^{n-1}} \right\}$$

— *все* n различных (сопряжённых) корней $f(x)$.

Определение 3.8 (для полей характеристики 2). Пусть $n \mid N$. *Циклотомическим классом* (или *классом сопряжённости*) элемента $\alpha \in \mathbb{F}_2^N$ над 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 $\Rightarrow$ циклотомические классы всех элементов поля $\mathbb{F}_2^N$ образуют *разбиение* его мультипликативной группы.
2. Если α — *примитивный элемент* поля $\mathbb{F}_2^{qn}$, то циклотомический класс α над подполем $\mathbb{F}_2^n$ *содержит ровно* q *элементов*, т.е. это класс
$$\left\{ \alpha^{2^{0\cdot n}} = \alpha,\ \alpha^{2^{1\cdot n}} = \alpha^{2^n},\ \alpha^{2^{2n}},\ \ldots,\ \alpha^{2^{(q-1)\cdot n}} \right\}.$$

3. Если α — *примитивный элемент* поля $\mathbb{F}_2^{qn}$ и циклотомический класс α^k над подполем $\mathbb{F}_2^n$ содержит m элементов, то полином

$$m_\beta(x) = \prod_{t=0}^{m-1}\left(x - (\alpha^k)^{2^t}\right) =$$
$$= x^{m-1} + \lambda_{m-2}x^{m-2} + \ldots + \lambda_1 x + \lambda_0$$

является м.м. *для всех элементов, входящих в данный циклотомический класс.*

Пример 3.9. Приведём примеры разложения *мультипликативных групп* полей $\mathbb{F}_2^{qn}$ на циклотомические классы над $\mathbb{F}_2^n$.

1. $n = 1$, $q = 3$ и α — примитивный элемент поля $\mathbb{F}_2^3 = F$. Тогда $\alpha^7 = 1$ и разложение F^* над $\mathbb{F}_2$ есть (каждый элемент циклотомического класса последовательно умножаем на $2^n = 2$) —
$$\{1\},\ \{\alpha, \alpha^2, \alpha^4\},\ \{\alpha^3, \alpha^6, \alpha^5\}.$$
2. $n = 2$, $q = 2$ и α — примитивный элемент поля $\mathbb{F}_2^4 = F$. Тогда $\alpha^{15} = 1$ и разложение F^* над $\mathbb{F}_2^2$ есть (каждый элемент циклотомического класса последовательно умножаем на $2^n = 4$) —
$$\{1\},\ \{\alpha, \alpha^4\},\ \{\alpha^2, \alpha^8\},\ \{\alpha^3, \alpha^{12}\},\ \{\alpha^5\},$$
$$\{\alpha^{10}\},\ \{\alpha^6, \alpha^9\},\ \{\alpha^7, \alpha^{13}\},\ \{\alpha^{11}, \alpha^{14}\}.$$
3. $n = 1$, $q = 4$ и α — примитивный элемент поля $\mathbb{F}_2^4 = F$. Тогда $\alpha^{15} = 1$ и разложение F^* над $\mathbb{F}_2$ есть (умножение на $2^n = 2$) —
$$\{1\},\ \{\alpha, \alpha^2, \alpha^4, \alpha^8\},\ \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9\},$$
$$\{\alpha^5, \alpha^{10}\},\ \{\alpha^7, \alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{26} = \alpha^{11}\}.$$

БЧХ-коды: определение (простейший случай) и основное свойство

Пусть выбраны параметр q, определяющий длину кода $n = 2^q - 1$ и *конструктивное расстояние* $d_c < n$.

Код БЧХ есть циклический (n, k)-код, в котором делящий $x^n - 1$ порождающий многочлен $g(x)$ является полиномом минимальной степени, имеющим корнями *нули кода* α, α^2, α^3, …, $\alpha^{d_c - 1}$, где α — примитивный элемент поля $\mathbb{F}_2^q$, $m = \deg g(x)$ и $k = n - m$.

Важнейшее свойство построенного БЧХ-кода: его кодовое расстояние d оказывается не менее выбранного конструктивного расстояния d_c.

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 3.9. *Синдромами полинома* $w(x)$, принятого при передаче сообщения, закодированного БЧХ-кодом с нулями α^i, $i = 1, \ldots, d - 1$ и, возможно, содержащего ошибки, назовём значения $w(x)$ 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;

- поскольку

$$w(x) = v(x) + e(x), \quad \text{то} \quad s_i = w(\alpha^i) = e(\alpha^i);$$

- *«все синдромы равны нулю»* $\Leftrightarrow$ $w(x)$ — кодовое слово.

- если $s_i \neq 0$, то $s_i = \alpha^{\text{какая-то степень}}$.

3.7 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) определить поле $\mathbb{F}_2^q = \mathbb{F}_2[x]/(a(x))$, выбрав неприводимый полином $a(x) \in \mathbb{F}_2[x]$ степени q и примитивный элемент α поля;
4) определить циклотомические классы элемента $\alpha \in \mathbb{F}_2^q$ над полем $\mathbb{F}_2$, в которые попадают нули кода $\alpha, \alpha^2, \ldots, \alpha^{d_c-1}$; пусть таких классов h;
5) найти минимальные многочлены $g_1(x), \ldots, g_h(x)$ каждого циклотомического класса;
6) вычислить порождающий полином
$$g(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_h(x).$$

Пример 3.10 (построения кодов БЧХ). Выберем $q = 3$ и построим различные БЧХ-коды длины $n = 2^3 - 1 = 7$.

Для получения разложения бинома $x^7 - 1$ рассмотрим поле $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^3$, $\deg a(x) = q = 3$. Тогда F^*, как показано ранее, разбивается на следующие циклотомические классы над $\mathbb{F}_2$:
$$\{1\},\ \{\alpha, \alpha^2, \alpha^4\},\ \{\alpha^3, \alpha^6, \alpha^5\}.$$

Конкретно в качестве порождающего многочлена возьмём примитивный многочлен $a(x) = x^3 + x + 1$, который является м.м. для примитивного элемента $\alpha = x$ и всего класса $\left\{ \alpha,\, \alpha^2,\, \alpha^4 \right\}$.

Для построения кодов, исправляющих разное 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 $\alpha,\, \alpha^2$ 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 $\alpha,\, \alpha^2,\, \alpha^3,\, \alpha^4$ входят в *два* циклотомических класса: $\left\{ \alpha,\, \alpha^2,\, \alpha^4 \right\}$ и $\left\{ \alpha^3,\, \alpha^6,\, \alpha^5 \right\}$, 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 $\alpha^3 = \alpha + 1$:

$$\begin{aligned} g_{\alpha^3}(x) &= \left(x - \alpha^3\right)\left(x - \alpha^5\right)\left(x - \alpha^6\right) = \\ &= x^3 + \left(\alpha^3 + \alpha^5 + \alpha^6\right)\, x^2 + \left(\alpha^8 + \alpha^9 + \alpha^{11}\right)\, x + \alpha^{14}. \end{aligned}$$

Вычислим коэффициенты полинома $g_{\alpha^3}(x)$ с учётом $\alpha^7 = 1$ и $\alpha^3 = \alpha + 1$:

$$\begin{aligned}
\alpha^3+\alpha^5+\alpha^6 &= (\alpha+1)+\alpha^2(\alpha+1)+(\alpha+1)^2 = \\
&= \alpha+1+\alpha^3+\alpha^2+\alpha^2+1 = 1\,, \\
\alpha^8+\alpha^9+\alpha^{11} &= \alpha^2+\alpha+\alpha^4 = \alpha^2+\alpha+\alpha(\alpha+1) = 0\,, \\
\alpha^{14} &= 1\,.
\end{aligned}$$

Т.о. $g_{\alpha^3}(x) = x^3+x^2+1$ (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 $\deg g(x) = 6$ и $k = 1$, 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.

Попытаемся построить лучший код для исправления 2-х ошибок, взяв бóльшую его длину.

Пример 3.11. 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 $\mathbb{F}_2$:

$$\{1\}\,,\ \{\alpha,\,\alpha^2,\,\alpha^4,\,\alpha^8\}\,,\ \{\alpha^3,\,\alpha^6,\,\alpha^{12},\,\alpha^9\}\,,$$
$$\{\alpha^5,\,\alpha^{10}\}\,,\ \{\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}\}\,.$$

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 $\alpha, \alpha^2, \alpha^3, \alpha^4$ 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 $\alpha, \alpha^2, \ldots, \alpha^6$, 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.

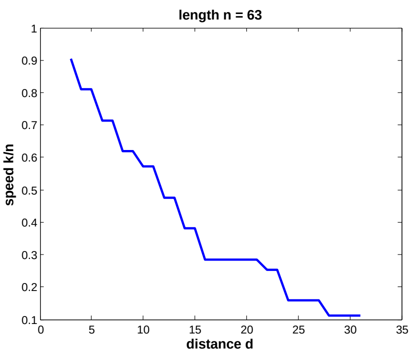
Очевидно $g_{\alpha^5}(x) = x^2+x+1$ (единственный неприводимый квадратный полином над $\mathbb{F}_2$) и порождающий полином полученного кода есть

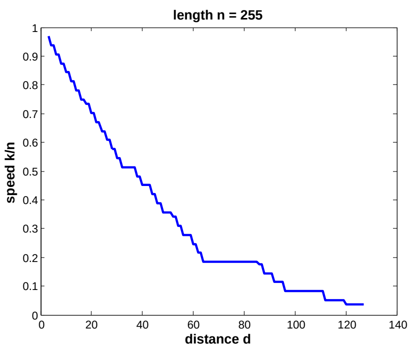
$$g(x) = g_\alpha(x)\cdot g_{\alpha^3}(x)\cdot g_{\alpha^5}(x) = \\ = x^{10}+x^8+x^5+x^4+x^2+x+1.$$

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 $R = 1/3$.

Зависимости скорости БЧХ-кодов от кодового расстояния





«Ступеньки» на графиках соответствуют ситуации, когда реальное кодовое расстояние оказалось больше, чем выбранное конструктивное.

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 3.4. 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 $s_1(x) = w(\alpha) = s(x)$ (синдром $s_2 = w(\alpha^2)$ нам не потребуется).

- При $s(x) \equiv 0$ считаем, что ошибок не произошло.
- Если $s(x) \not\equiv 0$, то определяем значение j, для которого $\alpha^j = s(x)$ и считаем, что произошла единичная ошибка в j-м разряде для $j = 0, 1, \ldots, n-1$.

Пример 3.12 (декодирование кода Хэмминга). Рассматриваем $(7,4)$-код Хэмминга, построенный в *Примере* 3.8 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 $\alpha^7 = 1$):

$$s(x) = w(\alpha) = \alpha^6 + \alpha = \left(\alpha^3\right)^2 + \alpha = (\alpha+1)^2 + \alpha = \\ = \alpha^2 + \alpha + 1 \neq 0\,.$$

Определим теперь значение $j \in \{0, \ldots, 6\}$, для которого $\alpha^j = s(x)$:

$$\begin{aligned} &\alpha^0 = 1, && \alpha^3 = \alpha + 1, \\ &\alpha^1 = \alpha, && \alpha^4 = \alpha(\alpha+1) = \alpha^2 + \alpha, \\ &\alpha^2 = \alpha^2, && \alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 = s. \end{aligned}$$

Т.о. 5-я позиция ошибки определена верно[11].

Если же произошло *две ошибки*, например, в 5 и 4-й позициях, то

$$w(x) = x^6 + x^4 + x, \quad s = 1,\ j = 0,$$
$$\widehat{v}(x) = x^6 + x^4 + x + 1 \leftrightarrow [1\ 1\ 0\ \underbrace{0\ 1\ 0\ 1}]^T$$

и будет раскодировано сообщение $[0\ 1\ 0\ 1]^T$ вместо посланного $[0\ 0\ 1\ 1]^T$.

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 $F = \mathbb{F}_2^q = \mathbb{F}[x]/(a(x))$, $\deg a(x) = q$ и α — нуль кода.

[11] Альтернативный метод декодирования кода Хэмминга см. на с. 187.

Пусть при передаче кодового слова произошло ν ошибок в позициях $j_1, \ldots, j_\nu$. Тогда

$$e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}, \quad \nu \leqslant r = \lfloor (d-1)/2 \rfloor.$$

Вычислим синдромы принятого полинома $w(x)$: $s_i = w(\alpha^i) = e(\alpha^i)$, $i = 1, \ldots, 2r$ и запишем систему

$$\begin{cases} s_1 = \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_\nu}, \\ s_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_\nu})^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = (\alpha^{j_1})^{2r} + \ldots + (\alpha^{j_\nu})^{2r}. \end{cases}$$

Решение $(j_1, \ldots, j_\nu)$ данной системы для некоторого $\nu \leqslant r$ определит искомые позиции ошибок[12].

Введём обозначения $\beta_i = \alpha^{j_i}$, $i = 1, \ldots, \nu$; эти величины называют *локаторами ошибок.*

Перепишем систему:

$$\begin{cases} s_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ s_2 = \beta_1^2 + \beta_2^2 + \ldots + \beta_\nu^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = \beta_1^{2r} + \beta_2^{2r} + \ldots + \beta_\nu^{2r}. \end{cases}$$

Определим *полином локаторов ошибок*

$$\sigma(x) = \prod_{i=1}^{\nu} (1 + \beta_i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_\nu x^\nu,$$

корнями которого являются величины $\beta_i^{-1} = \alpha^{-j_i}$, $i = 1, \ldots, \nu$.

[12] Такое решение всегда существует и единственно, т. к. код по построению способен исправлять до r ошибок.

Связь между σ_k и β_i 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

$$\begin{aligned} & s_1 + \sigma_1 = 0, \\ & s_2 + \sigma_1 s_1 + 2\sigma_2 = 0, \\ & s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 = 0, \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & s_\nu + \sigma_1 s_{\nu-1} + \ldots + \sigma_{\nu-1} s_1 + \nu\sigma_\nu = 0, \end{aligned}$$

$$\left.\begin{aligned} & s_{\nu+1} + \sigma_1 s_\nu + \ldots + \sigma_{\nu-1} s_2 + \sigma_\nu s_1 = 0, \\ & s_{\nu+2} + \sigma_1 s_{\nu+1} + \ldots + \sigma_{\nu-1} s_3 + \sigma_\nu s_2 = 0, \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & s_{2r} + \sigma_1 s_{2r-1} + \ldots + \sigma_{\nu-1} s_{2r-\nu+1} + \sigma_\nu s_{2r-\nu} = 0. \end{aligned}\right\} \quad (*)$$

Последние $2r-\nu$ равенств данной системы являются СЛАУ относительно $\sigma_1, \ldots, \sigma_\nu$. Известны несколько алгоритмов её решения, которые называют *декодерами.* Основная трудность здесь состоит в том, что *значение* ν *неизвестно.*

После нахождения $\sigma(x)$ можно, например, полным перебором[13], отыскать все его корни 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 α — нуль кода, примитивный элемент поля $\mathbb{F}_2^q = \mathbb{F}_2[x]/\left(a(x)\right)$, $\deg a(x) = q$.
Пусть принято слово $w(x)$.

1. Для слова $w(x)$ найти все синдромы $s_i = w(\alpha^i)$, $i = 1, \ldots, d-1$.
2. Найти полином локаторов ошибок $\sigma(x)$, используя тот или иной декодер.
3. Найти все корни $\sigma(x)$ полным перебором всех ненулевых элементов поля. $\mathbb{F}_2^q$; пусть найденные корни суть $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$.
4. Найти *позиции ошибок*
$$j_i \equiv_n -k_i,\ i = 1, \ldots, \nu.$$
5. Исправить ошибки, получив слово
$$\widehat{v}(x) = w(x) + x^{j_1} + \ldots + x^{j_\nu}.$$
6. Найти все значения $\widehat{v}(\alpha^i)$, $i = 1, \ldots, \nu$ и если не все они равны нулю, то выдать *отказ от декодирования.*

[13] т.н. *процедура Ченя*

Опишем *декодер на основе расширенного алгоритма Евклида*, который будем далее использовать.

Введём вспомогательный *синдромный полином*

$$s(x) = 1 + s_1x + s_2x^2 + \ldots + s_{2r}x^{2r},$$

где $s_i = w(\alpha^i)$, $i = 1, \ldots, 2r$ — синдромы и формально $s_0 = 1$.

Если перемножить полиномы — синдромный и локаторов ошибок, получим *полином значений ошибок*:

$$s(x)\sigma(x) = 1 + \lambda_1x + \lambda_2x^2 + \ldots + \lambda_{2r+\nu}x^{2r+\nu}.$$

Коэффициенты этого полинома определяются соотношением для произведения многочленов —

$$\lambda_i = \sum_{j=0}^{i} s_j\sigma_{i-j}, \quad i = 1, \ldots, 2r + \nu.$$

Замечаем, что значения λ_i по данной формуле для $i = \nu + 1, \ldots, 2r$ суть левые части СЛАУ $(*)$, 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}:

$$s(x)\sigma(x) = \underbrace{\left(1 + \lambda_1x + \lambda_2x^2 + \ldots + \lambda_\nu x^\nu\right)}_{=\lambda(x)} +$$
$$+ x^{2r+1}\left(\lambda_{2r+1} + \ldots + \lambda_{2r+\nu}x^{\nu-1}\right), \quad \nu \geqslant 1.$$

Это означает, что

$$s(x)\sigma(x) \equiv_{x^{2r+1}} \lambda(x).$$

Данное соотношение получило название *ключевого уравнения*.

Очевидно, ключевое уравнение может быть записано в виде соотношения Безу

$$s(x)\sigma(x) + x^{2r+1}a(x) \;=\; \lambda(x)$$

(напоминание: работаем в поле $\mathbb{F}_2^q \cong \mathbb{F}_2[x]/(a(x))$), которое может быть решено относительно $\sigma(x)$ расширенным алгоритмом Евклида. При этом:

- условие остановки — степень очередного полученного остатка $\leqslant r$;
- количество совершенных ошибок $\nu = \deg\sigma(x)$;
- при решении не требуется знать сам многочлен $\lambda(x)$.

Пример 3.13 (декодирования БЧХ-кода). Рассмотрим БЧХ $(15, 5, 7)$-код $15 = 2^q - 1$, $q = 4$ исправляющий до $r = 3$ ошибок. Пусть при построении кода в качестве поля разложения бинома $x^{15} - 1$ использовалось поле $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$ 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 $\mathbb{F}_2[x]/\big(x^4+x+1\big)$ как степеней его генератора α (дублируем таблицу со с. 75):

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:

$$\begin{aligned}
s_1 \;&=\; w(\alpha) \;= \\
&=\; (\alpha^3+1)+(\alpha^3+\alpha^2+\alpha)+(\alpha^2+1)+(\alpha^3+\alpha^2)+ \\
&+\,(\alpha+1)+\alpha^3+\alpha^2+\alpha+1 \;=\; \alpha, \\
s_2 \;&=\; w(\alpha^2) \;=\; (w(\alpha))^2 \;=\; \alpha^2, \\
s_3 \;&=\; w(\alpha^3) \;=\; \underbrace{\alpha^{42}}_{=\alpha^{12}}+\underbrace{\alpha^{33}}_{=\alpha^{3}}+\underbrace{\alpha^{24}}_{=\alpha^{9}}+\underbrace{\alpha^{18}}_{=\alpha^{3}}+\alpha^{12}+\alpha^9+
\end{aligned}$$

$$
\begin{aligned}
&+\alpha^6+\alpha^3+1 = \alpha^3+\alpha^6+1 = \cancel{\alpha^3}+\alpha^2+\cancel{\alpha^3}+1 = \\
&= \alpha^2+1 = \alpha^8, \\
s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^4, \\
s_5 &= w(\alpha^5) = \alpha^{70}+\alpha^{55}+\alpha^{40}+\alpha^{30}+\alpha^{20}+\alpha^{15}+ \\
&+\alpha^{10}+\alpha^5+1 = \\
&= \alpha^{10}+\alpha^{10}+\alpha^{10}+1+\alpha^5+1+\alpha^{10}+\alpha^5+1 = 1, \\
s_6 &= w(\alpha^6) = (w(\alpha^3))^2 = (\alpha^2+1)^2 = \alpha^4+1 = \alpha.
\end{aligned}
$$

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*

$$
\begin{aligned}
r_{-2}(x) &= x^7,\\
r_{-1}(x) &= s(x) = \alpha x^6 + x^5 + \alpha^4 x^4 + \\
&\quad + \alpha^8 x^3 + \alpha^2 x^2 + \alpha x + 1,\\
\sigma_{-2}(x) &= 0,\\
\sigma_{-1}(x) &= 1.
\end{aligned}
$$

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

$$
\begin{aligned}
r_{-2}(x) &= r_{-1}(x) q_0(x) + r_0(x),\\
q_0(x) &= \alpha^{14} x + \alpha^{13},\\
r_0(x) &= \alpha^8 x^5 + \alpha^{12} x^4 + \alpha^{11} x^3 + \alpha^{13},\\
&\quad \deg r_0(x) = 5 > 3,\\
\sigma_0(x) &= \sigma_{-2}(x) + \sigma_{-1}(x) q_0(x) = \\
&= q_0(x) = \alpha^{14} x + \alpha^{13}.
\end{aligned}
$$

Шаг 2. // *Делим с остатком* $r_{-1}(x)$ *на* $r_0(x)$

$$
\begin{aligned}
r_{-1}(x) &= r_0(x) q_1(x) + r_1(x),\\
q_1(x) &= \alpha^8 x + \alpha^2,\\
r_1(x) &= \alpha^{14} x^4 + \alpha^3 x^3 + \alpha^2 x^2 + \alpha^{11} x,\\
&\quad \deg r_1(x) = 4 > 3,\\
\sigma_1(x) &= \sigma_{-1}(x) + \sigma_0(x) q_1(x) = \\
&= \alpha^7 x^2 + \alpha^{11} x.
\end{aligned}
$$

Шаг 3. // *Делим с остатком* $r_0(x)$ *на* $r_1(x)$

$$
\begin{aligned}
r_0(x) &= r_1(x) q_2(x) + r_2(x),\\
q_2(x) &= \alpha^9 x,\\
r_2(x) &= \alpha^5 x + \alpha^{13},\\
&\quad \deg r_2(x) = 1 \leqslant 3,\\
\sigma_2(x) &= \sigma_0(x) + \sigma_1(x) q_2(x) = \\
&= \alpha x^3 + \alpha^5 x^2 + \alpha^{14} x + \alpha^{13} = \sigma(x).
\end{aligned}
$$

Это последний шаг алгоритма Евклида, т. к. степень остатка $r_2(x)$ не превосходит $r = 3$.

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 $\sigma(x)$ полным перебором[14], используя построенную ранее таблицу степеней α:

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 + \alpha^{13} = \alpha^2,\\
\sigma(\alpha^2) &= \alpha^7 + \alpha^9 + \alpha + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha,\\
\sigma(\alpha^3) &= \alpha^{10} + \alpha^{11} + \alpha^2 + \alpha^{13} = \mathbf{0},\\
\sigma(\alpha^4) &= \alpha^{13} + \alpha^{13} + \alpha^3 + \alpha^{13} = \alpha^2 + 1,\\
\sigma(\alpha^5) &= \alpha + 1 + \alpha^4 + \alpha^{13} = \alpha^{13},\\
\sigma(\alpha^6) &= \alpha^4 + \alpha^2 + \alpha^5 + \alpha^{13} = \alpha^3 + \alpha^2,\\
\sigma(\alpha^7) &= \alpha^7 + \alpha^4 + \alpha^6 + \alpha^{13} = \alpha^3 + 1,\\
\sigma(\alpha^8) &= \alpha^{10} + \alpha^6 + \alpha^7 + \alpha^{13} = \alpha^3 + \alpha^2 + 1,\\
\sigma(\alpha^9) &= \alpha^{13} + \alpha^8 + \alpha^8 + \alpha^{13} = \mathbf{0},\\
\sigma(\alpha^{10}) &= \alpha + \alpha^{10} + \alpha^9 + \alpha^{13} = \alpha,\\
\sigma(\alpha^{11}) &= \alpha^4 + \alpha^{12} + \alpha^{10} + \alpha^{13} = \alpha^2 + \alpha,\\
\sigma(\alpha^{12}) &= \alpha^7 + \alpha^{14} + \alpha^{11} + \alpha^{13} = 1,\\
\sigma(\alpha^{13}) &= \alpha^{10} + \alpha + \alpha^{12} + \alpha^{13} = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{14}) &= \alpha^{13} + \alpha^3 + \alpha^{13} + \alpha^{13} = \alpha^2 + 1,\\
\sigma(\alpha^{15}) &= \alpha + \alpha^5 + \alpha^{14} + \alpha^{13} = \mathbf{0}.
\end{aligned}$$

[14] ясно, что корней всего 3

4. По найденным корням α^3, α^9, α^{15} вычисляем позиции ошибок:

$$\begin{aligned} j_1 &= -3 \equiv_{15} 12, \\ j_2 &= -9 \equiv_{15} 6, \\ j_3 &= -15 \equiv_{15} 0. \end{aligned}$$

5. Т.о. полином ошибок $e(x) = x^{12} + x^6 + 1$ определён и кодовое слово —

$$\widehat{v}(x) = w(x) + e(x).$$

6. Проверка $\widehat{v}(\alpha) = \widehat{v}(\alpha^2) = \ldots = \widehat{v}(\alpha^6) = 0$ говорит от том, что восстановление верное[15]: $\widehat{v}(\alpha) = v(x)$.

БЧХ-коды: исторические сведения. Первым практически реализованным БЧХ-кодом был $(127, 92, 11)$-код, исправляющий 5 ошибок.

В системах передачи данных широко используется двоичный БЧХ $(255, 231, 7)$-код $(q = 8)$ со свойствами:

- степень порождающего код многочлена $g(x)$ — $m = n - k = 24$;
- 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.

[15] с учётом замечания на с. 141

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 (Форни, Берлекэмпа-Мэсси, Питерсона-Горенстейна-Цирлера, Евклидов алгоритм, ...).
- При небольших n среди кодов БЧХ существуют хорошие (но, как правило, не лучшие из известных) коды.
- 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.

Коды Рида–Соломона: общие сведения. Широко используемым частным случаем кодов БЧХ являются *коды Рида-Соломона* (Reed–Solomon codes), которые позволяют исправлять пакеты ошибок.

Пакет ошибок (error burst) — группа битов, в которой два последовательных ошибочных бита всегда разделены правильными битами, число которых менее установленного.

Коды Рида–Соломона:

- небинарные (в частности, очень распространены коды, работающие с *байтами*);
- часто используются в устройствах *цифровой записи звука*, в том числе на компакт-диски.

Пример 3.14 (негруппового блокового кода). Пусть по двоичному симметричному каналу с шумом требуется передавать $t = 4$ битовых сообщения S_1, S_2, S_3, S_4 длины 2.

Блоковый разделимый негрупповой код C, исправляющий 1 ошибку задаётся таблицей

S	C
0 0	0 0 1 1 0
0 1	0 1 1 0 1
1 0	1 0 0 1 1
1 1	1 1 0 0 0

«Зазор»: $2^5 - 4 \cdot (1 + 5) = 8$ слов; граница Плоткина достигается (проверьте)

Кодовое расстояние построенного кода C равно 3 и построен систематический $(5, 2, 3)$-код, содержащий исходное сообщение в первых двух позициях.

Помехоустойчивое кодирование применяется:

- для получения *надежной связи*, когда мощность принимаемого сигнала близка к мощности тепловых шумов[16];
- для *защиты против шума, намеренно организованного противником* в военных приложениях;
- при передаче данных *в вычислительных системах*[17];
- для защиты данных во внутренних и внешних ЗУ (ленты, диски...);
- 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

[16] Например, циклические коды используются в мобильной связи в стандартах GSM и CDMA.

[17] Эти системы 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.

исчезает при повторном вычислении выходного вектора.

В этих случаях применяются коды специально предназначенные для *обнаружения ошибок*, 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).

3.8 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 $(7,4,3)$-код Хэмминга, помещающий информационные биты в последние 4, а проверочные — в первые 3 позиции кода.

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:

$$v(x) \;=\; g(x)(ax^2{+}bx{+}c) \;=\; (x^6{+}x^3{+}1)(ax^2{+}bx{+}c) \;=$$
$$=\; ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c,$$
$$a, b, c \in \mathbb{F}_2.$$

В векторном виде все кодовые слова представляются как

$$[\, c,\; b,\; a,\; c,\; b,\; a,\; c,\; b,\; a\,]. \tag{$*$}$$

Очевидно, что минимальный хэммингов вес ненулевого кодового слова равен 3 и, следовательно, $d = 3$.

Проводим систематическое кодирование сообщения $u(x)$:

$$u(x) \;\mapsto\; v(x) \;=\; x^6u(x) + r(x),$$
$$x^6u(x) \;=\; x^6(x^2 + x) \;=\; x^8 + x^7.$$

Находим остаток $\deg r(x)$ от деления $x^6u(x)$ на $g(x)$:

$$\begin{array}{llllll|l}
x^8 & +\,x^7 & & & & & x^6 + x^3 + 1 \\ \cline{7-7}
x^8 & & +\,x^5 & & +x^2 & & x^2 + x \\ \cline{1-5}
 & x^7 & +\,x^5 & & +\,x^2 & & \\
 & x^7 & & +\,x^4 & & +\,x & \\ \cline{2-6}
 & & x^5 & +\,x^4 & +\,x^2 & +\,x &
\end{array}$$

Т.о. $r(x) = x^5 + x^4 + x^2 + x$ и

$$v(x) \;=\; x^8{+}x^7{+}x^5{+}x^4{+}x^2{+}x \;\leftrightarrow\; [0\ 1\ 1\ 0\ 1\ 1\ \underline{0\ 1\ 1}]^T.$$

Замечание. Очевидно задан тривиальный код утроения: кодовое слово есть трижды повторенное сообщение. Поэтому кодирование будет только систематическим и вид $v(x)$ сразу определён в $(*)$.

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. Очевидно, имеем $(7, 4, 3)$-код Хэмминга, в котором сообщение есть коэффициенты перед степенями 3, …, 6 формальной переменной x кодового полинома.

Для декодирования необходимо вычислить синдром $s = w(\alpha)$ с учётом $\alpha^3 = \alpha + 1$, где α — генератор поля $\mathbb{F}_2[x]/(a(x))$.

Если $s \equiv 0$, то считаем, что ошибок при передаче не произошло; иначе необходимо найти такое k, что $\alpha^k = s$ и перед восстановлением сообщения инвертировать k-й разряд $w(\alpha)$ (что, очевидно, имеет смысл при $k \in \{3, \ldots, 6\}$).

1. $\underline{w_1(x) = x^6 + x^2 + x} \leftrightarrow [0\ 1\ 1\ \underline{0\ 0\ 0\ 1}]$

$$s = w(\alpha) = \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha =$$
$$= (\alpha + 1)^2 + \alpha^2 + \alpha = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1 \neq 0.$$

Очевидно, $\alpha + 1 = \alpha^3$, т.е. $k = 3$, ошибка произошла в 3-м разряде и $\widehat{v}(x) = w(x) + e(x) = x^6 + x^3 + x^2 + x \leftrightarrow [0\ 1\ 1\ 1\ 0\ 0\ 1]$, $u(x) \leftrightarrow [1\ 0\ 0\ 1]$.

2. $\underline{w_2(x) = x^6 + x^5 + x^3 + x^2 + x} \leftrightarrow [0\ 1\ 1\ \underline{1\ 0\ 1\ 1}]$

$$s = w(\alpha) = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha =$$

$$= (\alpha+1)^2 + (\alpha+1)\alpha^2 + \alpha + 1 + \alpha^2 + \alpha =$$
$$= \alpha^2+1+\alpha^3+\alpha^2+\alpha^2+1 = \alpha^3+\alpha^2 = \alpha^2+\alpha+1 \neq 0.$$

Очевидно, $\alpha^3+\alpha^2 = (\alpha+1)\alpha^2 = \alpha^5$, т.е. $k = 5$, ошибка произошла в 5-м разряде и снова $u(x) \leftrightarrow [1\ 0\ 0\ 1]$.

3. $\underline{w_3(x) = x^6 + x^3 + x^2 + x} \leftrightarrow [0\ 1\ 1\ \underbrace{1\ 0\ 0\ 1}]$.

Убеждаемся, что в этом случае $s \equiv 0$, т.е. ошибок не произошло и $u(x) = v(x) \leftrightarrow [1\ 0\ 0\ 1]$.

Замечание. Декодирование систематического кода Хэмминга можно провести делением принятого полинома на порождающий: остаток от деления есть синдром s:

$$w(x) = q(x)\cdot g(x) + r(x), \qquad s = r(\alpha).$$

В нашем случае:

1. $x^6 + x^2 + x = (x^3+x+1)^2 + \underbrace{x+1}$;
2. $x^6 + x^5 + x^3 + x^2 + x =$
   $= (x^3+x^2+x+1)(x^3+x+1) + \underbrace{x^2+x+1}$;
3. $x^6 + x^3 + x^2 + x = (x^3+x)(x^3+x+1) + \underbrace{0}$.

<u>Задача</u> 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, уже ранее использованную нами (см. с. 75, 174).

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	α^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}	α^3+1	(1001)
α^{15}	1	(0001)

С помощью этой таблицы вычислим синдромы:

$$
\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14}+\alpha^{10}+\alpha^5+\alpha^4 = \\
&\qquad = (\alpha^3+1)+(\alpha^2+\alpha+1)+(\alpha^2+\alpha)+(\alpha+1) = \\
&\qquad = \alpha^3+\alpha+1 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12}+1+1+\alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = \big(w(\alpha^2)\big)^2 = \alpha^{28} = \alpha^{13}.
\end{aligned}
$$

Синдромный полином —

$$
s(x) = \alpha^{13}x^4+\alpha^{14}x^2+\alpha^7x+1.
$$

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:

Шаг 0. $r_{-2}(x) = x^5,$ // *Инициализация*
$r_{-1}(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1,$
$\sigma_{-2}(x) = 0,$
$\sigma_{-1}(x) = 1.$

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 $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$, где α — примитивный элемент поля $F = \mathbb{F}_2^5$.

При разбиении F^* на циклотомические классы всегда будет присутствовать пятиэлементный класс $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$.

Остальные рассматриваемые степени α будут входить в циклотомические классы

$$\{\alpha^3, \alpha^6, \dots\} \text{ и } \{\alpha^5, \dots\}.$$

Нетрудно установить, что эти классы также будут пятиэлементными:

$$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48} = \alpha^{17}\}, \quad (\text{т.к. } 34 \equiv_{31} 3);$$
$$\{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40} = \alpha^9, \alpha^{18}\}, \quad (\text{т.к. } 36 \equiv_{31} 5).$$

Ранее[18] были приведены неприводимые многочлены 5-й степени над $\mathbb{F}_2$: их шесть —

1) $x^5 + x^2 + 1$, 4) $x^5 + x^4 + x^2 + x + 1$,
2) $x^5 + x^3 + 1$, 5) $x^5 + x^4 + x^3 + x + 1$,
3) $x^5 + x^3 + x^2 + x + 1$, 6) $x^5 + x^4 + x^3 + x^2 + 1$.

Во многих монографиях[19] есть соответствующие таблицы. Все эти многочлены, как указано в таблицах, явля-

[18] см. с. 37

[19] Например, *Лидл Р., Нидеррайтер Г.* Конечные поля, Том 1, Таблица C.

ются примитивными (корень $\alpha = x$ — генератор мультипликативной группы соответствующего поля) и 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 —

$$(x^5+x^3+x^2+x+1)\Big|_{x=\alpha^3} = \alpha^{15}+\alpha^9+\alpha^6+\alpha^3+1 = \\ = (\alpha^3+1)^3+\alpha^4(\alpha^3+1)+\alpha(\alpha^3+1)+\alpha^3+1 = \ldots = 0,$$

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[20] 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	$\alpha^2 + 1$
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}	$\alpha^3 + 1$
α^{15}	1

Перебором найдём корни полинома ошибок

$$\sigma(x) = \alpha^6 x + \alpha^{15} = (\alpha^3 + \alpha^2)\, x + 1 :$$

$$\sigma(\alpha) = \alpha^4 + \alpha^3 + 1 = \alpha + 1 + \alpha^3 \neq 0;$$

$$\sigma(\alpha^2) = \alpha^5 + \alpha^4 + 1 = \alpha^2 + \alpha + \alpha + 1 + 1 = \alpha^2 \neq 0;$$

[20] см. с. 74 и 187

$$\begin{aligned} &\ldots\ldots \\ \sigma(\alpha^9) \ &= \ \alpha^{12} + \alpha^{11} + 1 \ = \\ &= \ (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) + 1 \ = \ \mathbf{0}. \end{aligned}$$

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 $\mathcal{G} = \langle\, G, \circ, e\,\rangle,\ |G| = n.$
- Множество $T,\ |T| = N > 0.$
  - $Bij(T)$ — множество всех биекций (перестановок) элементов T.
  - $Sym(T)$ — симметрическая группа множества T: $\quad Sym(T) = \langle\, Bij(T), *, 1_T\,\rangle.$

<u>Определение</u> 4.1 (I). $\quad \alpha \in \mathrm{Hom}\,(\,\mathcal{G},\, Sym(T)\,).$

Действие α группы $\mathcal{G}$ на множестве T: символически — $\mathcal{G} \underset{\alpha}{:} T$.

<u>Определение</u> 4.2 (II). $\quad \alpha = \langle\, \mathcal{G}, T, \circ, \star, e, 1_T\,\rangle$, где

$G \times G \xrightarrow{\circ} G$ — групповая операция;

$G \times T \xrightarrow{\star} T$ — новая операция.

Аксиомы для операций:

$$1)\ e \star t = t; \qquad 2)\ (g \circ h) \star t = h \star (g \star t).$$

Запись операции $\star$: $g(t) = t'$.
Тогда аксиомы: $e(t) = t$ и $(g \circ h)(t) = h(g(t))$.

Элементы g группы G порождают перестановки на T, обладающие указанными свойствами.

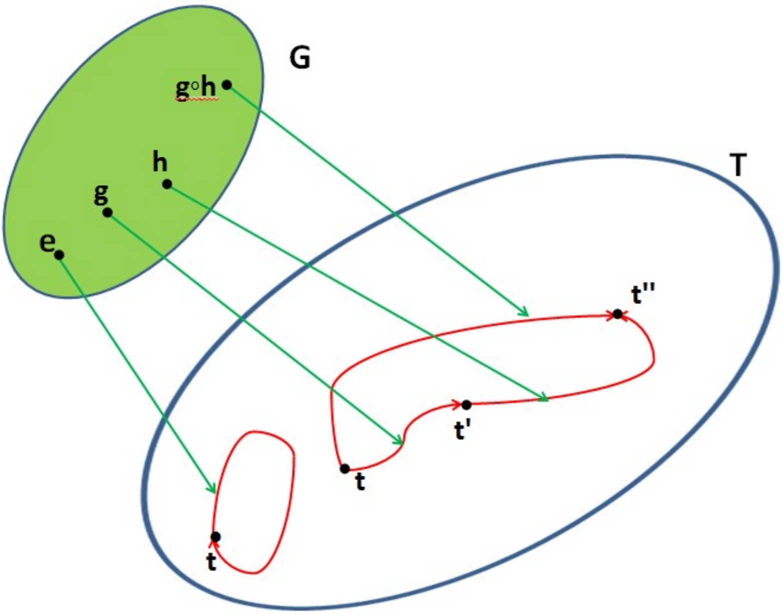


Рис. 4.1. К определению действия группы на множестве

<u>*Для данной перестановки g:*</u>

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

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 10 & 3 & 4 \end{pmatrix} =$$
$$= (1,9,3)(2,6)(4,8,10)(5)(7) = (1,9,3)(2,6)(4,8,10).$$

Тогда $Type(g) = \langle\, 2, 1, 2, 0, \ldots, 0 \,\rangle$ и

$C(g) = 2+1+2 = 5, \quad \big|\, T \,\big| = 2\cdot 1 + 1\cdot 2 + 2\cdot 3 = 10.$

По всей группе $\mathcal{G}$:

Отношение эквивалентности $\sim_{\mathcal{G}}$ на T —

$$t \sim_{\mathcal{G}} t' \stackrel{\text{def}}{=} \exists\, g \in G : g(t) = t'.$$

Свойства (R), (S) и (T) отношения $\sim_{\mathcal{G}}$ 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 — $C(\mathcal{G})$.

Если $C(\mathcal{G}) = 1$ (любой элемент T может быть переведён в любой), то действие $\mathcal{G} \underset{\alpha}{:} T$ называют *транзитивным*.

Фиксатор перестановки и стабилизатор элемента множества. Рассмотрим равенство

$$g(t) = t.$$

При его выполнении можно полагать постоянным либо t, либо g.

1. Фиксируем g, т.е. находим все элементы множества T, которые данная перестановка оставляет на месте — это *фиксатор перестановки* $g \in \mathcal{G}$:

$$\{\, t \in T \mid g(t) = t \,\} = \mathrm{Fix}\,(g) \subseteq T.$$

2. Фиксируем t, т.е. находим все перестановки g, которые оставляют данный элемент неподвижным — это *стабилизатор элемента* $t \in T$:

$$\{\, g \in G \mid g(t) = t \,\} = \mathrm{Stab}\,(t) \subseteq G.$$

Очевидно $\forall\, t \in T: \ e \in \mathrm{Stab}\,(t)$, т.е. $\mathrm{Stab}\,(t) \neq \varnothing$. Более того, стабилизатор есть подгруппа группы $\mathcal{G}$:

Утверждение 4.1. $\mathrm{Stab}\,(t) \leqslant \mathcal{G}$.

Доказательство. Для $t \in T$ рассмотрим $g, h \in \mathrm{Stab}\,(t)$. Тогда $g(t) = h(t) = t$ и $h^{-1}(t) = t$. Следовательно

$$(g \circ h^{-1}) \star t = t \Rightarrow g \circ h^{-1} \in \mathrm{Stab}\,(t)\,.$$

□

Поэтому стабилизатор $\mathrm{Stab}\,(t)$ называют ещё *стационарной подгруппой*[1] *элемента* t.

$\mathrm{Stab}\,(t)$ будем также обозначать G_t.

[1] или *изотопической подгруппой*

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

Следствие. *Длина орбиты $\mathrm{Orb}\,(t)$ равна индексу стационарной подгруппы $\mathrm{Stab}\,(t)$ в группе $\mathcal{G}$:*

$$\big|\,\mathrm{Orb}\,(t)\big| = \frac{\big|G\big|}{\big|\,\mathrm{Stab}\,(t)\big|} = [G : \mathrm{Stab}\,(t)]\,.$$

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 $\mathcal{G}$ действует на множестве T, то*

$$C(\mathcal{G}) = \frac{1}{|G|}\sum_{g\in G}\Big|\,\mathrm{Fix}\,(g)\Big| = \frac{1}{|G|}\sum_{t\in T}\Big|\,\mathrm{Stab}\,(t)\Big|;$$

при этом первое равенство называется леммой Бёрнсайда.

Доказательство. Пусть $|G| = n$, $|T| = N$ и действие $\mathcal{G} \underset{\alpha}{:} T$ 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

$$\sum_{g\in G}\Big|\,\mathrm{Fix}\,(g)\Big| = \big|M\big| = \sum_{t\in T}\Big|\,\mathrm{Stab}\,(t)\Big|.$$

Если x и y принадлежат одному классу эквивалентности по $\sim_{\mathcal{G}}$, то $\mathrm{Orb}\,(x) = \mathrm{Orb}\,(y)$ и их стационарные подгруппы имеют одинаковую мощность:

$$\big|\,\mathrm{Stab}\,(x)\,\big| = \frac{|G|}{|\,\mathrm{Orb}\,(x)\,|} = \frac{|G|}{|\,\mathrm{Orb}\,(y)\,|} = \big|\,\mathrm{Stab}\,(y)\,\big|.$$

Выберем по представителю $t_1, \ldots, t_{C(\mathcal{G})}$ из всех $C(\mathcal{G})$ орбит. Тогда

$$\big|M\big| = \sum_{t\in T}\Big|\,\mathrm{Stab}\,(t)\Big| = \sum_{i=1}^{C(\mathcal{G})}\big|\,\mathrm{Stab}\,(t_i)\big|\cdot\big|\,\mathrm{Orb}\,(t_i)\big| =$$

$$= \sum_{i=1}^{C(\mathcal{G})} \frac{|G|}{\bigl|\operatorname{Orb}(t_i)\bigr|} \cdot \bigl|\operatorname{Orb}(t_i)\bigr| = |G| \cdot C(\mathcal{G}).$$

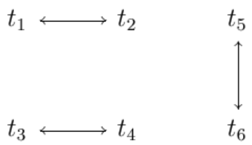
□

Пример 4.2. Действие четверной группы Клейна V_4 на множестве $T = \{\, t_1, \ldots, t_6 \,\}$:

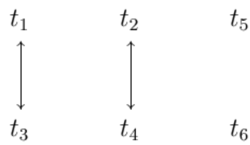
$\circ$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$\star$	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

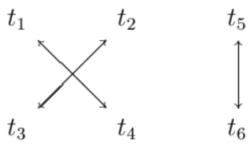
a :



b :



ab :



$$Type(e) = \langle 6, 0, 0, 0, 0, 0\rangle, \quad Type(a) = \langle 0, 3, 0, 0, 0, 0\rangle,$$
$$Type(b) = \langle 2, 2, 0, 0, 0, 0\rangle, \quad Type(ab) = \langle 0, 3, 0, 0, 0, 0\rangle.$$
$$C(e) = 6,\ C(a) = C(ab) = 3,\ C(b) = 4.$$
$$\operatorname{Stab}(t_1) = \operatorname{Stab}(t_2) = \operatorname{Stab}(t_3) = \operatorname{Stab}(t_4) = e \leqslant V_4,$$
$$\operatorname{Stab}(t_5) = \operatorname{Stab}(t_6) = \langle e, b\rangle \leqslant V_4.$$
$$\operatorname{Fix}(a) = \operatorname{Fix}(ab) = \varnothing,\ \operatorname{Fix}(b) = \{t_5, t_6\},\ \operatorname{Fix}(e) = T.$$
$$\bigl|\operatorname{Orb}(t_1)\bigr| = \frac{4}{1} = 4, \quad \bigl|\operatorname{Orb}(t_5)\bigr| = \frac{4}{2} = 2.$$

$$\frac{1}{4}\sum_{g\in G}\bigl|\operatorname{Fix}(g)\bigr| = \frac{6+2}{4} = 2,$$

$$\frac{1}{4}\sum_{t\in T}\bigl|\operatorname{Stab}(t)\bigr| = \frac{4\cdot 1 + 2\cdot 2}{4} = 2.$$

Как применять лемму Бёрнсайда?

> Для определения числа классов эквивалентности надо представить *отождествляемые элементы множества* T *как классы эквивалентности* действия некоторой группы $\mathcal{G}$ на T и по лемме Бёрнсайда определить $C(\mathcal{G})$.

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 $\mathcal{G} \cong \mathbb{Z}_2 = \{e, f\}$. Действие f: переставляет в слове крайние буквы.

Число неэквивалентных слов = число классов эквивалентности действия $\mathbb{Z}_2 \underset{\alpha}{:} T$ —

$$\bigl|\operatorname{Fix}(e)\bigr| = \bigl|T\bigr| = q^l, \qquad \bigl|\operatorname{Fix}(f)\bigr| = q^{l-2}\cdot q = q^{l-1}.$$

$$W = C(\mathbb{Z}_2) = \frac{1}{2}\sum_{g\in G} \bigl|\,\mathrm{Fix}\,(g)\bigr| = \frac{q^l + q^{l-1}}{2} = \frac{q^{l-1}(q+1)}{2}\,.$$

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)	$12\cdot 5 = 60$

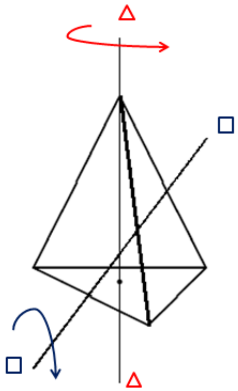
Икосаэдр имеет 20 граней, 30 рёбер и 12 вершин.

Октаэдр

Икосаэдр

Додекаэдр

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 ($\triangle$—$\triangle$); таких осей 4.

f — вращение на 180° вокруг оси, проходящей через центры двух противоположных рёбер ($\square$—$\square$); таких осей 3.

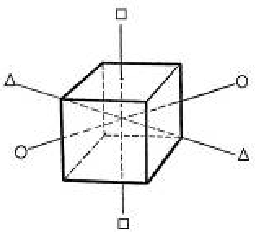
$|T| = (3-1)\cdot 4 + (2-1)\cdot 3 + 1 = 12.$

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 ($\square$—$\square$), таких осей 3;

f — вращение на 180° вокруг оси, проходящей через середины двух противоположных рёбер ($\circ$—$\circ$), таких осей 6;

r — вращение на 120° вокруг оси, проходящей через две противоположные вершины ($\triangle$—$\triangle$) 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 $\left|E_0\right| \cdot \left|V\right|$, где $\left|E_0\right|$ — число рёбер, выходящих из одной вершины и $\left|V\right|$ — число вершин многогранника.

Цикловой индекс. Существует универсальный способ вычисления числа $C(\mathcal{G})$ — количества классов эквивалентности (= орбит).

Сопоставим каждой перестановке $g \in \mathcal{G}$ вес $w(g)$ по правилу:

$$Type(g) = \langle \nu_1, \ldots, \nu_N\rangle \ \Rightarrow \ w(g) = \underbrace{x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}}_{\text{моном}}.$$

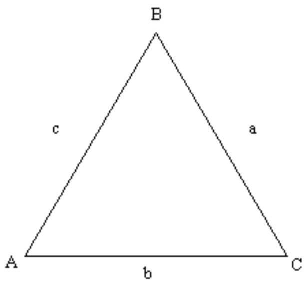
<u>*Определение*</u> 4.3. Средний вес подстановок в группе называется *цикловым индексом* действия $\mathcal{G} \underset{\alpha}{:} T$:

$$P(\mathcal{G} \underset{\alpha}{:} T, x_1, \ldots, x_N) = \frac{1}{|G|} \sum_{g \in G} w(g) = \\ = \frac{1}{|G|} \sum_{g \in G} x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}.$$

Будем также использовать обозначения $P_{\mathcal{G}}(x_1, \ldots, x_N)$ и $P_{\mathcal{G}}$, $P(\mathcal{G})$.

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, $N = 3$.
$\mathcal{G} \cong S_3$ — все перестановки сторон, $n = 3! = 6$.



$\mathcal{G} \underset{\alpha}{:} T$ — самодействие группы S_3

Треугольник — самодвойственная фигура $\Rightarrow$
$\Rightarrow$ действие на стороны $=$
$=$ действие на вершины

$$\mathcal{G} \underset{\alpha}{:} T = \langle t, f \rangle = \\ = \{ e, \underbrace{(abc)}_{t}, \underbrace{(acb)}_{t^2}, \underbrace{((a)(bc))}_{f}, \underbrace{((b)(ac))}_{tf}, \underbrace{((c)(ab))}_{t^2 f} \}.$$

$g \in S_3$	$Type(g)$	$w(g)$	# 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

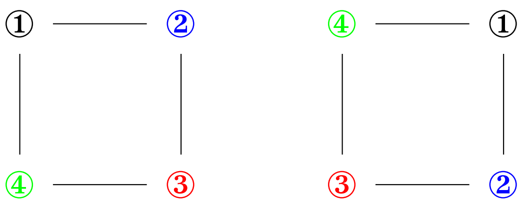
$$P(S_3) \;=\; \frac{1}{6}\Big[\, x_1^3 + 2x_3^1 + 3x_1^1x_2^1 \,\Big],$$

— цикловой индекс *самодействия группы* S_3, или, что то же, *группы симметрии треугольника.*

Зачем нужен цикловой индекс?
Пусть заданы множество T, группа $\mathcal{G}$ и действие $\mathcal{G} \underset{\alpha}{:} T$.

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 $g \in \mathcal{G}$ с типом $\langle\, \nu_1,\, \ldots,\, \nu_N \,\rangle$ будет иметь $\left|\,\mathrm{Fix}\,(g)\right| = r^{C(g)}$ неподвижных точек: каждый класс эквивалентности это g-цикл, их $C(g)$ и

$$\left|\,\mathrm{Fix}\,(g)\right| \,=\, x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}\Big|_{x_1=\ldots=x_N=r} \,=\, r^{C(g)}.$$

Отсюда, по лемме Бёрнсайда, число полученных классов эквивалентности = неэквивалентных раскрасок:

Теорема 4.1.

$$C(\mathcal{G} \underset{\alpha}{:} T) \,=\, P(\mathcal{G} \underset{\alpha}{:} T,\, x_1,\, \ldots,\, x_N)\Big|_{x_1=\ldots=x_N=r}.$$

Например, $P_{\mathcal{G}}(1,\, \ldots,\, 1) \,=\, 1$: 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):

$$\mathcal{G} = \{\, e,\, g \,\} \,\cong\, \mathbb{Z}_2; \qquad T\colon \underbrace{\bigcirc \overbrace{\bigcirc \ldots \bigcirc}^{l-2} \bigcirc}_{l}.$$

$g \in \mathcal{G}$	$Type(g)$	$w(g)$	# 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: $P(x_1,\, \ldots,\, x_l) \;=\; \dfrac{1}{2}\left[x_1^l + x_1^{l-2}x_2^1\right].$

$$W \;=\; P(q,\, \ldots,\, q) \;=\; \frac{q^l + q^{l-1}}{2}.$$

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?*

[2] т.н. *карусель*

[3] двойной пирамиды

1. Ожерелья одинаковы, если одно получается из другого *поворотом*.

Решение. $\mathcal{G} \cong \mathbb{Z}_5 = \langle t \rangle$, $t^5 = e$, $n = 5$.

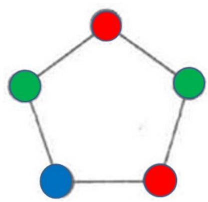
Элемент $\mathbb{Z}_5$	$Type(g)$	$w(g)$	# мономов
e	$\langle\, 5,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_1^5	1
$t,\, t^2,\, t^3,\, t^4$	$\langle\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_5	4

$$\text{Цикловой индекс: } P(x_1, \ldots, x_5) = \frac{1}{5}\left[\, x_1^5 + 4x_5 \,\right].$$

$$\#Col(3) = P(3, \ldots, 3) = \frac{1}{5}\left(3^5 + 4 \cdot 3\right) = 51.$$

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 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. $\mathcal{G}$ — *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 простртнстве — 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).

Цикловой индекс самодействия D_4:

$$P_{D_4}(x_1,\,\ldots,\,x_4) \;=\; \frac{1}{8}\left[\,x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2x_2\,\right].$$

Число раскрасок квадрата в r цветов:

$$P_{D_4}(r,\,\ldots,\,r) \;=\; \frac{1}{8}\left[\,r^4 + 2r + 3r^2 + 2r^3\,\right].$$

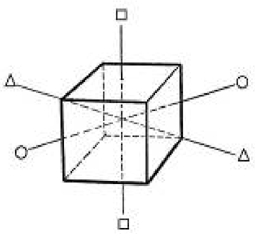
В частности, в два и три цвета:

$$\#Col(2) = \frac{2^4 + 4\cdot 2^2 + 2^4}{2^3} \;=\; 2+2+2 \;=\; 6,$$
$$\#Col(3) = \frac{3^4 + 2\cdot 3 + 3^4}{8} \;=\; 21.$$

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: $\mathcal{G} = O = \langle\, t,\ f,\ r\,\rangle$, $|O| = 24$.



$O = \langle t, f, r\rangle, t^4 = f^2 = r^3 = e$, 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, …, 4, а вершины грани ② — числами 5, …, 8 так, что вершина с номером i смежна с вершиной с номером $i+4$, $i = 1, 2, 3, 4$.

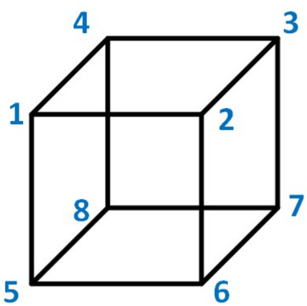
Перестановки далее указаны для случая, когда ось вращения

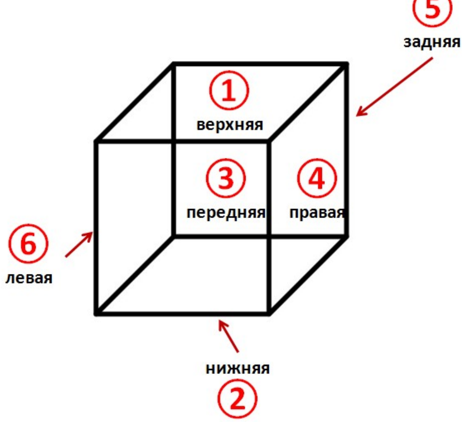
$\langle t \rangle$ проходит через середины граней ① и ②,

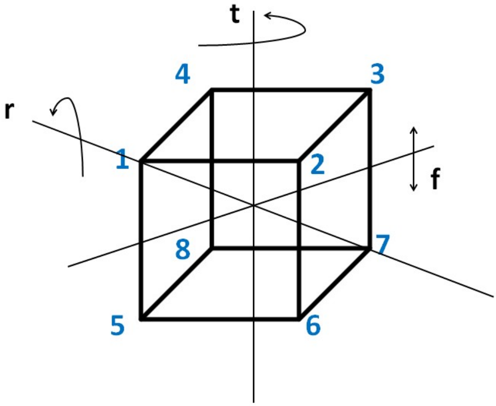
$\langle f \rangle$ проходит через середины рёбер (3-7) и (1-5),

$\langle s \rangle$ 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

$$P(x_1,\ \ldots,\ x_6) \;=\; \frac{1}{24}\left[\, x_1^6 + 6x_1^2 x_4 + 3x_1^2 x_2^2 + 6x_2^3 + 8x_3^2 \,\right].$$

$$\#Col(2) \;=\; \frac{1}{24}\left[2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 8\cdot 2^2\right] \;=\; 10,$$

$$\#Col(3) \;=\; \frac{1}{24}\left[3^6 + 12\cdot 3^3 + 3\cdot 3^4 + 8\cdot 3^2\right] \;=\; 48.$$

Цикловой индекс действия группы октаэдра на множестве R *рёбер куба* ($|R| = N = 12$):

$g \in O$	$Type(g)$	$w(g)$	#
e	$\langle\, 12,\ 0,\ \ldots \rangle$	x_1^{12}	1
t, t^3	$\langle\, 0,\ 0,\ 0,\ 3,\ 0,\ 0\,\rangle$	x_4^3	$3 \cdot 2 = 6$
t^2	$\langle\, 0,\ 6,\ 0,\ \ldots \rangle$	x_2^6	3
f	$\langle\, 2,\ 5,\ 0,\ \ldots \rangle$	$x_1^2 x_2^5$	6
r, r^2	$\langle\, 0,\ 0,\ 4,\ 0,\ \ldots \rangle$	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	$\langle\, 8,\ 0,\ \ldots \rangle$	x_1^8	1
t, t^3	$\langle\, 0,\ 0,\ 0,\ 2,\ 0,\ 0\,\rangle$	x_4^2	$3 \cdot 2 = 6$
t^2	$\langle\, 0,\ 4,\ 0,\ \ldots \rangle$	x_2^4	3
f	$\langle\, 0,\ 4,\ 0,\ \ldots \rangle$	x_2^4	6
r, r^2	$\langle\, 2,\ 0,\ 2,\ 0,\ \ldots \rangle$	$x_1^2 x_3^2$	$4 \cdot 2 = 8$

$$P(O \underset{\alpha}{:} V) \;=\; \frac{1}{24}\left[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\right].$$

Цикловые индексы самодействия $S_n, \mathbb{Z}_n, D_n$ и действия O на элементы куба.

$$P(S_n) = \sum_{\substack{(j_1,\ldots,j_n)\in\mathbb{N}_0^n \\ 1j_1+2j_2+\ldots+nj_n=n}} \frac{x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}}{(1^{j_1}j_1!)(2^{j_2}j_2!)\ldots(n^{j_n}j_n!)},$$

$$P(\mathbb{Z}_n) = \frac{1}{n}\sum_{d|n}\varphi(d)\,x_d^{n/d}, \quad \varphi \text{ — функция Эйлера},$$

$$P(D_n) = \frac{1}{2}P(\mathbb{Z}_n) + \begin{cases} \frac{1}{2}\,x_1x_2^{(n-1)/2}, & n \text{ нечётно}, \\ \frac{1}{4}\left[x_2^{n/2} + x_1^2x_2^{n/2-1}\right], & n \text{ чётно}, \end{cases}$$

$$P(O \underset{\alpha}{:} V) = \frac{1}{24}\left[x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2\right],$$

$$P(O \underset{\alpha}{:} E) = \frac{1}{24}\left[x_1^{12} + 3x_2^6 + 8x_3^4 + 6x_1^2x_2^5 + 6x_4^3\right],$$

$$P(O \underset{\alpha}{:} F) = \frac{1}{24}\left[x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2\right].$$

4.3 Решение комбинаторных задач с помощью теоремы Пойа

К множеству T, $|T| = N$, группе $\mathcal{G}$, $|G| = n$ и действию $\mathcal{G} \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \ldots, c_r\}$, меток («красок»), и совокупность функций $F = R^T$ — приписывания меток (*раскрашиваний*) элементам T.

$\mathcal{G}$, действуя на T, действует и на R^T — операция

$$R^T \times G \to R^T.$$

Придадим вес элементам R: $w(c_i) = y_i$, $i = \overline{1, r}$.

Теорема 4.2 (Редфилда-Пойа; 1927, 1937). *Цикловой индекс действия группы $\mathcal{G}$ на R^T есть*

$$P(\mathcal{G} \underset{\alpha}{:} R^T,\, y_1,\, \ldots,\, y_r) =$$

$$= P(\mathcal{G} \underset{\alpha}{:} T,\, x_1,\, \ldots,\, x_N)\Big|_{x_k = y_1^k + \ldots + y_r^k,\; k = \overline{1,N}}.$$

Следствие. *Если все веса выбраны одинаковыми ($y_1 = \ldots = y_r = 1$), то $x_1 = \ldots = x_N = r$ и $W(F)$ — число классов эквивалентности*

$$C(\mathcal{G} \underset{\alpha}{:} R^T) = C(\mathcal{G} \underset{\alpha}{:} T) = P(\mathcal{G} \underset{\alpha}{:} T, r, \ldots, r)$$

— лемма Бёрнсайда.

Что можно определить (подсчитать) с помощью:

леммы Бёрнсайда — *общее число* неэквивалентных разметок (раскрасок);

теорема Редфилда-Пойа — число разметок *данного типа*, т.е. содержащих данное количество элементов конкретного цвета.

Дьёрдь Пойа
(Pólya György, 1887–1985)
— венгерско-швейцарско-американский математик.
Работал в Высшей технической школе в Цюрихе,
а с 1940 г. — в Стэнфордском университете (США).

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: $\mathcal{G} = D_5$, цикловой индекс

$$P(x_1, \ldots, x_5) = \frac{1}{10}\left[\, x_1^5 + 4x_5 + 5x_1x_2^2 \,\right],$$

всего ожерелий $P(3, \ldots, 3) = 39$.

$x_1 = y_1+y_2+y_3,\;\; x_2 = y_1^2+y_2^2+y_3^2,\;\; \ldots,\;\; x_5 = y_1^5+y_2^5+y_3^5.$

$$\begin{cases} w(\textit{красный}) & = y_1, \\ w(\textit{синий}) & = y_2, \\ w(\textit{зелёный}) & = y_3 \end{cases} \Rightarrow \begin{cases} y_1 = y, \\ y_2 = y_3 = 1 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} x_1 & = y + 2, \\ x_2 & = y^2 + 2, \\ \ldots \\ x_5 & = y^5 + 2. \end{cases} \qquad \begin{array}{l} x_k \mapsto y^k + 2,\; k = \overline{1,5}; \\ P(y) = \displaystyle\sum_{i=1}^{5} u_i y^i; \\ \boxed{u_2 = ?} \end{array}$$

$$P(y) = \frac{1}{10}\left[\, u_0 + u_1y + u_2y^2 + \ldots + u_5y^5 \,\right] =$$

$$= \frac{1}{10}\left[\, (y+2)^5 + 4(y^5+2) + 5(y+2)(y^2+2)^2 \,\right] =$$

$$= \frac{1}{10}\left[\, \ldots + C_5^2 2^3 y^2 + \ldots + 5(y+2)(y^4+4y^2+4) \,\right] =$$

$$= \frac{1}{10}\left[\, \ldots + (10 \cdot 8 + 5 \cdot 2 \cdot 4)\, y^2 + \ldots \,\right].$$

$u_2 = 8 + 4 = 12.$

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 —

$$P(O \underset{\alpha}{:} V;\, x_1, \ldots x_8) = \frac{1}{24}\left[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\right].$$

1) $\quad \#Col(2) = P(x_1, \ldots, x_8)\Big|_{x_1 = \ldots = x_8 = 2} =$

$$= \frac{2^8 + 6\cdot 2^2 + 9\cdot 2^4 + 8\cdot 4\cdot 4}{3\cdot 2^3} = \frac{32 + 3 + 18 + 16}{3} = 23.$$

2) $w(\textit{красный}) = y,\ w(\textit{синий}) = 1,$
$x_k = y^k + 1,\ k = \overline{1,8}$:

$$\#Col(4,4) = \frac{1}{24}\left[\,(y+1)^8 + 9\cdot(y^2+1)^4 + 6\cdot(y^4+1)^2 + \right.$$
$$\left. + 8\cdot(y+1)^2(y^3+1)^2\,\right] =$$
$$= \frac{1}{24}\left[\ldots + C_8^4 y^4 + \ldots + 9(\ldots 4y^2 + 6y^4 + \ldots) + \right.$$
$$\left. \ldots + 6\cdot 2y^4 \ldots + 8(\ldots + 2y + y^2 + \ldots)(\ldots + 2y^3 + \ldots)\,\right].$$

$$u_4 = \frac{1}{24}\big[\,70 + 9\cdot 6 + 6\cdot 2 + 8\cdot 2\cdot 2\,\big] = \frac{168}{24} = 7.$$

3) $\#Col(\leqslant 2, *) = u_0 + u_1 + u_2$, очевидно $u_0 = u_1 = 1$.

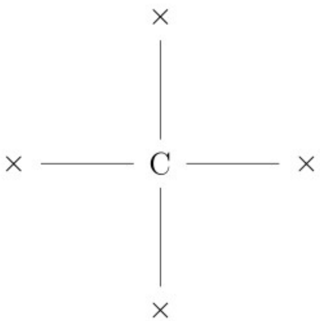
$$u_2 = \frac{1}{24}\big[\ldots + 28y^2 + 9(\ldots + 4y^2 \ldots) + 8(\ldots + y^2 + \ldots)\big] = \\ = \frac{28 + 36 + 8}{24} = 3.$$

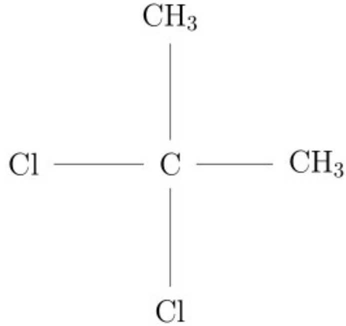
$\#Col(\leqslant 2, *) = 1 + 1 + 3 = 5.$

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: $x_k \;=\; \mathrm{H}^k + 3,\; k = \overline{1, 4}$.

$$\begin{aligned} &P(H) \;= \\ &= \frac{1}{12}\left[\, (\mathrm{H}+3)^4 + 8\,(\mathrm{H}+3)\left(\mathrm{H}^3+3\right) + 3\left(\mathrm{H}^2+3\right)^2 \right] = \\ &\quad= \frac{1}{12}\,\Big[\, \left(\mathrm{H}^4 + 4 \cdot \mathrm{H}^3 \cdot 3 + 6 \cdot \mathrm{H}^2 \cdot 9 + 4 \cdot \mathrm{H} \cdot 27 + 81\right) + \\ &\qquad +8\left(\mathrm{H}^4 + 3\mathrm{H}^3 + 3\mathrm{H} + 9\right) + 3\left(\mathrm{H}^4 + 6\mathrm{H}^2 + 9\right) \Big] \;= \\ &\qquad\qquad = \; 1 \cdot \mathrm{H}^4 + 3 \cdot \mathrm{H}^3 + 6 \cdot \mathrm{H}^2 + 11 \cdot \mathrm{H} + 15. \end{aligned}$$

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 — $1 + 3 + 6 + 11 + 15 \;=\; 36$.

Задача 4.8 (об ожерельях со стоимостью). *Стоимости камней для ожерелий равны: красного — 1 ед., сине-*

го — 2 ед., зелёного — 3 ед. Сколько существует ожерелий из 15 таких камней, стоимость которых равна 30 ед.?

Решение. Цикловой индекс самодействия группы диэдра (было ранее):

$$P(D_n) = \frac{1}{2n}\sum_{d|n}\varphi(d)\,x_d^{n/d} + \begin{cases} \frac{1}{2}x_1 x_2^{(n-1)/2}, & n \text{ нечётно},\\ \frac{1}{4}\left[x_2^{n/2} + x_1^2 x_2^{n/2-1}\right], & n \text{ чётно}, \end{cases}$$

Для $n = 15$: $D(15) = \{\,1,\,3,\,5,\,15\,\}$

$$\varphi(1) = 1, \quad \varphi(3) = 2, \quad \varphi(5) = 4, \quad \varphi(15) = 8.$$

$$P_{D_{15}} = \frac{1}{30}\left[\,x_1^{15} + 2x_3^5 + 4x_5^3 + 8x_{15}^1 + 15x_1x_2^7\,\right].$$

С учётом стоимости камней необходимая подстановка в цикловой индекс: красный — $y_1 = y$,
синий — $y_2 = y^2$,
зелёный — $y_3 = y^3$,

откуда $x_k = y^k + y^{2k} + y^{3k}$.

$$W = \frac{1}{30}\Big[\left(y + y^2 + y^3\right)^{15} + 2\left(y^3 + y^6 + y^9\right)^5 + \\ + 4\left(y^5 + y^{10} + y^{15}\right)^3 + 8\left(y^3 + y^{30} + y^{45}\right)^1 + \\ +15\left(y + y^2 + y^3\right)\left(y^2 + y^4 + y^6\right)^7\Big] = \ldots + u_{30}y^{30} + \ldots.$$

$$u_{30} = \frac{1}{30}\left[\sum_{i=0}^{7} C_{15}^{i,15-i,i} + 2\sum_{i=0}^{2} C_5^{i,5-i,i} + 4\sum_{i=0}^{1} C_3^{i,3-i,i} + \right. \\ \left. + 8 + 15\sum_{i=0}^{3} C_7^{i,7-i,i}\right] = 59\,788.$$

4.4 Задачи с решениями

Задача 4.9. *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 4.10. *Найти цикловой индекс для следующим образом определённого самодействия четверной группы Клейна*
$V_4 = \left\{ e,\, a,\, b,\, ab \mid a^2 = b^2 = (ab)^2 = e^2 = e,\, ab = ba \right\}$:

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

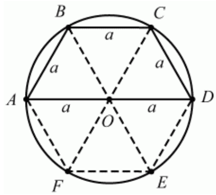
$$P_{V_4} = \frac{1}{4}\left[\, x_1^4 + 3x_2^2 \,\right].$$

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 4.11. *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 4.12. *На стеклянных пластинах рисуют одинаковые прямоугольники (не квадраты) и раскрашивают их стороны в* r *цветов.*

Сколько можно нарисовать таких различных прямоугольников? Конкретно, при $r = 2$?

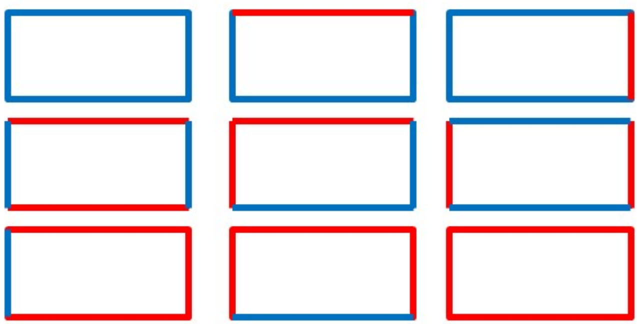
Решение. Найдём цикловой индекс $R \underset{\alpha}{:} S$ действия группы R самосовмещений прямоугольника в пространстве на его стороны. Группа $R = \langle t, f \rangle$ порождается образующими: t — вращение вокруг центра симметрии на $180°$, f — отражение вокруг оси, проходящей через середины противоположных 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 4.13. *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.

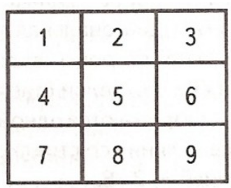
$g \in R$	$Type(g)$	$w(g)$	#
e	$\langle\, 4,\, 0,\, 0,\, 0\,\rangle$	x_1^4	1
t	$\langle\, 0,\, 2,\, 0,\, 0\,\rangle$	x_2^2	1
f	$\langle\, 0,\, 2,\, 0,\, 0\,\rangle$	x_2^2	2

$$P(R \underset{\alpha}{:} V;\, x_1,\, x_2,\, x_3,\, x_4) \,=\, \frac{1}{4}\left[\, x_1^4 + 3x_2^2\,\right]$$

Число прямоугольников:

$$\#Col(3) \,=\, P(R \underset{\alpha}{:} V; 3, \ldots, 3) \,=\, \frac{81+27}{4} \,=\, 27$$

Задача 4.14. *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	$(1)\ldots(9)$	$\langle\, 9,\, 0,\, \ldots \,\rangle$	x_1^9	1
t, t^3	$(5)(1397)(2684)$	$\langle\, 1,\, 0,\, 0,\, 2,\, \ldots \,\rangle$	$x_1x_4^2$	2
t^2	$(5)(19)(37)(28)(79)$	$\langle\, 1,\, 4,\, 0,\, \ldots \,\rangle$	$x_1x_2^4$	1
$s, f, \ldots$	$(2)(5)(8)(13)(48)(79)$	$\langle\, 3,\, 3,\, 0,\, \ldots \,\rangle$	$x_1^3x_2^3$	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 4.15 (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	$(1)\ldots(16)$	$\langle 16, 0, \ldots \rangle$	x_1^4	1
$t,\ t^3$	$(1,4,16,13)\ldots(6,7,11,10)$	$\langle 0, 0, 0, 4, \ldots \rangle$	x_4^4	2
t^2	$(1,16)\ldots(6,11)$	$\langle 0, 8, 0 \ldots \rangle$	x_2^8	1
f	$(1,4)\ldots(10,11)$	$\langle 0, 8, 0, \ldots \rangle$	x_2^8	2
s	$(1)\ldots(16)(2,5)\ldots(12,15)$	$\langle 4, 6, 0, \ldots \rangle$	$x_1^4 x_2^6$	2

Цикловой индекс действия группы D_4 на элементы компостера:

$$P(x_1,\,\ldots,\,x_4) \;=\; \frac{1}{8}\left[\,x_1^{16} + 2x_4^4 + 3x_2^8 + 2x_1^4x_2^6\,\right].$$

Наличие/отсутствие в клетке символа $\bullet$ описывается их отображением в двухэлементное множество (раскраске в два цвета), поэтому число различных компостеров есть $P(2,\,2,\,\ldots) =$

$$= \frac{1}{8}\left[\,2^{16} + 2\cdot 2^4 + 3\cdot 2^8 + 2\cdot 2^4\cdot 2^6\,\right] \;=\; 8548.$$

К аналогичной задаче сводится задача о числе фотошаблонов рисунков соединений для интегральных схем.

Задача 4.16. *Найти число различных вариантов раскраски граней куба в 2 и 3 цвета.*

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} F) \;=\; \frac{1}{24}\left[x_1^6 + \underline{6x_1^2x_4} + 3x_1^2x_2^2 + \underline{6x_2^3} + 8x_3^2\right].$$

$$\#Col(2) \;=\; \frac{2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 2^5}{3\cdot 2^3} \;=\; 10.$$

$$\#Col(3) = \frac{3^6 + 12 \cdot 3^3 + \cdot 3^5 + 8 \cdot 3^2}{3 \cdot 8} = 57.$$

<u>Задача</u> 4.17. *Определить число различных раскрасок всех граней правильной 4-угольной пирамиды П в 3 цвета.*

Решение. Занумеруем последовательно боковые грани П числами 1, … 4, а основание — 5.
$\mathcal{G} \cong \mathbb{Z}_4 = \langle\, t \,\rangle$, 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
$t, t^3 = (1234)(5)$	$\langle\, 1,\, 0,\, 0,\, 1,\, 0 \,\rangle$	$x_1 x_4$	2
$t^2 = (12)(34)(5)$	$\langle\, 1,\, 2,\, 0,\, 0,\, 0 \,\rangle$	$x_1 x_2^2$	1

$$P(x_1,\, \ldots,\, x_5) = \frac{1}{4}\left[\, x_1^5 + 2x_1x_4 + x_1x_2^2 \,\right],$$

$$P(3, \ldots, 3) = \frac{3^5 + 2 \cdot 3^2 + 3^3}{4} = \frac{9 \cdot 32}{4} = 72.$$

<u>Задача</u> 4.18. *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 4.19. *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 4.20. *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 иницидентны 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

$$P(T \underset{\alpha}{:} E, x_1, \dots, x_6) = \frac{1}{12}\left[\, x_1^6 + 8x_3^2 + 3x_1^2 x_2^2 \,\right].$$

$$\#Col(2) = \frac{2^6 + 8 \cdot 2^2 + 3 \cdot 2^4}{3 \cdot 2^2} = \frac{15 + 9 + 12}{3} = 12,$$

$$\#Col(3) = \frac{3^6 + 8 \cdot 3^2 + 3 \cdot 3^4}{3 \cdot 4} = 87.$$

Задача 4.21. *Найти число различных вариантов раскраски рёбер куба в 2 цвета.*

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} R) = \frac{1}{24}\left[\, x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2 x_2^5 + 8x_3^4 \,\right].$$

$$\#Col(2) = \frac{2^{12} + 6 \cdot 2^3 + 3 \cdot 2^6 + 7 \cdot 2^7}{3 \cdot 2^3} = 218.$$

Задача 4.22. *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 4.23. *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), $x_1 = y+2$, $x_2 = y^2+2$, $x_3 = y^3+2$.

$$P(y) = \frac{1}{6}\left[\,(y+2)^6 + (y^2+2)^3 + 2(y^3+2)^2 +\right.$$

$$+2(y^6+2)\,\big] = \frac{1}{6}\left[u_0+u_1y+u_2y^2+\ldots+u_6y^6\right] =$$
$$= \frac{1}{6}\Big[\big(2^6+2^3+2^3+4\big)+6\cdot 2^5\,y+$$
$$+\big(16\cdot 15+2\cdot 3\cdot 2^2\big)\,y^2+\ldots\Big].$$

$u_0 = 84/6 = 14$, $u_1 = 2^5 = 32$, $u_2 = (240{+}24)/6 = 44$.

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:

$$P(O \underset{\alpha}{:} F) = \frac{1}{3\cdot 2^3}\left[x_1^6 + \underline{6x_1^2x_4} + 3x_1^2x_2^2 + \underline{6x_2^3} + 8x_3^2\right].$$

1) $\#Col(2) = \dfrac{2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 2^5}{3\cdot 2^3} = \dfrac{30}{3} = 10.$

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:

$$W = \frac{1}{24}\left[\ldots + C_6^4y^4 + \ldots + 6(y^2+2y+1)(\underline{y^4}+1) + \right.$$
$$+3(\underline{y^2}+2y+1)(\underline{y^4}+2\underline{y^2}+1)+$$
$$\left. +6(y^6+3\underline{y^4}+3y^2+1) + 8(y^6+2y^3+1)\,\right].$$

$$u_4 = \frac{15+6+9+18}{3\cdot 8} = \frac{5+2+3+6}{8} = \frac{16}{8} = 2.$$

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) $\#Col(3) = \dfrac{1}{8}\left[\, 3^4 + 2\cdot 3 + 3\cdot 3^2 + 2\cdot 3^2\cdot 3 \,\right] = 21.$

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 $u_{10} + u_{11} + u_{12}$.

$$W = \frac{1}{8}\,\Big[\,(y_1 + (y_2+1))^4 + 2(y_1^4 + y_2^4 + 1) +$$
$$+3(y_1^2 + (y_2^2+1))^2 + 2(y_1 + (y_2+1))^2(y_1^2 + y_2^2 + 1)\,\Big]\ \boxed{=}$$

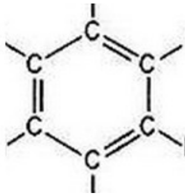
нас интересуют только члены с y_1^1 (одно красное ребро)

$$\frac{1}{8}\,\Big[\,y_1^4 + 4y_1^3(y_2+1) + 6y_1^2(y_2+1)^2 + \underline{4y_1(y_2+1)^3} +$$
$$+\,(y_2+1) + \ldots$$
$$+2(y_1^2 + \underline{2y_1(y_2+1)} + (y_2+1)^2)(y_1^2 + y_2^2 + 1)\,\Big] =$$
$$= \frac{1}{8}\,\left[\,\ldots + 4y_1(y_2+1)^3 + 4y_1(y_2+1)(y_2^2+1))\,\right] =$$
$$= \frac{1}{8}\,\Big[\ldots + 4y_1(y_2^3 + \underline{3y_2^2 + 3y_2^1 + 1}) +$$
$$+4y_1(y_2^3 + \underline{y_2 + y_2^2 + 1})\,\Big]\ \boxed{=}$$

нас интересуют только члены с y_2^0, y_2^1 и y_2^2 при y_1 (синих рёбер — 0, 1, 2)

$$\boxed{=}\ \frac{1}{8}\,[\,4\cdot 7 + 4\cdot 3\,] = \frac{4\cdot 10}{8} = 5.$$

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	$(1)\ldots(6)$	$\langle\, 6,\, 0,\, \ldots\, 0\,\rangle$	x_1^6	1
t, t^5	(123456)	$\langle\, 0,\, \ldots,\, 0,\, 1\,\rangle$	x_6^1	2
t^2, t^4	$(135)(246)$	$\langle\, 0,\, 0,\, 2, \ldots\, 0\,\rangle$	x_3^2	2
t^3	$(14)(25)(36)$	$\langle\, 0,\, 3,\, 0, \ldots\, 0\,\rangle$	x_2^3	1
f	$(14)(23)(56)$	$\langle\, 0,\, 3,\, 0,\, \ldots\, 0\,\rangle$	x_3^2	3
s	$(1)(4)(26)(35)$	$\langle\, 2,\, 2,\, 0,\, \ldots\,\rangle$	$x_1^2 x_2^2$	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 $x_1 = \ldots = x_6 = 2$ (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* $0, \ldots, 6$ *атомами водорода* — обозначение $y_1 = \mathrm{H}$, $y_2 = 1$ и подстановка $x_k \;=\; \mathrm{H}^k + 1$, $k = \overline{1, 6}$ в P.

$$W \;=\; \frac{1}{12}\left[\, (\mathrm{H}+1)^6 + 3(\mathrm{H}+1)^2(\mathrm{H}^2+1)^2 + 4(\mathrm{H}^2+1)^3 + \right.$$
$$\left. +2(\mathrm{H}^3+1)^2 + 2(\mathrm{H}^6+1)\,\right] \;=$$
$$=\; \mathrm{H}^6 + \mathrm{H}^5 + 3\cdot\mathrm{H}^4 + 3\cdot\mathrm{H}^3 + 3\cdot\mathrm{H}^2 + \mathrm{H} + 1\,.$$

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)

$$P(D_n) = \frac{1}{2n}\sum_{d|n}\varphi(d)\, x_d^{n/d} + \begin{cases} \frac{1}{2}x_1 x_2^{(n-1)/2}, & n \text{ нечётно}, \\ \frac{1}{4}\left[x_2^{n/2} + x_1^2 x_2^{n/2-1}\right], & n \text{ чётно}, \end{cases}$$

$n = 6 + 12 = 18,\ D(18) = \{1, 2, 3, 6, 9, 18\}$,

$$\begin{array}{lll} \varphi(1) = 1, & \varphi(3) = 2, & \varphi(9) = 6, \\ \varphi(2) = 1, & \varphi(6) = 2, & \varphi(18) = 6. \end{array}$$

По формуле: $P(D_{18}) =$

$$= \frac{1}{36}\left[x_1^{18} + x_2^9 + 2x_3^6 + 2x_6^3 + 6x_9^2 + 6x_{18}^1\right] + \\ + \frac{1}{4}\left[x_2^9 + x_1^2 x_2^8\right] =$$

$$= \frac{1}{36}\left[x_1^{18} + 10x_2^9 + 2x_3^6 + 2x_6^3 + 6x_9^2 + 6x_{18}^1 + 9x_1^2 x_2^8\right].$$

$x_k = y^k + 1, \quad W = \frac{1}{36}\big[(y+1)^{18} +$

$$+ 10(y^2+1)^9 + 2(y^3+1)^6 + 2(y^6+1)^3 + \\ + 6(y^9+1)^2 + 6(y^{18}+1) + 9(y+1)^2(y^8+1)^8\big] =$$

$$= \frac{1}{36}\Big[\ldots + \big(C_{18}^6 + 10C_9^3 + 2C_3^1 + 2C_6^2 + 0 + 0 + \\ + 9(C_8^2 + C_8^3)\big)\, y^6\Big] =$$

$$= \frac{1}{36}\left[\ldots + (18654 + 840 + 6 + 30 + 756)\, y^6\right] =$$

$$= 561\, y^6.$$

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:

$$P(O \underset{\alpha}{:} R) = \frac{1}{24}\left[\,x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4\,\right].$$

$y_k = x^k + 1,$

$$\begin{aligned} W = \frac{1}{24}\big[\,(y+1)^{12} + 6(y^4+1)^3 + 3(y^2+1)^6 + \\ +6(y+1)^2(y^2+1)^5 + 8(y^3+1)^4\,\big] = \\ = \frac{1}{24}\left[\ldots + \left(C_{12}^5 + 6C_2^1C_5^2\right)\, y^5\right] = \\ = \frac{1}{24}\left[\ldots + (792 + 6\cdot 2\cdot 10)\; y^5\right] = \ldots + \frac{792+120}{24}y^5 = \\ = \ldots + (33+5)\,y^5 = \ldots + 38\,y^5. \end{aligned}$$

Ответ: 38.

Глава 5

Частично упорядоченные множества

5.1 Основные понятия теории ч.у. множеств

Определение 5.1. Пару $\mathcal{P} = \langle P, \leqslant \rangle$, где P — непустое множество, а $\leqslant$ — рефлексивное, антисимметричное и транзитивное бинарное отношение на нём, называют *частично упорядоченным множеством* (сокращённо *ч.у. множеством*, англ. *poset*).

Рефлексивность (R): $x \leqslant x$;
Антисимметричность (AS): $(x \leqslant y) \,\&\, (y \leqslant x) \;\Rightarrow\; x = y$;
Транзитивность (T): $(x \leqslant y) \,\&\, (y \leqslant z) \;\Rightarrow\; x \leqslant z$.

Пример 5.1.

- $\langle \mathcal{P}(M), \subseteq \rangle$ — классический пример ч.у. множества (упорядочивание множеств *по включению*, $M \neq \varnothing$);
- $\langle \mathbb{N}, \leqslant \rangle$ и $\langle \mathbb{N}, | \rangle$ — два упорядочивания одного множества.
- Пусть M — множество людей, $h(x)$ — рост, а $w(x)$ — вес человека x.
  Определим на отношение ρ на M:

$$x\rho y \;\Rightarrow\; (h(x) \leqslant h(y))\,\&\,(w(x) \leqslant w(y))\,.$$

Является ли ρ отношением частичного порядка на M?

Нет. ρ — рефлексивно и транзитивно, но не является антисимметричным отношением: $x\rho y\,\&\,y\rho x \;\not\Rightarrow\; x = y$ (могут найтись два человека с одинаковыми ростом и весом).

Отношения со свойствами (R) и (T) называют *предпорядками.*

Понятное обозначение: $a < b \;\Leftrightarrow\; (a \leqslant b)\&(a \neq b)$

- если $(x \leqslant y)\vee(y \leqslant x)$, то x и y *сравнимы* $(x \sim y)$, иначе они *несравнимы* $(x \nsim y)$;
- *полный (линейный) порядок*, если $\forall\, x, y : x \sim y$;
- если в $\mathcal{P}$ нет ни одной пары различных сравнимых элементов, то это тривиально упорядоченное множество;
- x *непосредственно предшествует* y (y *непосредственно следует за* x), $x \lessdot y$, если $x \leqslant z \leqslant y \;\Rightarrow\; (z = x) \vee (z = y)$;
- $\{\, x \in P \mid a \leqslant x \leqslant b \,\}$ — *интервал* $[\,a, b\,]$;

  Ч. у. множество, все интервалы которого конечны — *локально конечное*;
- $v_1 < \ldots < v_n \stackrel{\text{def}}{=} [v_1, \ldots, v_n]$ — *цепь* $\mathbf{n}$, а совокупность попарно несравнимых элементов — *антицепь* в $\mathcal{P}$;

- цепь *максимальная* (*насыщенная*), если при добавлении к ней любого элемента она перестаёт быть цепью;
- $\geqslant$ — двойственный к $\leqslant$ порядок: $\leqslant^d \Leftrightarrow \geqslant$.

Рис. 5.1. Диаграммы 3-элементных ч.у. множеств

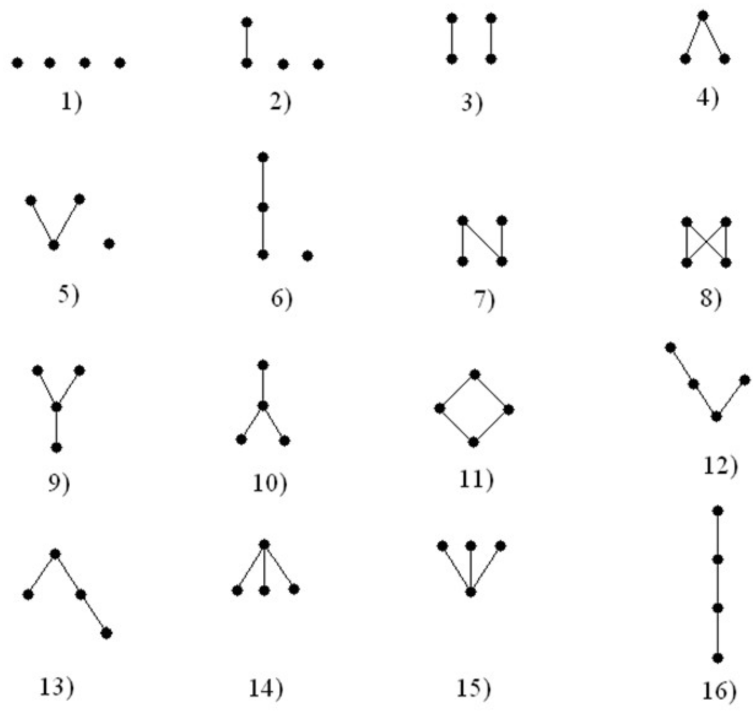


Рис. 5.2. Диаграммы всех 4-элементных ч.у. множеств

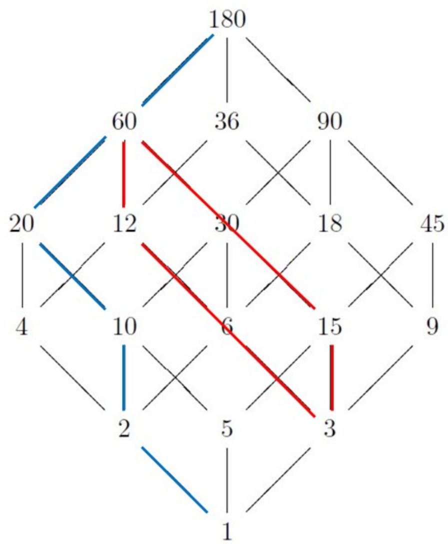


Рис. 5.3. Диаграмма $D(180)$ всех делителей числа $180 = 2^2 3^2 5$. Показаны одна из максимальных цепей и интервал $[\,3,\,60\,]$

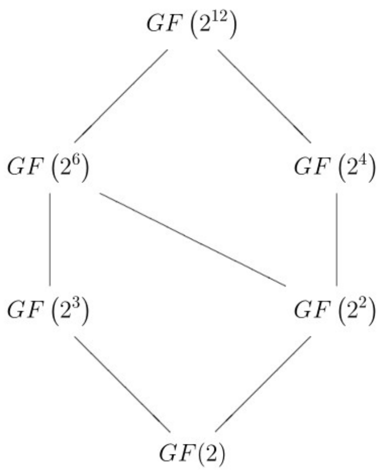


Рис. 5.4. Диаграмма Хассе всех подполей поля $GF\left(2^{18}\right)$, упорядоченных по включению.

Ч.у. множества: особые элементы

Определение 5.2. Элемент $u \in P$ ч.у. множества $\langle P, \leqslant \rangle$ называют:

- *максимальным*, если $u \leqslant x \Rightarrow u = x$,
- *минимальным*, если $u \geqslant x \Rightarrow u = x$,
- *наибольшим*, если $x \leqslant u$,
- *наименьшим*, если $x \geqslant u$

для любых $x \in P$.

Наибольший (1) и наименьший (0) — *граничные элементы*. В конечном ч.у. множестве имеется как минимум по одному максимальному и минимальному элементу.

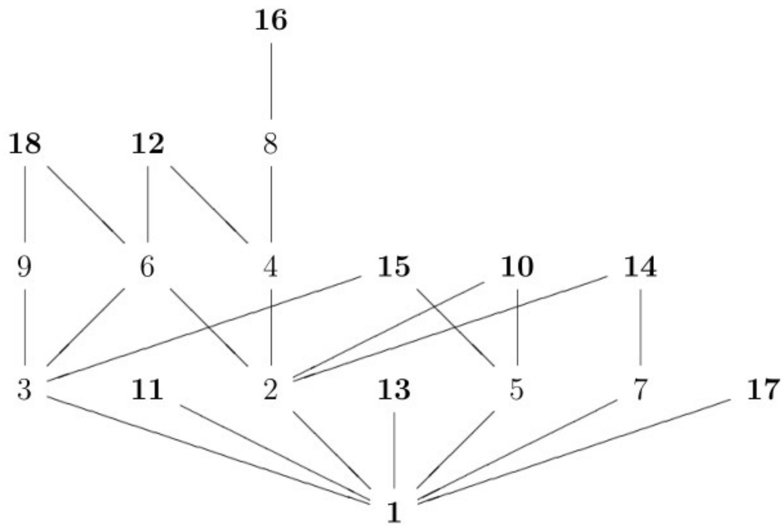


Рис. 5.5. Ч.у. множество $\langle \{1, \ldots, 18\}, | \rangle$. 1 — наименьший элемент, $11 \ldots 18$ — максимальные.

Ранжированные ч.у. множества.

Цепное условие Жордана-Дедекинда Все максимальные цепи между любыми двумя сравнимыми элементами элементами локально конечного ч.у. множества имеют одинаковую длину.

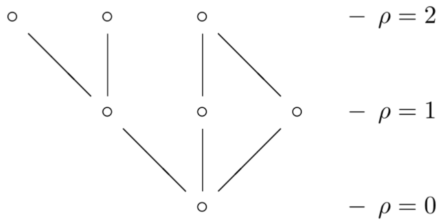
Если ч.у. множество удовлетворяет условию Жордана-Дедекинда и имеет наименьший элемент 0, то оно *ранжируемо*, т.е. на нём можно определить *функцию ранга* ρ:

1. $\rho(0) = 0$;

2. $a \lessdot b \;\Rightarrow\; \rho(b) = \rho(a) + 1$

и такое множество имеет *слои*.

Если множество ранжируемо, то любой его слой (но не только!) является антицепью.



Порядковые гомоморфизмы

<u>*Определение*</u> 5.3. Отображение $\varphi\colon P \to P'$ носителей ч.у. множеств называется соответственно

- *изотонным* (*монотонным*, *порядковым гомоморфизмом*), если $x \leqslant y \;\Rightarrow\; \varphi(x) \leqslant \varphi(y)$;
- *обратно изотонным*, если $\varphi(x) \leqslant \varphi(y) \;\Rightarrow\; x \leqslant y$;
- *антиизотонным*, если $x \leqslant y \;\Rightarrow\; \varphi(x) \geqslant \varphi(y)$.

Если φ изотонно, обратно изотонно и инъективно, то это *вложение* или *(порядковый) мономорфизм* ($P \overset{\varphi}{\hookrightarrow} P'$).

Сюръективный мономорфизм — *(порядковый) изоморфизм* ($P \cong P'$ или $P \overset{\varphi}{\cong} P'$).

Изоморфизм ч.у. множества в себя — *(порядковый) автоморфизм.*

Идеалы и фильтры ч.у. множеств

Определение 5.4. Подмножество J элементов ч.у. множества $\langle P, \leqslant \rangle$ называется его *(порядковым) идеалом*, если

$$(x \in J) \,\&\, (y \leqslant x) \;\Rightarrow\; y \in J.$$

Подмножество F элементов P называется его *(порядковым) фильтром*, если

$$(x \in F) \,\&\, (x \leqslant y) \;\Rightarrow\; y \in F.$$

$\varnothing$ и всё ч.у. множество P — *несобственные* порядковые идеалы.

Важное свойство: объединение и пересечение порядковых идеалов есть порядковый идеал.

Обозначение: $J(P)$ — множество всех порядковых идеалов ч.у. множества P.

Определение 5.5. Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $A \subseteq P$. Множества $A^{\vartriangle}$ и $A^{\triangledown}$

$$A^{\vartriangle} = \left\{ x \in P \mid \underset{A}{\forall} a\ (a \leqslant x) \right\} \text{ и}$$

$$A^{\triangledown} = \left\{ x \in P \mid \underset{A}{\forall} a\ (x \leqslant a) \right\}$$

называются верхним и нижним *конусами* множества A, а их элементы — верхними и нижними *гранями* множества A соответственно.

Для одноэлементного множества $A = \{a\}$ — $a^{\vartriangle}$ и $a^{\triangledown}$.

Понятно, что если $a \leqslant b$, то $a^{\vartriangle} \cap b^{\triangledown} = [\,a,\, b\,]$. $x^{\triangledown} = \langle x \rangle = J(x)$ — идеал, а $x^{\vartriangle}$ — фильтр P; такие идеалы и фильтры называют *главными*.

Пример 5.2.

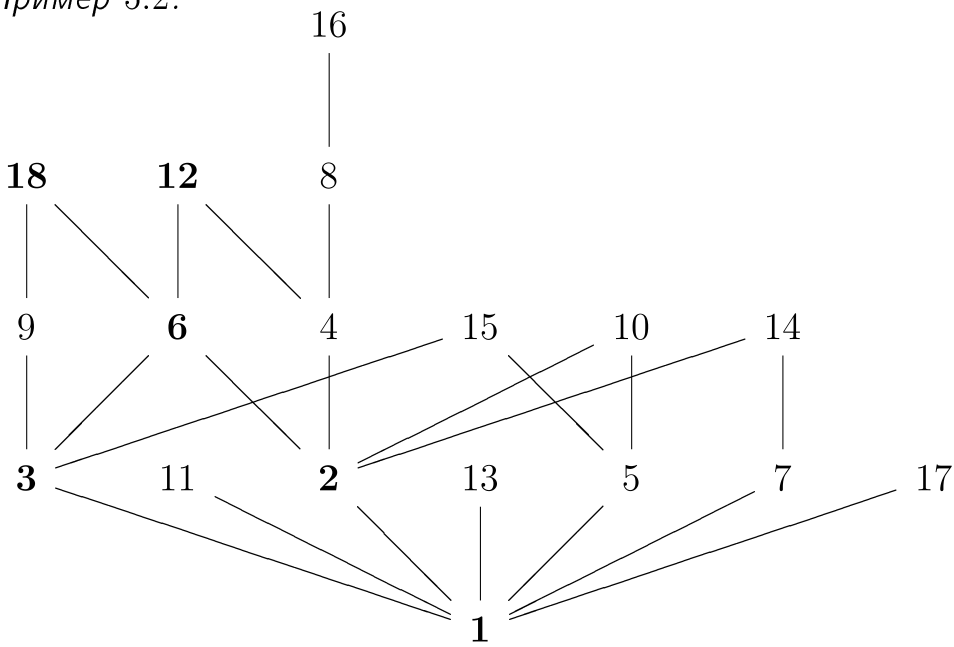


Рис. 5.6. Верхний и нижний конусы множества $\{\,2,\, 3\,\}$

Конечнопорождённый идеал:

$$\langle\, a_1,\, \ldots,\, a_k \,\rangle \stackrel{\text{def}}{=} \bigcup_{i=1}^{k} {a_i}^{\triangledown}, \quad a_i \nsim a_j,\; i \neq j.$$

Пример 5.3.

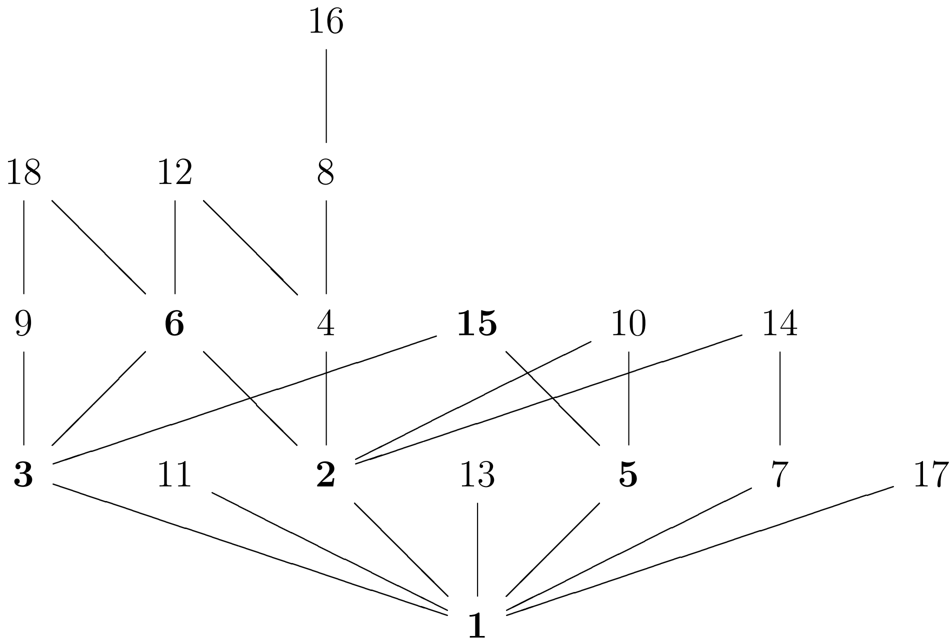
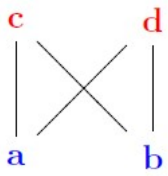


Рис. 5.7. Идеал $\langle\, 6,\, 15 \,\rangle$ ч.у. множества $\langle\, \{\, 1, \ldots, 18\}, \mid \rangle$ выделен

<u>*Определение*</u> 5.6. Пусть $\langle\, P, \leqslant \,\rangle$ — ч.у. множество и $A \subseteq P$.

- Наименьший элемент в $A^{\triangle}$ называется *точной верхней гранью множества* A (символически $\sup A$).
- Наибольший элемент в $A^{\triangledown}$ называется *точной нижней гранью множества* A (символически $\inf A$).

Пример 5.4 (sup A и/или inf A могут не существовать).



$\{a, b\}^{\triangle} = \{c, d\}$, но множество $\{c, d\}$ не имеет инфимума $\Rightarrow$ $\sup\{a, b\}$ отсутствует. Аналогично, отсутствует $\inf\{c, d\}$.

5.2 Операции над ч.у. множествами

Пересечение

$$\langle\, P, \leqslant_1 \rangle \cap \langle\, P, \leqslant_2 \rangle \ = \ \langle\, P, \leqslant_1 \cap \leqslant_2 \rangle.$$

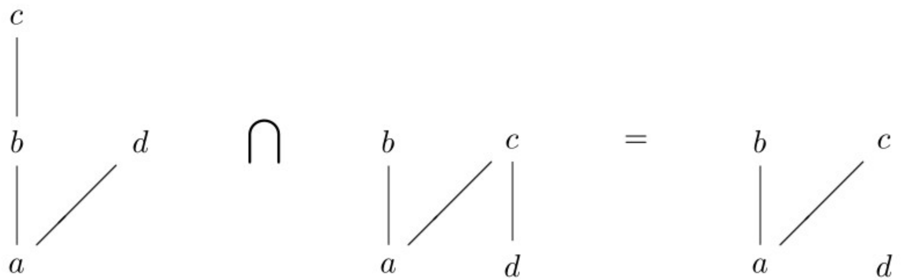


Рис. 5.8. Пересечение ч.у. множеств

Свойства ч.у. множеств могут не сохраняются при пересечении. Например, «быть цепью»: если P — цепь, тогда $P^{\sharp}$ — также цепь, а $P \cap P^{\sharp}$ — тривиально упорядоченное множество.

Прямая сумма. $\mathcal{P} = \langle\, P, \leqslant_P \rangle$ и $\mathcal{Q} = \langle\, Q, \leqslant_Q \rangle$ — два ч.у. множества, причём $P \cap Q = \varnothing$.

$$\mathcal{P} + \mathcal{Q} \ = \ \langle\, P \cup Q, \ \leqslant_P \vee \leqslant_Q \rangle.$$

Справедливы соотношения

$$P + Q \cong P + R \Rightarrow Q \cong R; \quad (P+Q)^\sharp \cong P^\sharp + R^\sharp.$$

$n\mathcal{P}$ — прямая сумма n экземпляров $\mathcal{P}$,
$n\mathbf{1}$ — n-элементная антицепь.

Диаграмма прямой суммы состоит из двух диаграмм соответствующих ч.у. множеств, рассматриваемых как единая диаграмма.

Ч.у. множество, не являющееся прямой суммой некоторых двух других ч.у. множеств, называется *связным*.

<u>*Прямое произведение.*</u> *Прямым* или *декартовым произведением* ч.у. множеств $\mathcal{P} = \langle\, P, \leqslant_P \rangle$ и $\mathcal{Q} = \langle\, Q, \leqslant_Q \rangle$ называется множество

$$\mathcal{P} \times \mathcal{Q} = \langle\, P \times Q, \leqslant \rangle,$$

$$\text{где } (p,\, q) \leqslant (p',\, q') \Leftrightarrow (p \leqslant_P p')\&(q \leqslant_Q q').$$

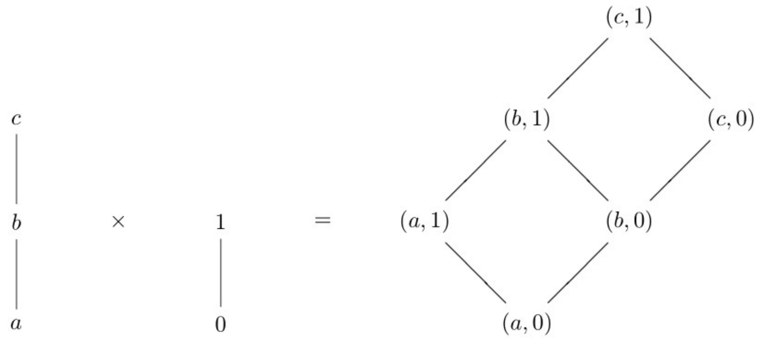


Рис. 5.9. Прямое произведение цепей **3** и **2**

$\mathcal{P}^n$ — прямое произведение n экземпляров $\mathcal{P}$: $B^n = \mathbf{2}^n$.

Если P, Q ранжированы и их ранговые функции суть ρ_P и ρ_Q, то $P \times Q$ также ранжировано и $\rho(x_1,\, x_2) = \rho_P(x_1) + \rho_Q(x_2)$;

Справедливы соотношения $P \times Q \cong Q \times P$

$$P \times R \cong Q \times R \;\Rightarrow\; P \cong Q\,, \quad P^n \cong Q^n \;\Rightarrow\; P \cong Q.$$

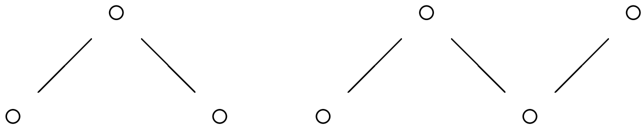


Рис. 5.10. Зигзаги (или заборы) $\mathbf{Z}_3$ и $\mathbf{Z}_4$

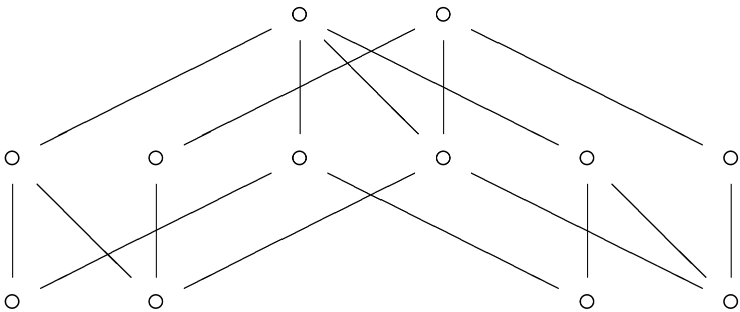
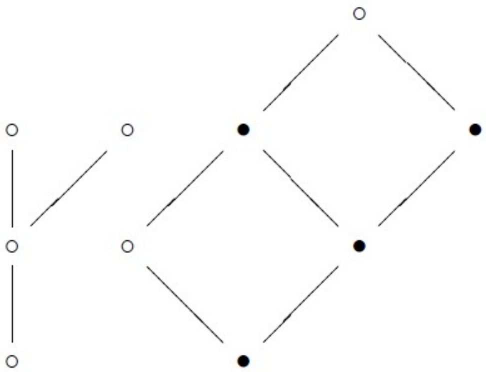


Рис. 5.11. Прямое произведение $\mathbf{Z}_3 \times \mathbf{Z}_4$

Теорема 5.1 (Оре). *Каждый частичный порядок изоморфен некоторому подмножеству декартова произведения цепей.*

Определение 5.7. *Мультипликативной размерностью* ч.у. множества $\mathcal{P}$ называется наименьшее число k линейных порядков $\mathbf{L}_i$ таких, существует вложение $\mathcal{P} \hookrightarrow \mathbf{L}_1 \times \ldots \times \mathbf{L}_k$.



5.3 Линеаризация

Принцип продолжения порядка

Теорема 5.2 (Шпильрайна-Дашника-Миллера).

1. *Любой частичный порядок может быть продолжен до линейного на том же множестве.*
2. *Каждый порядок есть пересечение всех своих линейных продолжений (линеаризаций).*

$$\mathcal{P} \to \mathbf{L_i}, \qquad \mathcal{P} = \mathbf{L}_1 \cap \ldots \cap \mathbf{L}_{e(\mathcal{P})},$$

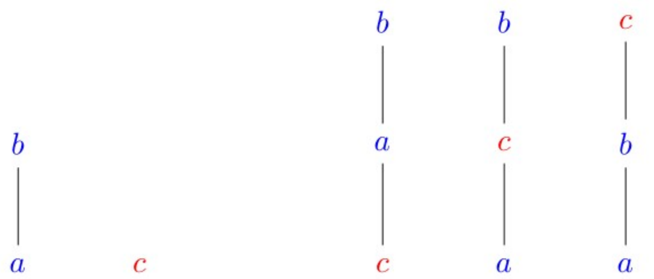
где $e(\mathcal{P})$ — число всех линеаризаций ч.у. множества $\mathcal{P}$.

для конечного случая, $|P| = n$ Если $\mathcal{P}$ — не цепь, то в P найдутся несравнимые элементы; произвольно определим порядок на них и продолжим его по транзитивности. Если получившиеся ч.у. множество ещё не цепь, то выберем новую пару несравнимых элементов и поступаем, как указано выше. Через конечное число шагов получаем линейный порядок.

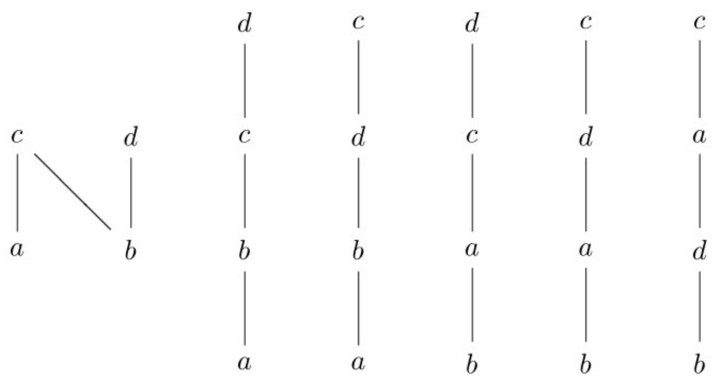
Т.к. возможен различный выбор пар несравнимых элементов и при каждом выборе можно полагать любой их порядок, то можно получить все возможные линейные продолжения исходного частичного порядка.

Пересечение всех таких цепей даст исходное ч.у. множество: если $x \leqslant y$, то аналогичное следование будет и во всех полученных линейных порядках, а при $x \nsim y$ всегда найдётся пара цепей с противоположным их следованием, что в пересечении цепей и даст несравнимость этих элементов. $\square$

Линейные продолжения ч.у. множеств: примеры...



$\mathbf{P}$ $\qquad$ $e(\mathbf{P}) = 3$



$\mathbf{P}$ $\qquad$ $e(\mathbf{P}) = 5$

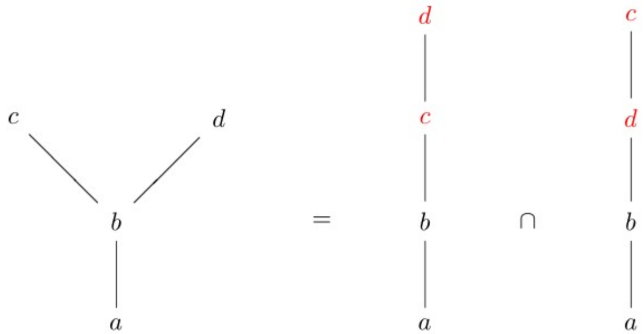


Рис. 5.12. Представление ч.у. множества пересечением цепей

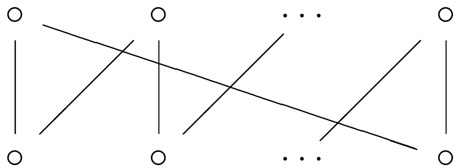


Рис. 5.13. Малая корона $\mathbf{s}_n$

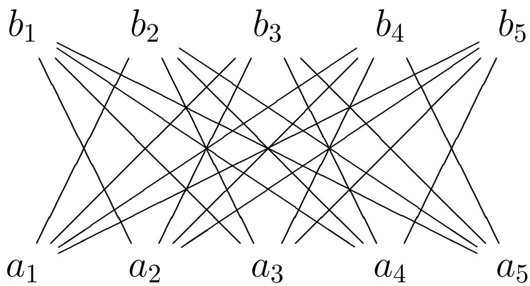


Рис. 5.14. Корона $\mathbf{S}_5$

«$e(\mathcal{P})=?$» — NP-полная задача, но:

- $e(\mathbf{2}\times\mathbf{n}) = \dfrac{1}{n+1}C_{2n}^{n}$ — *числа Каталана*;

- Для зигзагов справедливо представление
$$\sum_{n\geqslant 0} \frac{e(\mathbf{Z}_n)\, x^n}{n!} \;=\; \operatorname{tg} x \,+\, \sec x\,,$$
значения $\mathbf{Z}_n$ при чётных n — *числа секанса*, а при нечётных — *числа тангенса*;
- $e(\mathbf{S}_n) \;=\; (n+1)!(n-1)!\,;$
- $$\sum_{n\geqslant 1} \frac{e(\mathbf{s}_n)}{n!}\, x^n \;=\; \frac{x}{\cos^2 x}\,;$$
- $$\frac{\log(e(B^n))}{2^n} \;=\; \log \binom{n}{\lfloor n/2 \rfloor} - \frac{3}{2} \log e + o(1)\,.$$

Вероятностное пространство на линеарезациях При дискретных задач часто рассматривают связанное с ч.у. множеством P *вероятностное пространство* на множестве всех $e(P)$ его линеаризаций, в котором каждая линеаризация *равновероятна.*

В этом пространстве для элементов x, y, z, … ч.у. множества P рассматривают события E вида $x \leqslant y$, $(x \leqslant y)\,\&\,(x \leqslant z)$ и т.д.

Вероятность $\Pr[E]$ такого события:

$$\Pr[E] \;=\; \frac{\text{число линеаризаций, в которых имеет место } E}{e(\mathcal{P})}.$$

Теорема 5.3 (*XYZ-теорема*). *Пусть* $\langle\, P, \leqslant \rangle$ *— ч.у. множество и* x, y, $z \in P$. *Тогда*

$$\Pr[\, x \leqslant y\,] \cdot \Pr[\, x \leqslant z\,] \;\leqslant\; \Pr[\,(x \leqslant y)\,\&\,(x \leqslant z)\,]\,.$$

Проблема сортировки — определить линейный порядок $\mathbf{L}$ с помощью минимального количества вопросов «*верно ли, что* $x < y$ *в* $\mathbf{L}$?».

Обобщение: $\mathbf{L}$ — зафиксированная, но неизвестная линеаризация ч.у. множества $\mathcal{P}$.

Оптимальная процедура поиска $\mathbf{L}$ включает в себя нахождение элементов x и y, для которых $\Pr[\,x < y\,] \approx \frac{1}{2}$.

С.С. Кислицын (1968) высказал «*1/3 – 2/3 предположение*»: "*любое не являющееся цепью ч.у. множество содержит пару несравнимых элементов x и y, для которых*

$$\frac{1}{3} \leqslant \Pr[\,x \leqslant y\,] \leqslant \frac{2}{3}\text{''}.$$

Позднее это утверждение независимо выдвинули американские исследователи М. Фредман и Н. Линал.

Данное предположение до сих пор успешно противостоит всем попыткам его доказать и *представляет собой одну из наиболее интригующих проблем комбинаторной теории ч.у. множеств* (С. Фелснер и У.Т. Троттер).

На сегодняшний день наиболее сильный результат:

$$0,2764 \approx \frac{5-\sqrt{5}}{10} \leqslant \Pr[x \leqslant y] \leqslant \frac{5+\sqrt{5}}{10} \approx 0,7236\,.$$

Ч.у. множества: спектр Определение:

$$Spec\,(\mathcal{P}) = \{\,\Pr[\,a \leqslant b\,] \mid a, b \in P\,\}$$

Ясно, что

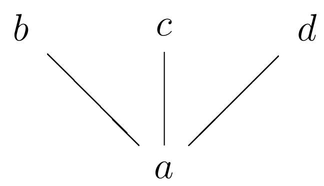
- поскольку $\Pr[\,a \leqslant b\,] = 1 - \Pr[\,b \leqslant a\,]$, спектр симметричен относительно $\frac{1}{2}$;

- для всех неодноэлементных тривиально упорядоченных множеств $Spec = \{ \frac{1}{2} \}$;
- $\{ 0, \frac{1}{2}, 1 \}$ — единственный трёхэлементный спектр;
- все четырёхэлементные спектры должны иметь вид $\{ 0, \alpha, 1-\alpha, 1 \}$, где $0 < \alpha < \frac{1}{2}$;

  Гипотеза (2002): $\alpha = \frac{1}{3}$.

Размерность ч.у. множеств. По теореме Шпильрайна ч.у. множество $\mathcal{P}$ совпадает с пересечением всех $e(\mathcal{P})$ своих линеаризаций, но тот же результат можно получить, взяв значительно меньшее число линейных продолжений.

Например, ч.у. множество $\mathcal{P}$



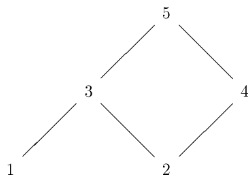
имеет 6 линеаризаций, но $\mathcal{P} = [a, b, c, d] \cap [a, d, c, b]$.

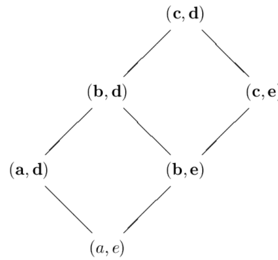
Пусть $\mathcal{P}$ — ч.у. множество и $\mathcal{R} = \{ \mathbf{L}_1, \ldots, \mathbf{L}_k \}$ — совокупность цепей такая, что $\mathcal{P} = \mathbf{L}_1 \cap \ldots \cap \mathbf{L}_k$, то говорят, что $\mathcal{R}$ *реализует* $\mathcal{P}$.

Определение 5.8. Наименьшее число линейных порядков, дающих в пересечении данное ч.у. множество $\mathcal{P}$ называется его *(порядковой) размерностью* (символически $\dim(P)$).

Теорема 5.4 (Оре). *Порядковая и мультипликативная размерности ч.у. множества совпадают.*

$[\,1, 2, 3, 4, 5\,] \cap [\,2, 4, 1, 3, 5\,]$:





— $[\,a, b, c\,] \times [\,d, e\,]$

$\dim(\mathcal{P})$ — *более тонкая оценка сложности ч.у. множества, чем* $e(\mathcal{P})$ Размерность ... имеют:

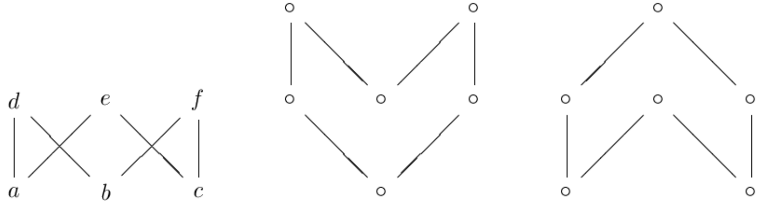
1 — только цепи;

2 — тривиально упорядоченные множества
(т.е. размерность не может интерпретироваться как мера отличия данного ч.у. множества от линейного);

— $\mathbf{Z}_n$;

— все отличные от цепей ч.у. множеств, при $|P| \leqslant 6$, кроме

3 — $\mathbf{s}_3$, $\mathbf{sh}$ и $\mathbf{sh}^{\sharp}$ (см. диаграммы) :



$\mathbf{n}$ — $\mathbf{S}_n$. Стандартный пример показывает, что существуют ч.у. множества сколь угодно большой размерности.

- $\varnothing \neq Q \subseteq P \;\Rightarrow\; \dim(\mathcal{Q}) \leqslant \dim(\mathcal{P})$, при удалении 1-го элемента его размерность уменьшается не более, чем на 1;
- $\dim(\mathcal{P} + \mathcal{Q}) = \max\left\{ \dim(\mathcal{P}), \dim(\mathcal{Q}) \right\}$, если хотя бы одно из множеств не является цепью и $\dim(\mathcal{P}+\mathcal{Q}) = 2$;
- $\dim(\mathcal{P} \times \mathcal{Q}) \leqslant \dim(\mathcal{P}) + \dim(\mathcal{Q})$;
- $\dim(\mathcal{P}) \leqslant |\mathcal{P}|/2$ при $|\mathcal{P}| \geqslant 4$ (теорема Хирагучи).

Теорема 5.5 («компактности»). *Пусть $\mathcal{P}$ — такое ч.у. множество, что любое его конечное ч.у. подмножество имеет размерность, не превосходящую d.*

Тогда $\dim(\mathcal{P}) \leqslant d$.

$$wp1: \;\; \frac{n}{4}\left(1 - \frac{c_1}{\log n}\right) \leqslant \dim(\mathcal{P}) \leqslant \frac{n}{4}\left(1 - \frac{c_2}{\log n}\right), \quad n = |\mathcal{P}|$$

Определение 5.9. Ч.у. множество $\mathcal{P}$ называется *d-несводимым* для некоторого $d \geqslant 2$, если $\dim(\mathcal{P}) = d$ и $\dim(\mathcal{P}') < d$ для любого собственного ч.у. подмножества $P' \subset P$.

d-несводимые множества:
2 — двухэлементная антицепь (единственное);

3 — $\mathbf{s}_3, \mathbf{sh}, \mathbf{sh}^\sharp + \ldots$ — описаны, регулярны и хорошо изучен

4 — достаточно часто встречаются и весьма причудливы;

t — $\mathbf{S}_t$ (единственное $2t$-элементное) $+ \ldots$;

- каждое t-несводимое ч.у. множество является ч.у. подмножеством некоторого $(t+1)$-несводимого.

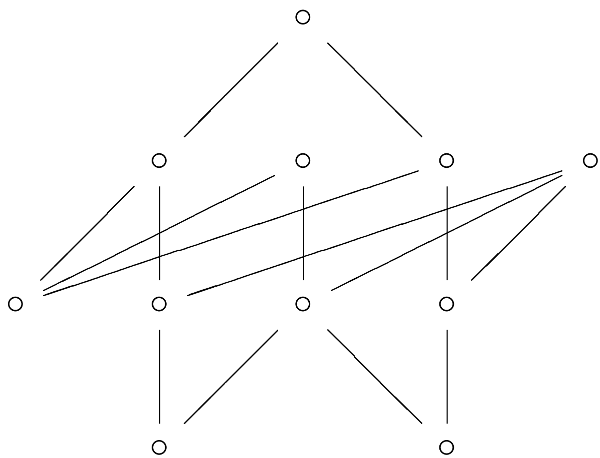


Рис. 5.15. 4-несводимое ч.у. множество

Проблема Ногина. Каково наибольшее значение $\pi(d,n)$ мощности множества максимальных элементов d-несводимого n-элементного ч.у. множества при $d \geqslant 4$?

Данная проблема до сих пор остаётся открытой.

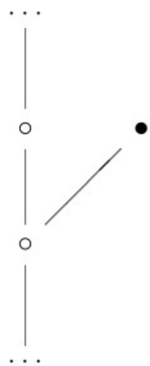
Утверждение 5.1.

$$\pi(d,n) \leqslant n-d\,.$$

5.4 Задачи с решениями

Задача 5.1. *Приведите пример ч.у.м., имеющего в точности один максимальный элемент и не имеющего наибольшего.*

Решение.



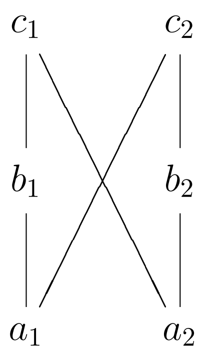
Задача 5.2. *В ч.у. множестве* $\langle\, \mathbb{N}, \,|\, \rangle$ *для подмножества* $A = \{12, 18\}$ *найти*

$$1)\ A^{\triangle}, \quad 2)\ A^{\triangledown}, \quad 3)\ \sup A, \quad 4)\ \inf A.$$

Решение.

1. $A^{\triangle} = \{\, 36n \mid n = 1, 2, \ldots \}$;
2. $A^{\triangledown} = \{\, 1, 2, 3, 6 \,\}$;
3. $\sup A = \text{НОК}\,(12, 18) = 36$;
4. $\inf A = \text{НОД}\,(12, 18) = 6$.

Задача 5.3. *Разложить в пересечение минимального количества цепей ч.у. множество* $\mathcal{P}$



Решение.

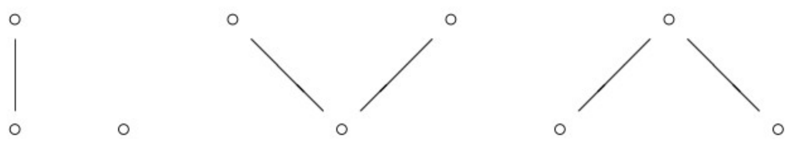
$$\mathcal{P} = [\,a_1,\, b_1,\, a_2,\, c_1,\, b_2,\, c_2\,] \cap [\,a_2,\, b_2,\, a_1,\, c_2,\, b_1,\, c_1\,]\,.$$

Задача 5.4. *1. Сколько существует частичных порядков на множестве* $\{\,a,\, b,\, c\,\}$*?*

2. Сколько среди них неизоморфных?

3. Сколько среди них линейных порядков?

Решение. Неизоморфных трёхэлементных порядков 5: тривиальный, $\mathbf{3}$ и



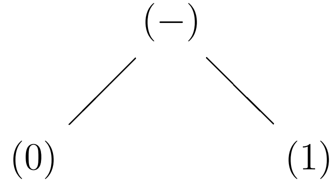
Они порождают порядки на $\{\,a,\, b,\, c\,\}$:

тривиальный	—	1,
цепь $\mathbf{3}$	—	6,
$\mathbf{2+1}$	—	6,
$\mathbf{Z}_3$ и двойственный к нему	—	по 3
Всего	—	19

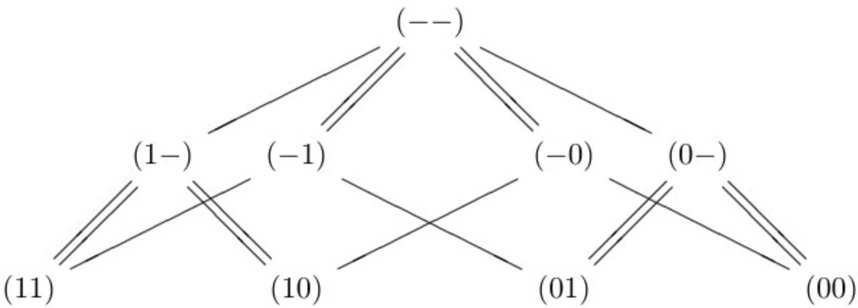
<u>Задача</u> 5.5. *Постройте ч.у. множества $I(1)$ и $I(2)$ всех интервалов булевых единичных кубов размерностей 1 и 2.*

Решение. Булев единичный кубов размерности n содержит 3^n различных интервалов, при этом имеется $C_n^k 2^k$ интервалов размерности k, $k = 0, 1, \ldots, n$.

$I(1)$:



$I(2) = I(1) \times I(1)$
(двойными линиями показаны экземпляры $I(1)$):



5.5 Модели Крипке

Интуиционистское исчисление высказываний ИИВ: формулы. Применение ч.у. множеств в математической логике *модели Крипке* как общего способа установления истинности формул логических исчислений.

Зафиксируем множества

- $Var = \{x, y, \dots\}$ *логических переменных* — символов *атомарных высказываний*;
- $\Phi = \{\neg, \&, \vee, \supset\}$ — *логических связок.*

Определение 5.10. *Формулой над множеством Φ логических связок называется либо некоторая логическая переменная (атомарная формула), либо одно из знакосочетаний вида $(\neg A)$, $(A \,\&\, B)$, $(A \vee B)$ или $(A \supset B)$ (молекулярная формула), где A и B — формулы.*

$\mathcal{A}$ — множество всех логических формул.

Для сокращения записи формул принимают соглашения — правила экономии скобок и приоритета связок: внешние скобки у формул опускаются и сила связок убывает в порядке, указанном при их введении выше ($>$ — «сильнее»)

$$\neg \;>\; \& \;>\; \vee \;>\; \supset.$$

Каждая логическая переменная может принимать, вообще говоря, счётное множество *истинностных значений* $\{\mathbf{0}, 1, \dots, \}$. Первое значение $\mathbf{0}$ назовём *выделенным.*

Неформально выделенное значение символизирует «истину» (*И*), а остальные — различные ситуации отсутствия истинности: неопределённость высказывания, различные формы его «ложности» (*Л*) и т.д. В классической логике множество истинностных значений сужается до двух: $\{\ ,\ \}$ и выделенное — .

Следующие формулы назовём *схемами аксиом* ИИВ:

1. $A \supset (B \supset A)$;
2. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$;
3. $A \,\&\, B \supset A$;
4. $A \,\&\, B \supset B$;
5. $A \supset (B \supset (A \,\&\, B))$;
6. $A \supset A \vee B$;
7. $B \supset A \vee B$;
8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
9. $\neg A \supset (A \supset B)$;
10. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$.

Аксиомы ИВВ получаются при подстановке в схемы конкретных формул вместо *метасимволов* A, B и C.

В ИИВ имеется единственное правило вывода, обозначаемое *MP* (лат. *modus ponens*, правило отделения(?) размещения), позволяющее из формул A и $A \supset B$ получить формулу B:

$$A,\ A \supset B \vdash B$$

Формула A называется *выводимой*, если найдётся конечная последовательность формул $A_1, \ldots, A_l$ такая, что $A_l = A$ и каждый элемент последовательности

- либо является аксиомой,
- либо получен по правилу *MP* из каких-то двух предыдущих формул.

Выводимость формулы A записывается как $\vdash A$, в случае отсутствия вывода пишут $\nvdash A$.

Пример 5.5 (пример вывода формулы в ИИВ). Приведём вывод формулы $x \vee y \supset y \vee x$.

Для удобства формулы вывода будем писать друг под другом, нумеруя их и давая краткие комментарии по их получению.

(1) $x \supset y \vee x$ — подстановка в схему 7

(2) $y \supset y \vee x$ — подстановка в схему 6

(3) $(x \supset y \vee x) \supset ((y \supset y \vee x) \supset (x \vee y \supset y \vee x))$ — подстановка в аксиому 8: $A \mapsto x$, $B \mapsto y$, $C \mapsto y \vee x$

(4) $(y \supset y \vee x) \supset (x \vee y \supset y \vee x)$ — по MP из (1) и (3)

(5) $x \vee y \supset y \vee x$ — по MP из (2) и (4)

Напоминание: 6. $A \supset A \vee B$; 7. $B \supset A \vee B$; 8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$.

Пусть Γ — конечное множество формул. Формула B называется *выводимой из множества формул* Γ (символически $\Gamma \vdash B$), если найдётся конечная последовательность формул $B_1, \ldots, B_l$ такая, что $B_l = B$ и каждый элемент этой последовательности

- либо является аксиомой,
- либо принадлежит Γ,
- либо получен по правилу MP из каких-то двух предыдущих формул.

Факт выводимости $\Gamma \vdash B$ не изменится, если вместо множества Γ взять конъюнкцию составляющих его формул, так что можно рассматривать только одноэлементные множества Γ и опуская фигурные скобки, писать $A \vdash B$.

Знак $\vdash$ является символом отношения предпорядка на множестве $\mathcal{A}$.

Проблема выводимости — одна из важнейших проблем любого логического исчисления L: «выводима ли в L данная формула?».

$\vdash A$ — можно либо предъявить соответствующий вывод, либо доказать его существование;

$\nvdash A$ — возможно лишь дать доказательство несуществования вывода A.

Метатеория — теория, изучающая язык, структуру и свойства некоторой другой (*предметной*, или *объектной*) теории:

- корректность,
- непротиворечивость,
- различные виды полноты,
- проблема разрешимости,
- независимость систем аксиом и правил вывода
- …

Классическое исчисление высказываний КИВ: определение Если к схемам аксиом добавить ещё одну:

11. $A \vee \neg A$ — логический закон *TND* (лат. *tertium non datur*, «третьего не дано»),

то получим *классическое исчисление высказываний КИВ*.

Тогда каждой логической переменной можно приписать одно из двух истинностных значений $\mathbf{1}$ или $\mathbf{0}$, понимаемых как «истина» и «ложь» соответственно, и по правилам

$$|\neg A| = \mathbf{1} \;\Leftrightarrow\; |A| = \mathbf{0};$$

$$|A \mathbin{\&} B| = \mathbf{1} \;\Leftrightarrow\; |A| = |B| = \mathbf{1};$$

$$|A \vee B| = \mathbf{0} \;\Leftrightarrow\; |A| = |B| = \mathbf{0};$$

$$|A \supset B| = \mathbf{1} \;\Leftrightarrow\; |B| = \mathbf{1} \text{ или } |A| = \mathbf{0}.$$

получить оценку $|F| \in \{\mathbf{1}, \mathbf{0}\}$ любой формулы F.

Формулы, истинные при любых *интерпретациях* — возможных вариантах приписываний логическим переменным значений ($\mathbf{1}$ или $\mathbf{0}$) — называются *тавтологиями*.

Примеры тавтологий: все аксиомы 1–11, $\neg\neg x \supset x$, $\neg(x \vee y) \supset \neg x \mathbin{\&} \neg y$, ...

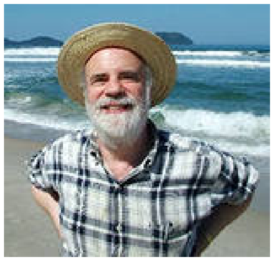
В КИВ выводимыми оказываются все тавтологии и только они $\Rightarrow$ проблема выводимости сводится к проверке формулы на тавтологичность.

В ИИВ задача радикально усложняется: это исчисление не имеет конечнозначной интерпретации, т.е. если в любом конечном наборе $Tr = \{\,\mathbf{0},\, 1,\, \ldots,\, k-1\}$ объявив значение $\mathbf{0}$ выделенным и задав правила оценки формул так, чтобы при всех интерпретациях переменным из Var значений из Tr все аксиомы всегда принимали бы только значение $\mathbf{0}$, найдётся невыводимая

формула ИИВ такая, что её оценка тоже всегда будет принимать выделенное значение.
ИИВ: проблема разрешимости

- Любая выводимая в ИИВ формула выводима и в КИВ.
- Обратное неверно: например, формулы, получаемые из схемы TND и $\neg\neg x \supset x$, $\neg(x \vee y) \supset \neg x \mathbin{\&} \neg y$, ... невыводимы в ИИВ.

Для разрешения проблемы выводимости в ИИВ применим метод, основанный на построении *шкал Крипке.*



Сол Крипке (Saul Aaron Kripke, 1940) — американский философ и логик, один из десяти выдающихся философов последних 200 лет. Ещё юношей внёс значительный вклад в математическую логику, философию математики и теорию множеств.

Шкалы Крипке: построение. Чтобы задать такую шкалу нужно:

- указать ч.у. множество $\langle W, \leqslant \rangle$, элементы носителя которого называют *мирами*;
- для каждого мира указать, какие из логических переменных в нём являются истинными (остальные переменные в этом мире ложны).

Факт истинности переменной x в мире w записывают символически $w \Vdash x$, ложности — $w \nVdash x$.
При формировании шкалы Крипке требуется, чтобы

$$u \leqslant v \text{ и } u \Vdash x \Rightarrow v \Vdash x,$$

т.е., как говорят, «*область истинности переменной наследуется вверх*» или «*сохраняется в бо́льших мирах*».

Неформально порядок $u \leqslant v$ между мирами интерпретируется как то, что *мир v есть состояние мира u в следующий момент времени*, понимая время не в физическом, а в логическом смысле: каждый мир описывается состоянием знаний в данный момент и однажды установленная истинность или доказанный факт остаётся таковым и впоследствии.

Логическое время не обязательно обладает линейным порядком.

Определение 5.11. *Шкала Крипке* есть тройка $\langle W, \leqslant, \Vdash \rangle$, где редукт $\langle W, \leqslant \rangle$ — ч.у. множество, а $\Vdash \subseteq W \times Var$ — соответствие «один ко многим», ставящее каждому миру совокупность истинных в нём логических переменных и удовлетворяющее условию наследования истинности.

Для построенной шкалы Крипке определим истинность данной формулы A в любом мире w:

$w \Vdash A \mathbin{\&} B \;\Leftrightarrow\; w \Vdash A$ и $w \Vdash B$;

$w \Vdash A \vee B \;\Leftrightarrow\; w \Vdash A$ или $w \Vdash B$;

$w \Vdash A \supset B \;\Leftrightarrow\; \forall (u \geqslant w)\ u \Vdash B$ или $u \nVdash A$;

$w \Vdash \neg A \;\Leftrightarrow\; \forall (u \geqslant w)\ u \nVdash A$

(т.е. если $\Vdash \neg A$, то не существует большего мира, в котором бы $\Vdash A$).

Введённые шкалы Крипке задают *семантику* ИИВ, придавая смысл формулам — разделяя их на истинные и ложные в данном мире.

- *Истинная* в данном мире формула остаётся истинной и в *старших* (бо́льших) мирах.
- *Ложная* в данном мире формула была ложной и во всех *младших* (меньших) мирах.
- Если формула содержит только связки $\&$ и $\vee$, то её истинность в данном мире не зависит от её истинности в других мирах.
- Истинности *импликации* и *отрицания* используют порядок на множестве миров.
- Следствием предыдущего является факт независимости импликации от других связок: в ИИВ, например, формулы $A \supset B$ и $\neg A \vee B$ логически не эквивалентны.

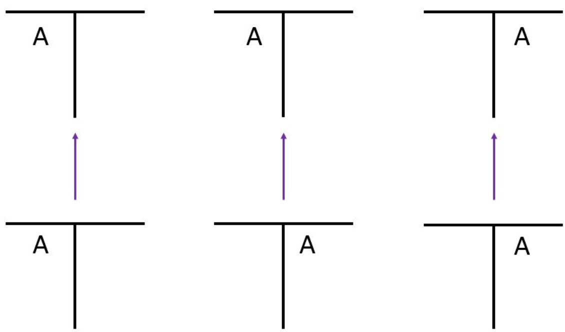


Рис. 5.16. Шкалы Крипке: варианты истинности формулы в шкале из двух миров

Теорема 5.6 (*корректности ИИВ относительно шкал Крипке*). *Формула, выводимая в ИИВ, истина во всех мирах всех шкал Крипке.*

Доказательство. Покажем, что
(1) все аксиомы истины во всех мирах и
(2) правило МР сохраняет истинность.

Второе очевидно: если и A, и $A \supset B$ истины во всех мирах, то B будет также истина во всех мирах.

Замечание: чтобы в мире w проверить оценку

- *истинность* импликации $A \supset B$ надо удостовериться, что $w \Vdash A \Rightarrow w \Vdash B$ ($w \nVdash A$ эта импликация подавно истина);
- *ложность* импликации $A \supset B$ надо удостовериться, что $w \Vdash A \Rightarrow w \nVdash B$. □

Теорема 5.7 (*корректности ИИВ относительно шкал Крипке*). *Формула, выводимая в ИИВ, истина во всех мирах всех шкал Крипке.*

Доказательство. Покажем, что (1) все аксиомы истины во всех мирах и (2) правило МР сохраняет истинность.

Второе очевидно: если и A, и $A \supset B$ истины во всех мирах, то B будет также истина во всех мирах.

Замечание: чтобы в мире w проверить оценку

- *истинность* импликации $A \supset B$ надо удостовериться, что $w \Vdash A \Rightarrow w \Vdash B$ ($w \nVdash A$ эта импликация подавно истина);
- *ложность* импликации $A \supset B$ надо удостовериться, что $w \Vdash A \Rightarrow w \nVdash B$.

Проверим 1-*ю аксиому* $A \supset (B \supset A)$.

Если в некотором мире u имеет место $u \Vdash A$, то во всех мирах $v \geqslant u$ (в том числе и в u) справедливо $v \Vdash B \supset A$.

Проверим 2-*ю аксиому*
$(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.

Пусть существует мир u, где она ложна $\Rightarrow$ в нём должны быть истины формулы $A \supset (B \supset C)$, $A \supset B$ и A, а C — ложна.

Но из $u \Vdash A$ и $u \Vdash A \supset B$ следует $v \vDash B$ во всех мирах $v \geqslant u$. При $u \vDash A \supset (B \supset C)$ это означает справедливость $w \vDash C$ во всех мирах $w \geqslant v$. Отсюда следует справедливость $u \vDash C$ — противоречие.

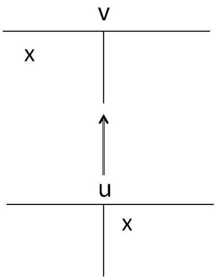
Остальные аксиомы проверяются аналогично. $\square$

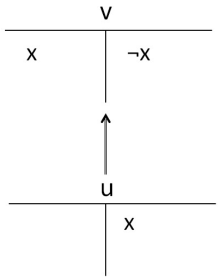
Следствие. *Для доказательства невыводимости формулы в ИИВ достаточно указать шкалу Крипке, в одном из миров которой она ложна.*

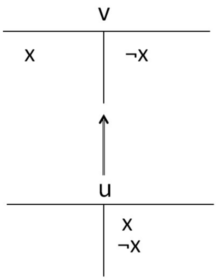
Такая шкала называется *контрмоделью* для данной формулы. Существует контрмодель, являющаяся корневым деревом, в которой мир с ложной формулой — его корнем.

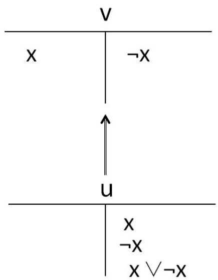
Пример 5.6. 1. Постоим шкалу Крипке, содержащую мир, в котором формула $x \vee \neg x$ ложна.

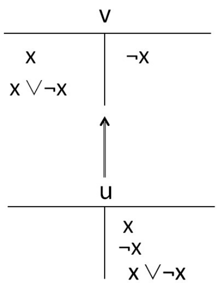
Возьмём два мира u и v такие, что $u \leqslant v$, $u \nVdash x$ и $v \Vdash x$. Тогда $v \nVdash \neg x$, откуда $u \nVdash \neg x$, что, в свою очередь даёт $u \nVdash x \vee \neg x$ (но $v \Vdash x \vee \neg x$).











2. Постоим шкалу Крипке, содержащую мир, в котором формула $\neg x \vee \neg\neg x$ ложна.

Пусть в мире u данная формула ложна, т.е. $u \nVdash \neg x \vee \neg\neg x$. Тогда $u \nVdash \neg x$ и $u \nVdash \neg\neg x$.

Построим два несравнимых между собой мира v и w, бо́льшие u, в которых:

- $v \nVdash \neg x$ и $v \Vdash \neg\neg x$;

- $w \not\Vdash \neg\neg\, x$ и $w \Vdash \neg\neg\, x$.

Искомая контрмодель получена:

- правила истинности и ложности формул в модели соблюдены;
- формула x будет истинна только в мире v.

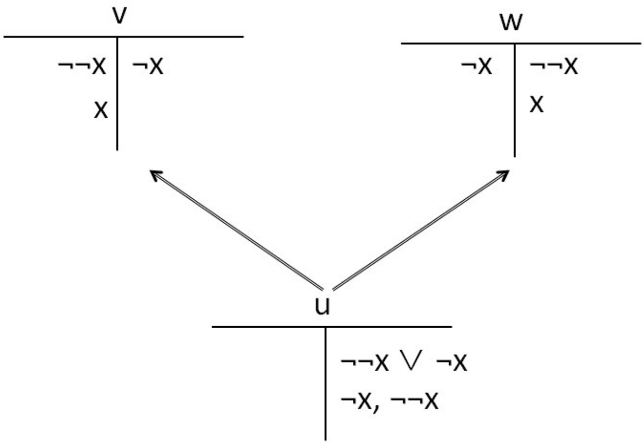


Рис. 5.17. Контрмодель для $\neg\, x \vee \neg\neg\, x$

Шкалы Крипке: применение

- Метод автоматической верификации параллельных вычислительных систем (англ. *model checking*), позволяет проверить, удовлетворяет ли заданная модель системы формальным спецификациям. В качестве модели обычно используют шкалы Крипке, а для спецификации аппаратного и программного обеспечения — *темпоральную* (временную) логику.

- *Модальные логики* формализуют *сильные* и *слабые модальные* выражения вида «необходимо/возможно», «всегда/иногда», «здесь/где-то» и т.д. Заменив в определении шкалы Крипке частичный порядок на

  – отношение толерантности — получим семантику для брауэровой логики B;

  – аморфное отношение — семантику для логики $S5$;

  – диагональное — модель для модальной логики M.