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*

2016

Глава 1

Группы, кольца, поля

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 $y = x^{-1}$.

Группы G со свойством $x \circ y = y \circ x$ называются *коммутативными* или *абелевыми*.

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:

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

Примеры 1.1.

1. *Числовые группы* — все они абелевы:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно *сложения*. Для них используют *аддитивную запись* $x + y$, единичный элемент называют *нулем* (0), обратный к x — *противоположным* $(-x)$.
- *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. 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:

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

в перестановке π — m циклов.

Циклы длины 1 = 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:

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

Симметрическая группа S_n при $n > 1$ порождается транспозициями $(1,2), (1,3), \ldots, (1,n)$.

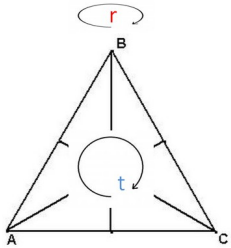
4. *Группы симметрии (самосовмещений) объекта — совокупность преобразований, совмещающих объект с самим собой.*

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

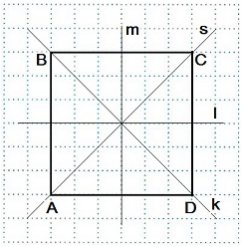
$$D_3 = \langle t, r \rangle = \{ e, (ABC), (ACB), (A)(BC), (B)(AC), (C)(AB) \} = S_3.$$



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

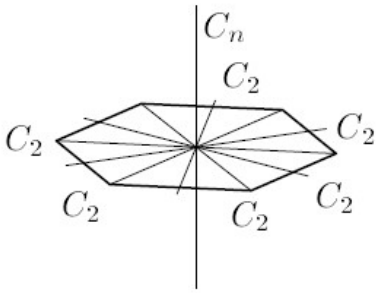


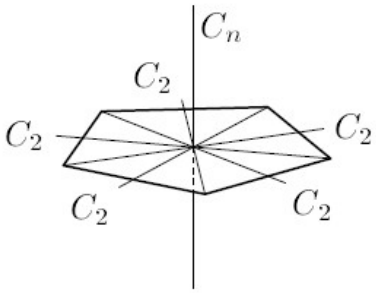
$D_4 = \langle t, r, f \rangle = \{ e, (ABCD), (AC)(BD), (ADCB), (AD)(BC), (AB)(CD), (BD), (AC) \}$.

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.

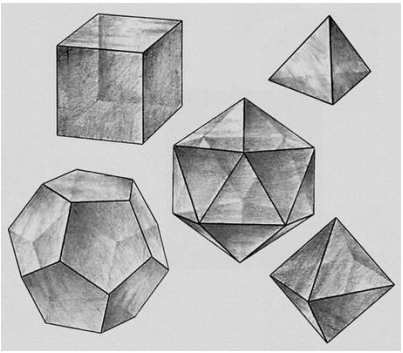




$|D_n| = 2n$: тождественная перестановка + $(n-1)$ поворотов вокруг оси C_n + n отражений вокруг осей C_2.

4.2. Группы *вращений* правильного многогранника — это не все симметрии многогранника, а только повороты, 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 $H \leqslant G$.

Определение левого и правого *смежные классы по подгруппе* H *(с представителем* x*)* соответственно:

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

при этом

$$h_1 \neq h_2,\ h_1, h_2 \in H \leqslant G \ni x \ \Rightarrow\ xh_1 \neq xh_2.$$

Утверждение 1.1. *Смежные классы с разными представителями либо не пересекаются, либо совпадают.*

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

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

Определение 1.2. Для групп $\langle\, G, *\,\rangle$ и $\langle\, G', \circ\,\rangle$ отображение $\varphi : G \to G'$ называется *изоморфизмом*, если оно

1) взаимно однозначно;
2) сохраняет операцию:

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

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

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

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

Если в определении изоморфизма снять требование биективности φ, то получим определение *гомоморфизма групп.*

Например, всегда существует гомоморфизм произвольной группы в единичную E.

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

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

Для циклических групп возможны два случая.

1. Все степени порождающего элемента различны — группа состоит из элементов $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$, т.е. она изоморфна группе $\langle\, \mathbb{Z}, + \,\rangle$ целых чисел по сложению.

   Это — единственная бесконечная циклическая группа.

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;
- изоморфность любой конечной циклической группы с числом элементов n группе
$$\mathbb{Z}_n = \langle \{0, 1, \ldots, n-1\}, +_{\mathrm{mod}\, n} \rangle .$$

Свойства циклических групп:

- Все циклические группы *абелевы*.
- 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.

  Например:
  $H = \{ \ldots -6, -3, 0, 3, 6, \ldots \} = 3\mathbb{Z}$.
- Всякая циклическая группа является гомоморфным образом группы $\mathbb{Z}$.

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

Определение 1.3. Значение *функции Эйлера* $\varphi(n)$ — количество чисел из интервала $[1, \ldots, n-1]$, взаимно простых с n.

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

Свойства (p — простое число):

- $\varphi(p) = p - 1$;
- $\varphi(n^k) = n^{k-1}\varphi(n)$, 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 $\varphi(\cdot)$

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

В группе $\mathbb{Z}_6 = \langle \{0, 1, 2, 3, 4, 5\}, +_6 \rangle$ — $\varphi(6) = 2$ генератора.

сколько генераторов в $\mathbb{Z}$?

Ответ: два — 1 и -1.

Конкретный *Пример* циклической группы: группа $\left\langle \frac{2\pi}{n} \right\rangle$ вращений в плоскости вокруг центра правильного n-угольника, совмещающих его с собой.

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 1.4. 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*

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

Обычно рассматривают *ассоциативные кольца* с ассоциативной операцией умножения:

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

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

Тривиальное кольцо — $\{0\}$; в нём и только в нём $0 = 1$.

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

$$\forall\, r_1, r_2 \in R : (r_1 \cdot r_2 = 0) \;\Rightarrow\; (r_1 = 0) \vee (r_2 = 0).$$

Важное для нас

Определение 1.5. *Целостным кольцом* называют нетривиальное унитальное ассоциативно-коммутативное кольцо без делителей нуля.

Примеры 1.2.

1. Кольцо целых чисел $\mathbb{Z}$ с обычными операциями сложение и умножение на нём — целостное; обратимые элементы в нём — ± 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 $\mod n$.

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

Определение 1.6. 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 1.7. Подмножество S кольца $\langle R, +, \cdot, 0 \rangle$ называется его *подкольцом*, если $a - b \in S$ (ясно, что тогда и $0 \in S$) и $a \cdot b \in S$ для всех $a, b \in S$.

Подкольцо *собственное*, если $S \neq R$.

Кстати, термин «*собственный*» не что иное, как неудачный перевод слова «*proper*», следовало бы говорить «*правильный*» или «*настоящий*», но это уже исторически сложилось и не исправить...

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 $\mathbb{Z}_8$ — $3 \cdot 3 = 1$, $3 + 3 = 6$. Элемент 3 в первом кольце отличается от элемента 3 во втором, как Вася Петров от Васи Иванова. Это *омонимы* — одинаково звучащие слова с разным смыслом.

Идеалы колец и факторкóльца

Определение 1.8. Подкольцо I коммутативного кольца[1] R называется его *идеалом*, символически $I \lhd R$, если

$$\forall\, i \in I \;\; \forall\, r \in R : \; ri \in I.$$

[1] 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*.

Определение 1.9. Идеал I унитального коммутативного кольца R называется *главным* и *порождённым элементом* $a \in R$, если

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

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

Пример 1.2. $(n) = n\mathbb{Z} \lhd \mathbb{Z}$, $\mathbb{Z}$ — КГИ.

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

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

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

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

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 1.3.

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

Определение 1.10. Идеал I называется *максимальным* в кольце R, если не существует такого идеала I', что $I \subset I' \subset R$.

Пример 1.4. 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 1.11. 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.

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

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

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

Пример 1.5. • *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 $\deg f(x) = n$ многочлена.

Евклидовы кольца — КГИ.

Поле

Определение 1.13. 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.*

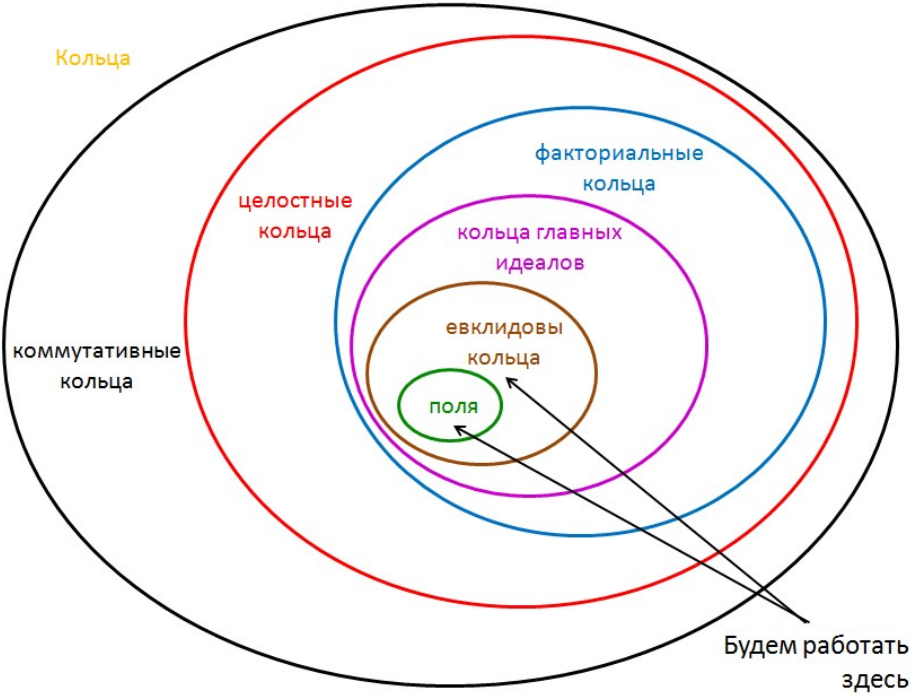


Рис. 1.2. От колец к полям

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 ком- позиции 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.

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

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 $Z_2 : 1 + 1 = 0$, а в Z_5 — $1 + 1 = 2$,
т.е. операция сложения в 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.
- $(p) = \{ np \mid n \in \mathbb{Z} \} = p\mathbb{Z} = \{ 0, \pm p, \pm 2p, \ldots \}$ — *идеал*, порождённый числом p.
- $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z} = \{ \overline{0}, \overline{1}, \ldots, \overline{p-1} \}$ — *кольцо вычетов по модулю этого идеала* = классы остатков от деления на p:

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

Черту над символами классов вычетов часто не ставят.

Поскольку p — простое, то $\mathbb{Z}/(p)$ — не просто 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: поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ и фактор-кольцо $\mathbb{Z}/(4)$ —

$\mathbb{F}_3$:

$+$	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 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 ∞;)).
$\mathbb{Q}$, $\mathbb{R}$ — поля нулевой характеристики.
$\{0, 1, 2, \ldots, \operatorname{char}\Bbbk - 1\}$ — минимальное подполе поля $\Bbbk$.

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

1. $\Bbbk[x]$ — *кольцо многочленов* (от *формальной* переменной x) над полем $\Bbbk$:

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

2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$; 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 $P_1 Q_2 = P_2 Q_1$;

   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 бинома

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

а при $i = 1, \ldots, p-1$ числитель коэффициента $C_p^i = \frac{p!}{i!(p-i)!}$ 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. $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ — *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.

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

Проверяем 3:

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

— т.е. $\operatorname{ord} 3 = 5$ и 3 — не генератор, 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), $p-1 = 10 = 2 \cdot 5$,

$$q \in \left\{ \tfrac{10}{2} = 5,\ \tfrac{10}{5} = 2 \right\}$$

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

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

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

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 $\mathbb{Z}_2[x]$:

$$\begin{array}{l|l} x^4 & x^2+1 \\ \underline{x^4+x^2} & \underline{} \\ \quad x^2 & x^2+1 \\ \quad \underline{x^2+1} & \\ \quad\quad 1 & \end{array} \qquad \text{т.е. } x^4 = (x^2+1)^2 + 1.$$

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:

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

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.

Свойство «неприводимости» зависит от поля: многочлен x^4+1 неприводим в над $\mathbb{Q}[x]$, но приводим над $\mathbb{F}_2[x]$: $\quad x^4 + 1 = (x^3 + x^2 + x + 1) \cdot (x + 1)$.

Вопросы для кольца многочленов над данным полем:

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

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

поле $\mathbb{C}$ — только многочлены 1-й степени;

поле $\mathbb{R}$ — 1) многочлены 1-й степени,

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

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

Далее нас будут интересовать неприводимые (и чаще — нормированные) многочлены в конечных полях.

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

Неприводимые многочлены кольца $\mathbb{F}_2[x]$. 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 $\mathbb{F}_2$: $x^2 + x + 1$.

Третья степень: $x^3 + ax^2 + bx + 1$.
(почему свободный член не равен нулю?)

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 3 решения:

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 разлагаться в произведение двух неприводимых многочленов 2-й степени:

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

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. Для справки: вот они —

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

Неприводимые многочлены из $\mathbb{F}_3[x]$.
Многочлены степени 1:

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

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

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

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

Для всех ли p *и* n *существуют неприводимые многочлены в* $\mathbb{F}_p$*?*

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...)

Зачем нужны неприводимые многочлены?
С помощью неприводимых многочленов 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
$$a(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x],\ a_n \neq 0.$$

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 $r(x)$:
$$\overline{r(x)} = \left\{ f(x) \in \mathbb{F}_p[x] \mid f(x) = a(x)\cdot q(x) + r(x) \right\}.$$

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

Расширения простых полей

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

Доказательство.

1. Кольцо многочленов $\mathbb{F}_p[x]$ евклидово, идеал $(a(x))$ — максимальный $\Rightarrow$ $\left\{ \overline{r(x)} \right\}$ — поле.
2. Его мощность $\left| \left\{ \overline{r(x)} \right\} \right|$ = число многочленов над $\mathbb{F}_p$ степени не выше $n-1$, т.е. p^n.

□

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

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 $\mathbb{F}_p^n$.*

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

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

Это значит, что $x+1$ — примитивный элемент 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). Опередить, 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 $GF(5) = \{0,1,2,3,4\}$:

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

убеждаемся $a(x)$ — неприводимый многочлен (а если бы это был многочлен 4-й степени?).

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

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 k взаимно просто с $p^n - 1$, то α^k — *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.

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:

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

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 $F = \mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_2^3$; 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 $F = \mathbb{F}_2[x]/(x^3 + x + 1)$.
В F $x^3 = x + 1$ и

$$
\begin{aligned}
\alpha &= x^2 + x,\\
\alpha^2 &= x^4 + x^2 = \not{x}^2 + x + \not{x}^2 = x,\\
\alpha^3 &= \alpha \cdot \alpha^2 = x^3 + x^2 = x^2 + x + 1,\\
\alpha^4 &= (\alpha^2)^2 = x^2,\\
\alpha^5 &= \alpha^2\alpha^3 = x^3 + x^2 + x = \not{x} + 1 + x^2 + \not{x} = x^2 + 1,\\
\alpha^6 &= x^4 + x^2 + 1 = x^2 + x + x^2 + 1 = x + 1,\\
\alpha^7 &= x^2(x^2 + x + 1) = x^4 + x^3 + x^2 =\\
&= \not{x}^2 + \not{x} + \not{x} + 1 + \not{x}^2 = 1.
\end{aligned}
$$

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 $F = \mathbb{F}_5[x]/(x^2 + x + 1) \cong \mathbb{F}_5^2$; 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 $F = \mathbb{F}_5[x]/(x^2 + x + 1)$.

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 $a(x) \mid x^m - 1$.

Примеры 2.1. 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 $x^t-1 \;\dot{\not}\; x^3+x+1$ 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.

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

Отсюда:

- пары чисел (a,b) и $(a-kb,b)$ имеет одинаковые общие делители;

- вместо $a - kb$ (для «ускорения») 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 $r_{-2} \geqslant r_{-1} > r_0 > r_1 > \ldots > r_n \geqslant 1$.

Пример 2.5. По алгоритму Евклида найдём 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; открыто за 106 лет до рождения Э. Безу). *Для любых натуральных a, b и $d = НОД\,(a, b)$ найдутся целые коэффициенты Безу x, y такие, что $d = ax + by$.*

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

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

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

Замечание: коэффициенты Безу определены неоднозначно:

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

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

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

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 2.6. 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 2.7. В поле $\mathbb{Z}/(101)$ решить уравнение

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

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

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

для пары многочленов $\big(a(x),\, b(x)\big)$, *может быть найден расширенным алгоритмом Евклида.*

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 2.8. Найдём $(x^2+x+3)^{-1}$ в поле

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

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: $r_{-2}(x) = x^4+x^3+x^2+3$,
$r_{-1}(x) = x^2+x+3$,
$y_{-2}(x) = 0$,
$y_{-1}(x) = 1$ — задание начальных значений.

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

Шаг 2: $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
$q_1(x) = 4x$,
$r_1(x) = 3$, $\deg r_1(x) = 0$
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + 4x(x^2+5) = 4x^3+6x+1$.

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 над 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 2.9. 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 $\Bbbk$.

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 характеристики $p > 0$ есть векторное пространство над $GF(p)$ (p — простое).*

Доказательство. В рассматриваемом поле $GF(q)$, $q \geqslant p$:
сложение — наследуется операция сложения в $GF(q)$;
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 $\mathbb{F}_p$:

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

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

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

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

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

2. Пусть

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

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

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

Например:

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

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

изоморфизм задаётся соответствием

$$\overline{1} \mapsto 1,\ \overline{x} \mapsto i.$$

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

Доказательство. Если поле $\Bbbk_1$ содержится в поле ($\Bbbk_1 \subset \Bbbk_2$), 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.

Докажем далее, что м.м. для каждого элемента β:

1) существует,
2) единственен,
3) неприводим.

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

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

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

Ясно, что

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

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

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

а значит и $a_n^{-1}a(x)$.

С другой —

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

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

Примитивные многочлены

Примеры 2.2.

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. $\square$

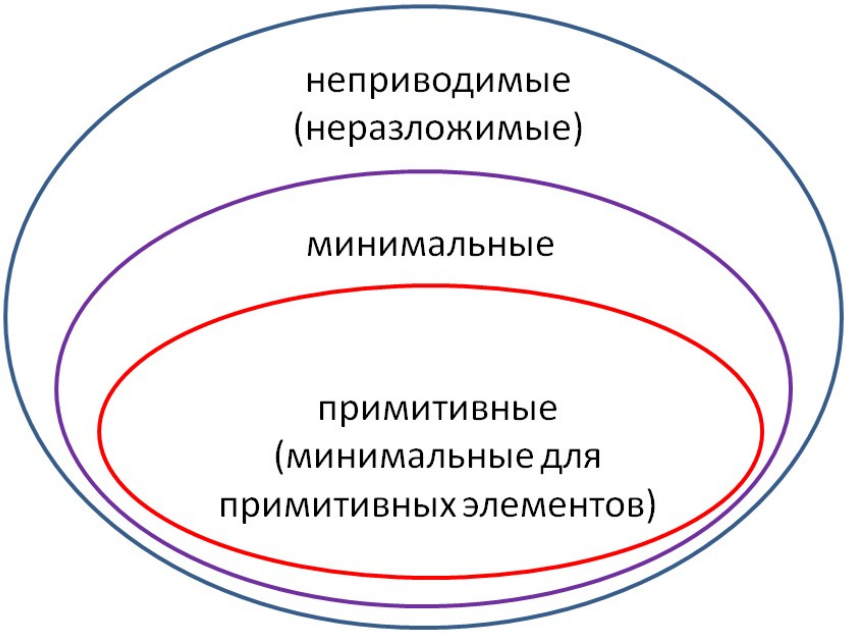


Рис. 2.1. Соотношение множеств неприводимых, минимальных и примитивных многочленов

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

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

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

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

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

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 $\{\beta_1, \ldots, \beta_{p^n-1}\} = F^*$*, 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 2.10. 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!*[1]) 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 $f(x)$.

□

Пример 2.11 (продолжение *Примера* 2.10). Продолжаем разложение $x^{15} + 1 \in \mathbb{F}_2[x]$.

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

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

Имеем

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

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

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

[1] Теорема 2.1

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

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

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

Любой элемент F выражается через базис:

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

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

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

т.е. β — корень уравнения

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

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

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 корень известен: 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 β, β^p, β^{p^2}, …, $\beta^{p^{n-1}}$ 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

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

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

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

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

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

Нахождение корней неприводимого многочлена

Примеры 2.3. 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 $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right)$ он имеет корни x и x^3.

Поскольку $x^2 = -2x + 1 = x + 1$, то

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

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

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

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

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 $n = \text{НОК}\,(n_1, \ldots, n_k)$.

Примеры 2.4. 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[2].

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 $x^3 = -2x - 4 = 3x + 1$:

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

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

Найдём отдельно x^{10}:

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

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 $F = \mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$ (поскольку корень $2 \in F$).

2. Решить уравнение

$$f(x) = x^8 + x^4 + x^2 + x + 1 = 0, \text{ где } f(x) \in \mathbb{F}_2[x].$$

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

Решение. В таблицах неприводимых многочленов данный многочлен отсутствует.

Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над $\mathbb{F}_2$ многочленов:

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

Уравнения $f_1(x)=0$ и $f_2(x)=0$ ранее были решены: их корни соответственно суть

x, x^2, x^3+1, x^3+x^2+x в поле $F_1 = \mathbb{F}_2[x]/\big(x^4+x^3+1\big)$

и

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

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

Степени обоих расширений поля $GF(2)$ совпадают ($=4$) и поля F_1 и F_2 изморфны (*пока не доказано!*), т.о. все 8 корней уравнения $f(x)=0$ лежат в поле $GF(2^4)$.

Для записи данных корней выберем представление F_1 поля $GF(2^4)$. Тогда запись корней $f_1(x)=0$ останется без изменений, а корни $f_2(x)=0$ надо представить как элементы F_1.

Приравнивая многочлены, порождающие данные поля, получим

$$x^4+x^3+1 = x^4+x^3+x^2+x+1 \;\Rightarrow\; x^2+x = x(x+1) = 0.$$

Ясно, что при подстановке $x \mapsto x+1$ полученное равенство останется справедливым. Применим данную постановку для изоморфного преобразования полей $F_1 \leftrightarrow F_2$.

Находим представления корней многочлена $f_2(x)$ в поле F_1:

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

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

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:

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

Отсюда

1) $c = -a$ и коэффициент при x^2 есть $b - a^2 + d = 0$;
2) из $bd = 2$ следует, что либо $b = 1$ и $d = 2$, либо $b = 2$ и $d = 1$, т.е. в любом случае $b + d = 3 = 0$;
3) но тогда из п. (1) $a^2 = 0$, т.е. $a = c = 0$ и коэффициент при x равен $0 \Rightarrow$ противоречие.

Т.о. полином $f(x) = x^4 + 2x + 2 = 0$ над $\mathbb{F}_3$ *неприводим*.

Теперь рассмотрим поле $\mathbb{F}_3[x]/\left(x^4 + 2x + 2\right)$.

В нём $f(x) = x^4 + 2x + 2 = 0$, т.е. $x^4 = x + 1 = 0$, и корни $f(x)$ суть x, x^3, x^{3^2}, x^{3^3}.

Вычислим x^9 и x^{27}:

$$x^9 = \left(x^4\right)^2 x = (x + 1)^2 x = x^3 + 2x^2 + x;$$
$$x^{27} = \left(x^9\right)^3 = (x^3 + 2x^2 + x)^3 = x^9 + 2x^6 + x^3 =$$
$$= (x^3 + 2x^2 + x) + 2x^2x^4 + x^3 =$$
$$= x^3 + 2x^2 + x + 2x^3 + 2x^2 + x^3 =$$
$$= x^3 + x^2 + x.$$

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

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

Ответ: в поле $\mathbb{F}_2[x]/\big(x^5 + x^2 + 1\big)$ уравнение

$$f(x) = x^5 + x^2 + 1 = 0$$

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

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.

$\alpha^4 = \alpha + 1$	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: $(x^3 + x + 1) \cdot (x^2 + x + 1) = ?$

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:
     $$\alpha^7\alpha^{10} = \alpha^{17} = \alpha^2 = x^2.$$

Таким образом: $(x^3+x+1)\cdot(x^2+x+1) = x^2$.

Нахождение минимальных многочленов. Пусть $a(x)$ — нормированный неприводимый многочлен над $\mathbb{F}_p$.

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

- либо $\beta^d = x$, тогда $m_\beta(x) = a(x)$ и $\deg m_\beta(x) = \deg a(x)$;
- либо $\beta^d = \beta$, тогда $m_\beta(x) = (x-\beta)\cdot(x-\beta^p)\cdot\ldots\cdot(x-\beta^{p^{d-1}})$ и $\deg m_\beta(x) = d \leqslant \deg a(x)$.

Пример 2.12. Найдём минимальные многочлены для элементов x^2+x, x и $x+1$ поля

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

В этом поле $x^4 = x+1$.

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

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

Т.о. м.м. $m_\beta(x)$ имеет 2 корня: β и β^2, его степень равна 2 и $m_\beta(x) = x^2+x+1$ — единственный неприводмый многочлен из $\mathbb{F}_2[x]$.

2. $\beta = x$. Вычисляем элементы, сопряжённые с x:

$$x^2,$$
$$x^4 = x + 1,$$
$$x^8 = (x+1)^2 = x^2 + 1$$
$$x^{16} = (x^2+1)^2 = x^4 + 1 = x + \not{1} + \not{1} = x.$$

Т.о. м.м. $m_x(x)$ имеет 4 корня: x, x^2, x^4, x^8, его степень равна 4 и $m_x(x) = x^4 + x + 1$ — порождающий многочлен поля F (x — *примитивной элемент* F, а $x^4 + x + 1$ — *примитивный многочлен*).

3. $\beta = x + 1$. Вычисляем элементы, сопряжённые с β:

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

Т.о. м.м. $m_{x+1}(x)$ также есть порождающий поле F многочлен $x^4 + x + 1$.

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.

□

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):

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

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:

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

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 $n \in \mathbb{N}$:

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

Например:

$\mu(1) = 1$ (по определению), $\mu(6) = 1$,
$\mu(2) = -1$, $\mu(7) = -1$,
$\mu(3) = -1$, $\mu(8) = 0$,
$\mu(4) = 0$, $\mu(9) = 0$,
$\mu(5) = -1$, $\mu(10) = 1$.

Основное свойство функции Мёбиуса:

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

Теорема 2.9 (формула Гаусса).

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

Например:

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

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

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

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, α, α^2, $\ldots$, α^{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 $\deg f$.

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

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:*

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

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.

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

2.

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

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:

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

□

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. □

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 $\overline{x}$:

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

т.к. в этом кольце $x^n = 1$.

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

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

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.

□

Примитивные корни (т.е. 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 многочлен $x^n - 1$. Справедливо:

- В $\mathbb{F}_q$ выполняется равенство $x^{kp} - 1 = (x^k - 1)^p$, поэтому интересен случай, когда n взаимно просто с p: тогда у многочлена $x^n - 1$ кратных корней нет (он взаимно прост со своей производной nx^{n-1}).
- Равенство $x^n = 1$ означает, что $\operatorname{ord} x \mid n$ в циклической группе $\mathbb{F}_q^*$.

Вывод: корни уравнения $x^n - 1 = 0$ 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

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

Примеры 2.5. 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

- Любая конечное целостностное кольцо является полем.
- Характеристика конечного поля — простое число.
- Любое конечное поле характеристики p состоит из $q=p^n$ элементов $n\in\mathbb{N}$.
- $\alpha\in\{GF(q)\setminus 0\}\Rightarrow \operatorname{ord}\alpha \mid q-1$.

- Мультипликативная группа поля $GF(q)$ является циклической: в ней существует $\varphi(q-1)$ примитивных элементов (генераторов, элементов порядка $q-1$).

  Для нахождения самих генераторов 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 корнем. Минимальные многочлены неприводимы и единственны для каждого β.
- Любой элемент поля $F = \mathbb{F}_p^n$ является корнем многочлена $x^{p^n} - x$:
$$x^{p^n} - x = \prod_{a \in F} (x - a).$$
- Для того, чтобы векторное подпространство V кольца $R = \mathbb{F}_p[x]/(x^n - 1)$ было циклическим, необходимо и достаточно, чтобы оно было идеалом R.

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

2.7 Задачи с решениями

Задача 2.1. *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.

$p = 2$: — утверждение тривиально.

$p > 2$: 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 $(*)$, т.е. -1.

Ещё одно Решение. Для $p = 2$ утверждение очевидно.

При $p > 2$ обозначим

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

и заметим, что

$$(p-1)^2 = p^2 - 2p + 1 \equiv_p 1.$$

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

Или, что то же, $(p-1)! \equiv_p -1$.

Задача 2.3. *Построить поле из* 4*-х элементов.*

Решение. Это поле $\mathbb{F}_2^2$, оно может быть построено как фактор-кольцо $\mathbb{F}_2[x]/(a(x))$, где $a(x)$ — неприводимый многочлен из $\mathbb{F}_2[x]$ степени 2.
Но такой многочлен только один: x^2+x+1.
Следовательно, $\mathbb{F}_2^2 = \{0, 1, x, x+1\}$ и $x^2 = x+1$ (черту над элементами не пишем).

Таблицы сложения и умножения в поле:

$+$	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. *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 2.5. *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 2.6. *Перечислить все подполя поля* $GF\left(2^{30}\right)$.

Решение. Поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$ iff $k \mid n$, поэтому подполями $GF\left(2^{30}\right)$ будут поля $GF\left(2\right)$, $GF\left(2^2\right)$, $GF\left(2^5\right)$, $GF\left(2^6\right)$, $GF\left(2^{10}\right)$, $GF\left(2^{15}\right)$ и само поле $GF\left(2^{30}\right)$.

Задача 2.7. *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 2.8. *Многочлен* $f(x) = x^3+2x^2+4x+1 \in \mathbb{F}_5[x]$ *разложить на неприводимые множители.*

Решение.

1. $f(2) = 2^3+2\cdot 2^2+4\cdot 2^2+1 = 25 \equiv_5 0$,

$$(x-2) \equiv_5 (x+3)$$

2.
$$\begin{array}{r|l} x^3+2x^2+4x+1 & x+3 \\ \cline{2-2} x^3+3x^2 & x^2+4x+2 \\ \cline{1-1} \quad 4x^2+4x & \\ \quad 4x^2+2x & \\ \cline{1-1} \quad\quad 2x+1 & \\ \quad\quad 2x+1 & \\ \cline{1-1} \quad\quad\quad 0 & \end{array}$$

3. Перебором убеждаемся, что многочлен x^2+4x+2 неприводим в $\mathbb{F}_5$.

Задача 2.9. *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:
$$x^2 + 1,$$
$$x^2 + x + 2,$$
$$x^2 + 2x + 2.$$
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 2.10. *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 2.11. *Разложить на неприводимые множители все нормированные многочлены* 3*-й степени из* $\mathbb{F}_2[x]$.

Решение. Вычисляя значения многочленов при $x = 0, 1$, приходим к выводу, что

$$
\begin{aligned}
f_1(x) &= x^3 = x \cdot x \cdot x,\\
f_2(x) &= x^3 + 1 = (x+1)(x^2+x+1),\\
f_3(x) &= x^3 + x = x(x+1)^2,\\
f_4(x) &= x^3 + x^2 = x^2(x+1),\\
f_5(x) &= x^3 + x + 1 \text{ — неприводим},\\
f_6(x) &= x^3 + x^2 + 1 \text{ — неприводим},\\
f_7(x) &= x^3 + x^2 + x = x(x^2+x+1),\\
f_8(x) &= x^3 + x^2 + x + 1 = (x+1)^3.
\end{aligned}
$$

Задача 2.12. *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:

$$
\begin{aligned}
f_1(x) &= x^2 + 1,\\
f_2(x) &= x^2 + x + 2,\\
f_3(x) &= x^2 + 2x + 2.
\end{aligned}
$$

Задача 2.13. *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 2.14. *1. Проверить, что*

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

является полем.

2. Выразить обратный к $1 - x$ *в* F.

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

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

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

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

Ответ: $(1 - x)^{-1} = x + 2$ в F.

Задача 2.15. *Найти порядок элемента* $\beta = x + x^2$ *в мультипликативной группе*

1. *поля* $F_1 = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$;
2. *поля* $F_2 = \mathbb{F}_2[x]/\big(x^4 + x^3 + 1\big)$.

Решение. $\beta = x + x^2 = x(x+1)$.
Мультипликативная группа указанных полей состоит из $2^4 - 1 = 15$ элементов.
Примарное разложение 15: $15 = 3 \cdot 5$, поэтому равенство $\beta^d = 1$ нужно проверить для $d = \frac{15}{5} = 3$ и $d = \frac{15}{3} = 5$.

1. $x^4 = x + 1$

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

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

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

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

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

Задача 2.16. *Найти количество нормированных неприводимых многочленов*

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

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

1. ((7)) над $\mathbb{F}_2$

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

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

2. ((6)) над $\mathbb{F}_5$

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

$$\left. + \mu(3)5^2 + \mu(6)5 \right] = \frac{1}{6} \left[15625 - 125 - 25 + 5 \right] = 2\,580.$$

Задача 2.17. *Для поля* $F = \mathbb{F}_3[x]/\left(-2x^2 + x + 2\right)$ *построить таблицу соответствий между полиномиальным и степенным представлением его ненулевых элементов.*

С помощью данной таблицы вычислить выражение
$$S = \frac{1}{2x+1} - \frac{2(2x)^7}{(x)^9(x+2)}.$$

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

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

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

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

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

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

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 генератор F пришлось бы искать.

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

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

Задача 2.18. *Для поля* $F = \mathbb{F}_3[x]/(x^2+1) \cong \mathbb{F}_3^2$ *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 $x+1$:

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

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

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

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 2.19. *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?

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

Поэтому искомый идеал составят элементы кольца (многочлены степени не выше 3), кратные $f(x)$:

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

Проведём умножение:

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

2. 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 $f(x) = x^2+x+2 \not| x^4+1 = a(x)$?
Тогда кратные $f(x)$ составят в R идеал $(\text{НОД}(f(x),a(x)))$.

Задача 2.20. *В поле* $F = \mathbb{F}_7[x]/\left(x^4+x^3+x^2+3\right)$ *найти элемент, обратный к* x^2+x+3.

Решение. Обратный элемент к $b = x^2+x+3$ находим, решая уравнение

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

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

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

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$
// Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком
$q_0(x) = x^2+5,$
$r_0(x) = 2x+2,$
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) =$
$= -q_0(x) = -x^2-5.$

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x),$
// Делим $r_{-1}(x)$ на $r_0(x)$ с остатком
$q_1(x) = 4x,$
$r_1(x) = 3,$
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) =$
$= 1 + 4x(x^2+5) =$
$= 4x^3+6x+1.$

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 2.21. *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

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

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

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

$$= 3x^2 + 3x + 2 = 3(2x + 2) + 3x + 2 = 4x + 3.$$

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

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

с помощью расширенного алгоритма Евклида:

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

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,
// Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком
$q_0(x) = 4x + 4$,
$r_0(x) = 1$,
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) =$
$= -4x - 4 = x + 1$.

3. Вычислим обратную матрицу

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

Проверка:

$$\begin{pmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{pmatrix} \times \begin{pmatrix} x + 3 & 1 \\ 4x & 3x \end{pmatrix} =$$

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

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

$$= \begin{pmatrix} 2(2x+2)+x+2 & 3(2x+2)+4x+4 \\ 3(2x+2)+4x+4 & 4(2x+2)+2x+3 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Задача 2.22. *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

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

Делим частное $g(x)$ на x^2+x+1:

$$g(x) = x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = \\ = (x^2+x+1)(x^7+x^4+x^3+x^2+x+1)+x,$$

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:

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

— делится!

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

$$x^6+x^5+x^3+x^2+1 = \\ =(x^3+x+1)\cdot(x^3+x^2+x+1)+x^2, \\ x^6+x^5+x^3+x^2+1 = (x^3+x^2+1)\cdot x^3+x^2+1.$$

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 2.23. *Найти поле характеристики* 3, *в котором многочлен* $f(x) = x^3+x+2 \in \mathbb{F}_3[x]$ *раскладывается на линейные множители.*

В данном поле найти все корни данного многочлена.

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

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

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

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

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

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

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

Построенное поле $\mathbb{F}_3[x]/\left(x^2+2x+2\right)$ — 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 $\mathbb{F}_3[x]/\left(x^2+2x+2\right)$ 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 $\mathbb{F}_3[x]/\left(x^2+2x+2\right) = GF(3^2)$.

Задача 2.24. *Найти м.м. для всех элементов β поля* $\mathbb{F}_2/\left(x^4+x+1\right)$.

Решение.

$\beta = 0$: $m_0(x) = x$.

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

$\beta = \alpha$: сопряжённые с α элементы — α^2, α^4, α^8 и

$$m_\alpha(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) = \\ = x^4 + x + 1.$$

$\beta = \alpha^3$: сопряжённые с α^3 элементы суть α^6, α^{12}, $\alpha^{24} = \alpha^9$, их м.м. —

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = \\ = x^4 + \left(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\right)x^3 + \\ + \left(\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\right.$$

$$+\alpha^9\alpha^{12}\big)\,x^2+\big(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12}\big)\,x+$$
$$+\big(\alpha^3\alpha^6\alpha^9\alpha^{12}\big) \;=\; x^4+\big(\alpha^3+(\alpha^3+\alpha^2)+(\alpha^3+\alpha)+$$
$$+\,(\alpha^3+\alpha^2+\alpha+1)\big)\,x^3+(\ldots)\,x^2+(\ldots)\,x+\alpha^{30} \;=$$
$$=\; x^4+x^3+x^2+x+1.$$

$\beta=\alpha^5$: единственный сопряжённый с α^5 элемент — α^{10} (т.к. $\alpha^{20}=\alpha^5$), их м.м. —

$$m_{\alpha^5}(x) \;=\; (x-\alpha^5)(x-\alpha^{10}) \;=\; x^2+x+1.$$

$\beta=\alpha^7$: сопряжённые с α^7 элементы — α^{14}, $\alpha^{28}=\alpha^{13}$, $\alpha^{56}=\alpha^{11}$, их м.м. —

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

Задача 2.25. *Найти минимальный многочлен* $m(x)\in\mathbb{F}_5[x]$, *который имеет корень* α^3, *где* α — *примитивный элемент поля*

$$F \;=\; \mathbb{F}_5[x]/\big(x^2+x+2\big).$$

Решение.

1. Известно, что минимальный многочлен $m(x)$ 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 будет $\alpha^{5^2-1}=\alpha^{24}=1 \;\Rightarrow$ сопряжённым с α^3 будет только элемент α^{15} (т.к. $\alpha^{75}=\alpha^{24\cdot3+3}=\alpha^3$). Поэтому минимальный многочлен

$m(x)$ имеет степень 2 класс, образованный α^3 содержит только два элемента α^3 и α^{15}:

$$m(x) = (x-\alpha^3)(x-\alpha^{15}) = x^2 - (\alpha^3+\alpha^{15})x + \alpha^{18}.$$

3. Найдём коэффициенты многочлена $m(x)$ учётом $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
\alpha^3 &= \alpha\cdot\alpha^2 = \alpha(4\alpha+3) = 4\alpha^2+3\alpha = \\
&= 4(4\alpha+3)+3\alpha = 4\alpha+2, \\
\alpha^{15} &= (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5+2 = \\
&= 4\alpha^2\alpha^3+2 = 4(4\alpha+3)(4\alpha+2)+2 = \\
&= 4(\alpha^2+1)+2 = 4(4\alpha+4)+2 = \alpha+3, \\
\alpha^3+\alpha^{15} &= 4\alpha+2+\alpha+3 = 0, \\
\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = \\
&= 4(4\alpha+3)+4\alpha+1 = 3.
\end{aligned}$$

Ответ: $m(x) = x^2+3$.

Задание: убедитесь, что x — примитивный элемент поля F.

Задача 2.26. *Найти корни многочлена*

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

Решение. Вычисляем значения $f(x)$ для $x \in GF(5) = \{0, 1, 2, 3, 4\}$:

$$f(0) = 4,\ f(1) = 2,\ f(2) = 1,\ f(3) = 0.$$

Таким образом, $x = 3$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x-3$ (или на $x+2$), получим $x^3+3x^2+4x+4 = (x-3)\cdot(x^2+x+2)$.

Перебором элементов $x \in GF(5)$ убеждаемся $f_2(x) = x^2 + x + 2$ — неприводимый многочлен.

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

Вычисляем:

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

Ответ: $\{\, 3,\, x,\, 4x + 4 \,\}$.

Задача 2.27. *Является ли многочлен*

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

примитивным?

Решение. Подстановкой в $f(x)$ всех элементов $0, \ldots, 4$ поля $\mathbb{F}_5$ убеждаемся, что данный многочлен 2-й степени не имеет линейных делителей и, следовательно, *неприводим*.

Порядок мультипликативной группы $GF(5^2)$ есть $25 - 1 = 24 = 2^3 \cdot 3$. Определим порядок элемента её x, для которого $x^2 = -x - 2 = 4x + 3$.

Поскольку простые делители 24 суть 2 и 3, проверим равенство $x^d = 1$ для $d \in \{\, \frac{24}{2} = 12,\, \frac{24}{3} = 8 \,\}$. Имеем:

$$x^4 = (x^2)^2 = (4x+3)^2 = x^2 + 4x + 4 = \ldots$$
$$\ldots = 3x + 2 \neq 1,$$
$$x^8 = (x^4)^2 = (3x+2)^2 = -x^2 + 2x + 4 = \ldots$$

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

Следовательно $\operatorname{ord} x = 24$ и рассматриваемый многочлен *примитивен* в поле $\mathbb{F}_5[x]/\big(x^2+x+2\big)$.