Пособие по алгебре

Электронный задачник для самотестирования студентов

Учебно-методический проект

Участники команды:
Сарибекян Г.Э.
Катаев И.И.
Парфенюк М.Д.
Воротынцев А.В.

Руководитель проекта:
Анашкин А.В.

Аннотация

Учебно-методическое пособие предназначено для студентов НИУ ВШЭ и других вузов, обучающихся по направлению подготовки 10.05.01 «Компьютерная безопасность».

Пособие содержит как задачи для тренировки, так и задачи на доказательство. В дополнение к настоящей версии задачника предлагается программа-задачник для составления и решения большего числа задач с коротким ответом (доступ по следующей ссылке:
https://github.com/TeddyReady/MathTasksRenderer/releases/tag/v2.1).

Данный сборник включает себя как теоретическую часть, так и практическую.

При составлении сборника были использованы различные источники (см. список литературы). Часть задач предложена составителями.

В теоретической части пособия приведены необходимые теоретические сведения для применения в решении задач. К их дополнению рекомендуем пользоваться источниками, приведенными под пунктктами 1-7, 10 и 11 списка литературы. Отдельно отмечаем 12 пункт из списка литературы,который ссылается на видео-лекции, подготовленные руководителем проекта Анашкиным А.А.

В практической части пособия содержатся задачи по теории групп, колец и полей. Задачи разбиты по соответствующим темам. Некоторые снабжены ответами, задачи повышенной трудности — указаниями, а в некоторых случаях — решениями. Многие задачи естественным образом объединяются в группы; ключ к решению может находиться в предыдущих задачах. Часть задач предполагают разбора на семинарах. В дополнению к настоящему пособию рекомендуем пользоваться источниками, приведенными под пунктктами 8, 9, 11 списка литературы.

Содержание

1 Группы. Теоретическая часть

1.1 Группа. Подгруппа. Смежный класс по подгруппе

Пусть S - это некоторое множество, тогда произвольное отображение $\mathbf{S} \to \mathbf{S}$ будем называть `бинарной` операцией на множестве S.

Определение 1.1 ***Группой*** $(\mathbb{G}, \cdot)$ *называется множество* G *с бинарной операцией* $\cdot$ *на нём, для которой выполняется:*

1. ***Ассоциативность***

$$\forall a, b, c \in \mathbb{G}: \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

2. ***Нейтральный элемент***

$$\exists e : \forall g \in \mathbb{G} \quad g \cdot e = e \cdot g = g$$

3. ***Существование обратного элемента***

$$\forall g \in \mathbb{G}\ \exists g^{-1}: \qquad g \cdot g^{-1} = g^{-1} \cdot g = e$$

Определение 1.2 ***Абелевой группой*** *называется группа с коммутативной операцией, то есть:*

$$\forall a, b \in \mathbb{G}: \quad a \cdot b = b \cdot a$$

ПРИМЕЧАНИЕ:

Определение 1.3 *Группоид - это множество с бинарной операцией.*
Полугруппа *- это группоид + условие 1.*
Моноид *- это полугруппа + условие 2.*
Группа *- это моноид + условие 3.*
Абелева группа *- это группа + коммутативность.*

Определение 1.4 ***Подгруппой*** $\mathbb{H}$ ***группы*** $\mathbb{G}$ *называется подмножество* $\mathbb{G}$*, образующее группу относительно операции группы* $\mathbb{G}$*.*

Подгруппы группы $\mathbb{G}$, отличные от подгрупп e и $\mathbb{G}$, называются её *собственными подгруппами.*

Определение 1.5 *Класс эквивалентности множества* S *по отношению эквивалентности* R_H *называется* ***левым смежным классом группы*** $\mathbb{G}$ ***по подгруппе*** $\boldsymbol{H}$***.***

Напоминание Отношение эквивалентности обладает свойствами рефлективности, симметричности и транзитивности. Наиболее простым отношением эквивалентности является равенство.
Обозначение: левый смежный класс, порожденный элементом $a \in S$:

$$aH = \{b \in S | \exists h \in H : a * h = b\} \text{ или } a + H = \{b \in S | \exists h \in H : a + h = b\}$$

Второе равенство справедливо для аддитивной символики.
Классы эквивалентности или не пересекаются, или совпадают. Поэтому отношение R_H разбивает множество S на **левые смежные классы**. Такое разбиение называется левосторонним разложением группы $\mathbb{G}$ по подгруппе H.

1.2 Нормальный делитель. Фактор-группа

Определение 1.6 *Подгруппа* $\mathbb{H} = (T, *)$ *называется* ***нормальной подгруппой*** *группы* $\mathbb{G} = (S, *)$ *тогда и только тогда, когда для каждого элемента* $a \in S$ *для любого элемента* $h \in \mathbb{H}$ *верно, что*

$$a' * h * a \in \mathbb{H},$$

где a' *- это элемент, симметричный элементу* $a \in \mathbb{G}$

Доказательство
$\Rightarrow$ Если для каждого элемента $a \in S$ верно $aH = Ha$, то для любого элемента $h \in \mathbb{H}$ найдется такой элемент $h_1 \in \mathbb{H}$, что

$$a * h_1 = h * a,$$

Откуда

$$a' * (a * h_1) = a' * (h * a), \quad h_1 = a' * h * a$$

то есть $a' * h * a \in \mathbb{H}$.
$\Leftarrow$ Если для каждого элемента $a \in S$ для любого элемента $h \in \mathbb{H}$ верно $a' * h * a \in \mathbb{H}$, то

$$a' * h * a = h_1 \in \mathbb{H},$$

Откуда

$$a * (a' * h * a) = a * h_1, \quad h * a = a * h_1$$

T.e $Ha \subseteq aH$
Включение $aH \subseteq Ha$ доказывается аналогично, рассматривая произведение $(a')' * h * a', a' \in S$.
Поэтому $aH = Ha$ ■

Теорема 1.7 *Пусть $\mathbb{G} = (S, *)$, и $N = (T, *)$ - её нормальная подгруппа. Тогда рассмотрим разложение группы $\mathbb{G}$ по нормальной подгруппе. Введём операцию умножения смежных классов:*

$$a, b \in S: \quad (aN)(bN) = (ab)N$$

Теорема 1.8 *Если N – нормальная подгруппа группы $\mathbb{G} = (S, *)$, то введенная выше операция умножения смежных классов корректна.*

Определение 1.9 *Группа смежных классов группы $\mathbb{G}$ по нормальной ее подгруппе N с операцией их умножения называется **фактор-группой** группы $\mathbb{G}$ по подгруппе N и обозначается $\boldsymbol{G/N}$.*

1.3 Теорема Лагранжа

Теорема 1.10 *Порядок каждой подгруппы конечной группы делит порядок группы.*

Доказательство. Пусть $G = (S, *)$ – конечная группа, а H – ее подгруппа. Рассмотрим левостороннее разложение группы G по подгруппе H. Тогда по утверждению, что все левые смежные классы равномощны, их мощность равна порядку подгруппы H. Каждый элемент множества S лежит ровно в одном левом смежном классе, поэтому

$$|G| = |H| \cdot \{ \text{ число левых смежных классов } \}$$

Откуда $|H|||G|$. ■

Теорема 1.11 *Порядок каждого элемента конечной группы делит порядок группы.*

Доказательство. Пусть $\mathbb{G} = (S, *)$ – конечная группа, и $a \in S$ – какой-то ее элемент. Достаточно рассмотреть циклическую ее подгруппу H = <a> с образующим элементом $a \in S$. Тогда порядок элемента a равен порядку группы H, и по теореме Лагранжа делит порядок группы $\mathbb{G}$.
Число смежных классов конечной группы G по подгруппе называется **индексом подгруппы** H в группе G и обозначается как (G : H).
Следствие теоремы Лагранжа. Порядок конечной группы равен произведению порядка какой-то ее подгруппы на индекс этой подгруппы в группе, т.е.

$$|G| = |H| \cdot (G : H), \text{ где}$$

G – конечная группа, а H – ее подгруппа. ■

1.4 Циклическая группа. Число образующих элементов циклической группы порядка m

Определение 1.12 *Группа G называется* ***циклической****, если найдется такой элемент $a \in G$, что $\langle a \rangle = G$, т. е. все элементы группы G являются (целыми) степенями этого элемента a, называемого в этом случае* ***циклическим образующим группы*** *G. Если ord $(a) = n < \infty$, то $G = \langle a \rangle$ — циклическая группа из n элементов; если же ord $(a) = \infty$, то $G = \langle a \rangle$ — бесконечная (****счетная!****) циклическая группа.*

Замечание Любая циклическая группа $G = \langle a \rangle$ является конечной или счетной коммутативной группой. Поэтому любая некоммутативная группа не является циклической и любая несчетная группа не является циклической группой.

Теорема 1.13 *Если $G = \langle a \rangle$ — конечная циклическая группа порядка n (т.е. ord $(a) = n$), $b = a^k \in G, k \in \mathbb{Z}$,то элемент b является циклическим образующим группы G (т. е. $G = \langle a \rangle = \langle b \rangle$) тогда и только тогда, когда числа k и n взаимно просты.*

Доказательство. Так как $|\langle b \rangle| =$ ord (b), то $G = \langle a \rangle = \langle b \rangle$ тогда и только тогда, когда:

$$\text{ord (b)} = |\langle b \rangle| = |\langle a \rangle| = \text{ord (a)}.$$

Учитывая, что ord (b) $= \frac{n}{d}$, где $d = \gcd(k, n)$, мы видим, что ord (b) = ord (a) = n тогда и только тогда, когда d = 1, т. е. числа k и n взаимно просты. ■

Примечание: Здесь и далее под gcd (от англ. Greatest Common Divisor) понимаем наибольший общий делитель (НОД).

1.5 Гомоморфизм групп. Ядро гомоморфизма

Определение 1.14 *Отображение $f : (G, *) \to (G', \cdot)$, для которого $f(a * b) = f(a) \cdot f(b), \forall a, b \in G$, называется* ***гомоморфизмом****. Биективные гомоморфизмы называются* ***изоморфизмами****.*

Для гомоморфизмов $f : (G, *) \to (G', \cdot)$ определим:

$$Im(f) = \{g' \in G' | g' = f(g), g \in G\}$$

(образ гомоморфизма f);

$$Ker(f) = \{g \in G | f(g) = e'\}$$

где e' — нейтральный элемент группы G' (*ядро гомоморфизма f*).

Теорема 1.15 *(свойства гомоморфизма групп). Пусть G и G' — группы, e и e; соответственно — их нейтральные элементы, $f : G \to G'$ — гомоморфизм групп. Тогда:*

1. $f(e) = e'$
2. $f(x^{-1}) = (f(x))^{-1}, \forall x \in G$
3. $H' = Im\ f$ - *подгруппа* G'
4. *Если $G = \langle a \rangle$, то Im $\langle f\langle a \rangle \rangle$ — также циклическая группа*
5. *Если ord $(a) < \infty, \forall a \in G$, то ord $(f(a))$ является делителем числа ord (a) (если f — инъективный гомоморфизм, то ord $(f(a))$ = ord (a))*
6. $f(g^{-1}hg) = (f(g))^{-1} f(h) f(g)$
7. $Ker(f)$ — *нормальная подгруппа группы G*
8. *Для $x, y \in G, f(x) = f(y)$ тогда и только тогда, когда $xy^{-1} \in Ker(f)$*
9. f — *инъективное отображение тогда и только тогда, когда $Ker(f) = \{e\}$*

1.6 Центр группы. Свойства

Определение 1.16 *Подгруппа группы G называется центром, если верно:*

$$Z(G) = \{a \in G | ax = xa, \forall x \in G\}$$

Пусть G - группа и $x \in G$.

Определение 1.17 *Централизатор x - это множество* $C(x) = \{a \in G | ax = xa\}$

То есть, центральные элементы - это такие элементы, которые коммутируют со всеми элементами группы. В частности, единица всегда является центральным элементом, а в абелевой группе все элементы - центральные.

СВОЙСТВА

1. Любая подгруппа, содержащаяся в центре группы, является нормальной абелевой подгруппой. В частности, $Z(G)$ - нормальная абелева подгруппа в группе G.
2. G - абелева группа $\iff Z(G) = G$.
3. $z \in Z(G) \iff C(z) = G \iff$ класс сопряжённых элементов, содержащий z, состоит из одного элемента z.

1.7 Классы сопряжённых элементов

Определение 1.18 *Класс сопряжённости - множество элементов группы G, обозначаемое* $[g]$ *или Cl(g), образованное из элементов, сопряжённых заданному* $g \in G$, $^-hgh^{-1}$, *где h — произвольный элемент группы G.*

В силу того, что сопряжение элементов является отношением эквивалентности, все члены класса сопряжённости сопряжены друг с другом, то есть, если h $\in$[g], g $\in [h]$, и классы сопряжённости заданной группы не пересекаются, образуя её разбиение на непересекающиеся подмножества.

Доказательство.

1. **Рефлексивность:** Для каждого $a \in S$ выберем $e \in H$ – нейтральный элемент. Тогда a * e = a, поэтому aR_Ha.
2. **Симметричность:** Пусть для элементов $a, b \in S$ верно aR_Hb, т.е.найдется такой элемент $h \in H$, что $a * h = b$. Тогда

   $$a * h = b, a * h * h' = b * h', \quad a = b * h'$$

   Т.к. H – группа, $h' \in H$. Откуда bR_Ha.
3. **Транзитивность:** Пусть для элементов $a, b, c \in S$ верно aR_Hb и bR_Hc, т.е. найдутся такие элементы $h_1 \in H$ и $h_2 \in H$, что $a * h_1 = b$ и $b * h_2 = c$. Тогда

   $$a * (h_1 * h_2) = (a * h_1) * h_2 = b * h_2 = c$$

   Т.к. H – группа, $h_1 * h_2 = h \in H$. Откуда aR_Hc . ■

Элементы g_1 и g_2 группы G называются сопряжёнными, если существует элемент $h \in G$, для которого $hg_1h^{-1} = g_2$. Сопряжённость является отношением эквивалентности, а потому разбивает G на классы эквивалентности, это, в частности, означает, что каждый элемент группы принадлежит в точности одному классу сопряжённости, и классы $[g_1]$ и $[g_2]$ совпадают тогда и только тогда, когда g_1 и g_2 сопряжены, и не пересекаются в противном случае.

Определение 1.19 *Класс сопряжённости - класс эквивалентности по отношению сопряжённости. Обозначение: класс эквивалентности, содержащий элемент x:* $C(x) = C_G(x) = \{gxg^{-1} | g \in G\}$

Обозначение: левый смежный класс, порожденный элементом $a \in S$:

$$aH = \{b \in S | \exists h \in H : a * h = b\} \text{ или } a + H = \{b \in S | \exists h \in H : a + h = b\}$$

Теорема 1.20 *В каждом левом (правом) смежном классе группы по конечной подгруппе число элементов совпадает с порядком этой подгруппы.*

Доказательство. Пусть $H = \{h_1 = e, h_2, ..., h_m\}$ – конечная подгруппа группы $\mathbb{G} = (S; *)$. Тогда для элемента $a \in S$ левый смежный класс aH состоит из элементов вида:

$$a * h_1, a * h_2, ..., a * h_m$$

Поэтому $|aH| <= |H|$.
Предположим, что $|aH| < |H|$. Т.е. найдутся такие элементы $h_i, h_j \in H, h_i \neq h_j$,что

$$a * h_i = a * h_j.$$

Тогда по правилу сокращения $h_i = h_j$ – противоречие. Следовательно, $|aH| = |H|$. ■

1.8 Декартово произведение групп

Произведение подгрупп — не обязательно подгруппа. Пусть имеются две группы G_1 и G_2.

Определение 1.21 *Рассмотрим их декартово произведение, то есть, такое множество упорядоченных пар:*

$$\{(x_1, x_2) | x_1 \in G_1, x_2 \in G_2\}$$

Введём для них "покомпонентное"умножение: $(x_1, x_2)(y_1, y_2) \stackrel{\text{def}}{=} (x_1 y_1, x_2 y_2)$
Проверим его на соответствие требованиям к группам. Свойство ассоциативности имеет место, так как оно имело место в компонентах. Элемент (1, 1) - является единицей относительно введённой операции. Для (x_1, x_2) обратным, очевидно, будет (x_1^{-1}, x_2^{-1}).
Таким образом, результат декартова произведения групп тоже является группой, которую называют *внешним прямым произведением групп* G_1 *и* G_2 и обозначают $G_1 \cdot G_2$.
Некоторое свойство (без доказательства)
1. Множество элементов вида $(x_1, 1)$ и $(1, x_2)$ - это нормальные подгруппы группы $G_1 \cdot G_2$, изоморфные группам G_1 и G_2 соответственно.

1.9 Представление подстановок произведением независимых циклов

Определение 1.22 *Пусть X — произвольное множество. Перестановкой на множестве X называется любое биективное отображение $\sigma : X \to X$. Нас будут интересовать только перестановки конечных множеств. Элементы конечного множества из n элементов будем обозначать просто натуральными числами от 1 до n. Итак, пусть X = 1,...,n. Перестановку $\sigma : X \to X$ удобно тогда записывать в виде следующей таблицы:*

$$\begin{pmatrix} 1 & 2 & 3 & ... & n \\ & & & ... & \end{pmatrix}$$

которую во многих учебниках называют подстановкой, соответствующей перестановке σ.

Определение 1.23 *Разложим теперь подстановки из S_n в произведение более простых подстановок, называемых циклами. Цикл - это перестановка, в которой элементы переставляются по циклу:*

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_{k-1} \mapsto i_k \mapsto i_1$$

Теорема 1.24 *Любая подстановка в S_n раскладывается в произведение независимых циклов. Эти циклы определяются однозначно по подстановке, с точностью до их перестановки.*

1.10 Четность перестановок

Определение 1.25 *Говорят, что в данной перестановке два числа образуют инверсию (беспорядок), если большее из чисел в данной перестановке стоит левее меньшего. В противном случае эти два числа образуют порядок.*

Рассмотрим перестановку шестого порядка:

$$2, 5, 1, 4, 6, 3$$

Подсчитаем общее количество инверсий в данной перестановке. Для этого поступим следующим образом: возьмём единицу и сосчитаем, сколько чисел стоит левее единицы:
1 – две инверсии, затем единицу вычеркнем из перестановки; теперь возьмём двойку и подсчитаем, сколько чисел стоит левее двойки; 2 – ноль инверсий; вычёркиваем двойку и принимаемся за тройку; левее тройки стоит три числа, то есть тройка даёт нам три инверсии; вычёркиваем тройку и считаем, сколько чисел будет левее четвёрки; четвёрка даёт одну инверсию, вычёркиваем четвёрку и считаем количество чисел левее пятёрки; пятёрка даёт 0 инверсий, вычёркиваем пятёрку и считаем количество инверсий, которые даёт шестёрка; шестёрка даёт 0 инверсий.
1 – две инверсии; 2 – ноль инверсий; 3 – три инверсии; 4 – одна инверсия; 5 – ноль инверсий; 6 – ноль инверсий. Общее число инверсий, таким образом, получается шесть.

Определение 1.26 *Перестановка называется чётной, если общее количество инверсий есть чётное число и, соответственно, нечётной, если общее количество инверсий, содержащихся в этой перестановке, число нечётное.*

Очевидно, что тождественная подстановка является четной, так как не содержит ни одной инверсии.
Транспозиция (i, j) всегда нечетна.
Множество всех четных перестановок (обозначаемое через A_n) замкнуто относительно операций умножения и взятия обратной перестановки (то есть, является группой).

1.11 Представление подстановок произведением транспозиций

Определение 1.27 *Транспозицией называется такое преобразование перестановки, при котором какие – либо два её элемента меняются местами, а все остальные элементы остаются на своих местах. (то есть, цикл длины 2)*

СВОЙСТВА / ТЕОРЕМЫ

1. Транспозиция меняет чётность перестановки на противоположную
   Доказательство. Если k и l находились в инверсии в перестановке (были переставлены), после умножения на (k, l) они встали на места; если они находились в правильном порядке, то оказались в инверсии. При этом количество инверсий элементов, стоящих между k и l, после умножения на (k, l) либо увеличится на 2, либо уменьшится на 2, что не влияет на четность.

2. Любой цикл длины k есть произведение (k - 1) транспозиции:

$$(i_1, ..., i_k) = (i_1, i_2) \cdot (i_2, i_3) \cdot ... \cdot (i_{k-1}, i_k)$$

   Доказательство. Если $\sigma = \mathrm{id}$, можно считать, что она раскладывается в произведение 0 транспозиций.
   Если $\sigma \neq \mathrm{id}$, то существует хотя бы одна инверсия, т.е. есть такое место в нижнем ряду, где подряд идут элементы k и l, причем $k > l$. Умножим на транспозицию (k, l). В результате элементы k и l

переставятся, и число инверсий уменьшится ровно на одну. Продолжаем эту процедуру, пока все элементы не встанут на свое место. В итоге получим:

$$\begin{pmatrix} 1 & 2 & 3 & ... & n \\ & & & ... & \end{pmatrix} \text{(k, l) (...) ... (...)} = \ = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ & & & ... & \end{pmatrix} = \text{(k, l) (...) ... (...)}$$

Цикл, как перестановка, является четным, если его длина нечетна и наоборот.

2 Группы. Задачи для тренировки

2.1 Алгебраические структуры. Группы и их свойства

2.1.1 Какие из следующих множеств чисел относительно сложения образуют полугруппу, а какие группу:

1) множество N натуральных чисел;
2) множество целых неотрицательных чисел;
3) множество целых неположительных чисел;
4) множество $\mathbb{Z}$ целых чисел;
5) множество $2\mathbb{Z}$ четных чисел;
6) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n \neq 0$;
7) множество $\mathbb{Q}$ рациональных чисел;
8) множество иррациональных чисел;
9) множество $\mathbb{R}$ вещественных чисел;
10) множество C комплексных чисел?

2.1.2 Какие из следующих множеств чисел относительно умножения образуют полугруппу, а какие группу:

1) множество натуральных чисел;
2) множество целых неотрицательных чисел;
3) множество целых неположительных чисел;
4) множество $\mathbb{Z}$ целых чисел;
5) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n \neq 0$;
6) множество $\mathbb{Q}$ рациональных чисел;
7) множество $\mathbb{Q}$ ненулевых рациональных чисел;
8) множество $\mathbb{Q}_+$ положительных рациональных чисел;
9) множество иррациональных чисел;
10) множество $\mathbb{R}$ вещественных чисел;
11) множество $\mathbb{R}$ ненулевых вещественных чисел;
12) множество $\mathbb{R}_+$ положительных вещественных чисел;
13) множество C комплексных чисел;
14) множество C ненулевых комплексных чисел;
15) множество U_n всех значений корня n-й степени из 1;
16) множество U всех комплексных чисел, по модулю равных 1;
17) множество H_n чисел вида

$$\rho(\cos\tfrac{2\pi k}{n} + i\sin\tfrac{2\pi k}{n}),$$
где $\rho > 0, k = 0, 1, ..., n-1$?

2.1.3 Образуют ли полугруппу/группу:

1) вещественные числа относительно вычитания;
2) вещественные числа относительно операции -$a - b$;
3) ненулевые вещественные числа относительно деления;
4) натуральные числа относительно операции $\{a, b\}$?

2.1.4 Образует ли полугруппу/группу множество положительных вещественных чисел относительно указанной операции •:

1) $a \bullet b = a^b$;
2) $a \bullet b = (a^2)(b^2)$?

2.1.5 Пусть X — некоторое непустое множество. Образует ли множество 2^X полугруппу/группу относительно указанной операции? Указать нейтральный элемент, если он существует:

1) объединение множеств;
2) пересечение множеств;
3) симметрическая разность множеств?

2.1.6 Какие из следующих множеств с указанными операциями образуют полугруппу, а какие группу:

1) множество векторов плоскости относительно сложения;
2) множество векторов пространства относительно сложения;
3) множество векторов пространства относительно скалярного произведения;
4) множество векторов пространства относительно векторного произведения?

2.2 Группы перестановок

2.2.1 Найти произведение подстановок

1) $S_4 : \left(\begin{smallmatrix}1&2&3&4\\3&1&4&2\end{smallmatrix}\right) \cdot \left(\begin{smallmatrix}1&2&3&4\\3&1&2&4\end{smallmatrix}\right) = ?$

2) $\mathrm{S}_9 : \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\6&4&9&7&1&5&2&8&3\end{smallmatrix}\right) \cdot \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\4&8&5&2&1&3&6&9&7\end{smallmatrix}\right) = ?$

3) $S_8 : (4, 6, 7, 3, 1, 2, 5, 8) \cdot (7, 1)(6, 8, 3, 4)(2, 5) = ?$

4) $S_6 : (2, 5, 6) \cdot (5, 1, 4, 2) = ?$

2.2.2 Найти обратную подстановку

1) $S_{10} : \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\4&10&7&1&8&6&9&3&2&5\end{smallmatrix}\right)^{-1} = ?$

2) $\mathrm{S}_{10} : \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\6&7&8&4&10&9&3&1&2&5\end{smallmatrix}\right)^{-1} = ?$

3) $S_3 : (2, 1)^{-1} = ?$

4) $S_7 : (4, 1, 2, 6, 7, 3)^{-1} = ?$

2.2.3 Вычислить цикловой тип данных подстановок

1) $S_8 : \left(\begin{smallmatrix}1&2&3&4&5&6&7&8\\3&2&7&1&6&4&5&8\end{smallmatrix}\right) = ?$

2) $\mathrm{S}_9 : \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\3&8&4&2&9&7&1&5&6\end{smallmatrix}\right) = ?$

3) $\mathrm{S}_{10} : (5, 3)(7, 10, 1, 8)(9, 6) = ?$

4) $\mathrm{S}_4 : (1, 3, 4) = ?$

2.2.4 Определить четность данных подстановок

1) $S_{10} : \delta\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\4&3&10&2&5&8&1&9&6&7\end{smallmatrix}\right) \Rightarrow ?$

2) $\mathrm{S}_4 : \delta\left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right) \Rightarrow ?$

3) $\mathrm{S}_7 : \delta(6, 1, 4)(2, 5, 3, 7) \Rightarrow ?$

4) $\mathrm{S}_5 : \delta(2, 1, 4, 5, 3) \Rightarrow ?$

2.2.5 Вычислить количество беспорядков данных подстановок

1) $S_{10} : \Delta\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\5&10&2&4&9&1&7&3&8&6\end{smallmatrix}\right) = ?$ 2) $\mathrm{S}_9 : \Delta\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\6&4&9&2&7&3&1&5&8\end{smallmatrix}\right) = ?$

3) $\mathrm{S}_{10} : \Delta(10,8,2,1,6)(7,4,9,5,3) = ?$ 4) $\mathrm{S}_4 : \Delta(3,4) = ?$

2.2.6 Определить порядок данных подстановок

1) $S_6 :\ ord\left(\begin{smallmatrix}1&2&3&4&5&6\\4&6&2&5&1&3\end{smallmatrix}\right) = ?$ 2) $\mathrm{S}_5 :\ ord\left(\begin{smallmatrix}1&2&3&4&5\\5&4&3&1&2\end{smallmatrix}\right) = ?$

3) $\mathrm{S}_{10} :\ ord(2,6,1,7,8,3,4) = ?$ 4) $\mathrm{S}_4 :\ ord(2,1,3,4) = ?$

2.2.7 Запишите подстановку в виде произведения транспозиций

1) $S_6 : \left(\begin{smallmatrix}1&2&3&4&5&6\\5&1&2&3&4&6\end{smallmatrix}\right) = ?$ 2) $\mathrm{S}_5 : \left(\begin{smallmatrix}1&2&3&4&5\\4&1&5&3&2\end{smallmatrix}\right) = ?$

3) $\mathrm{S}_{13} : (5,13,7,11,4)(6,1,8,12,2,10,3,9) = ?$ 4) $\mathrm{S}_{10} : (7,8,3,5,10,6,9,4,1,2) = ?$

2.2.8 Разложить в произведение транспозиций соседних элементов

1) $S_5 : \left(\begin{smallmatrix}1&2&3&4&5\\1&4&5&3&2\end{smallmatrix}\right) = ?$ 2) $\mathrm{S}_4 : \left(\begin{smallmatrix}1&2&3&4\\1&3&2&4\end{smallmatrix}\right) = ?$

3) $\mathrm{S}_4 : (1,2,3) = ?$ 4) $\mathrm{S}_6 : (3,2,5,1,4,6) = ?$

2.2.9 Вычислите функцию Эйлера

1) $\varphi(75) = ?$ 2) $\varphi(32) = ?$ 3) $\varphi(89) = ?$ 4) $\varphi(71) = ?$ 5) $\varphi(16) = ?$

6) $\varphi(81) = ?$ 7) $\varphi(10) = ?$ 8) $\varphi(66) = ?$ 9) $\varphi(36) = ?$ 10) $\varphi(100) = ?$

2.2.10 Доказать степень алгебраической структуры и найти ее порядок

1) множество всех подстановок (биективных отображений) множества $\{1,2,...,n\}$ на себя образует группу относительно произведения. Эта группа называется симметрической группой степени n и обозначается S_n.
2) множество всех четных подстановок образует подгруппу в S_n. Эта подгруппа называется знакопеременной группой степени n и обозначается A_n.

3 Группы. Задачи на доказательство

1) Показать, что каждая группа порядка ≤ 5 абелева.

2) Показать, что группа порядка 15 - циклическая.

3) Показать, что существуют две неизоморфные группы порядка 4, а именно циклическая и произведение двух групп порядка 2.

4) Пусть p - наименьшее простое число, делящее порядок конечной группы G, H - подгруппа индекса p. Показать, что H нормальна в G.

5) Показать, что существуют ровно две неизоморфные неабелевы группы порядка 8. (Одна из них задается образующими σ , τ и соотношениями $\sigma^4 = 1$, $\tau^4 = 1$, $\tau\sigma\tau = \sigma^3$. Другая - группа кватернионов.)

6) Пусть G - группа и A - ее нормальная абелева подгруппа. Показать, что G/A действует на A посредством сопряжений, и таким путем можно получить гомоморфизм G/A в Aut(A).

7) Определить все группы порядка ≤ 10 с точностью до изоморфизма.

8) Группа G называется *периодической*, если $\forall\, x \in G \;\; \exists\, n \in \mathbb{N} : x^n = 1$. Показать, что в категории периодических абелевых групп существуют бесконечные прямые произведения.

9) Пусть G - группа и H - ее подгруппа конечного индекса. Показать, что в G существует нормальная подгруппа N конечного индекса, содержащаяся в H.
Указание: если $(G : H) = n$, то найти гомоморфизм G в S_n, ядро которого содержится в H.

10) Рассматривая Z и Q как аддитивные группы, показать, что Q/Z - периодическая группа, которая имеет одну и только одну подгруппу порядка $n \in \mathbb{N}$, и притом каждая такая подгруппа циклическая.

11) Показать, что если A - циклическая группа порядка n и d - положительное целое число, являющееся делителем n, то A содержит ровно одну подгруппу порядка d, причем эта подгруппа циклическая.

12) Пусть G - циклическая группа порядка n и H - циклическая группа порядка m. Показать, что в случае взаимно простых m, n группа $G \cdot H$ будет циклической (порядка mn).

13) Пусть X — некоторое непустое множество (возможно, бесконечное). Доказать, что

13.1) множество всех отображений $X \to X$ относительно операции произведения образует полугруппу, но (при $|\mathbb{Z}| \neq 1$) не группу;

13.2) множество всех биективных отображений $X \to X$ относительно операции произведения образует группу.

14) Доказать, что множество всех отображений множества $\{1, 2, ..., n\}$ в себя относительно операции композиции (произведения) образует полугруппу, но (при $n > 1$) не группу.

15) Доказать, что множество нечетных подстановок подгруппы не образуют.

4 Группы. Задачи с решением

Задача № 1. Найти все различные смежные классы группы $G = (\mathbb{Z}_6, +)$ вычетов по модулю 6 по ее подгруппе $H = \{0, 3\}$.

Решение. Множество смежных классов группы $\mathbb{G}$ по ее подгруппе H задается в виде $g + H$, $g \in G$. Отсюда получаем, что $\{g + H | g \in G\} = \{0 + H, 1 + H, 2 + H\} = \{(0, 3), (1, 4), (2, 5)\}$.

Ответ: {(0,3), (1,4), (2,5)}.

Задача № 2. Найти число классов сопряженных элементов группы G=$(\mathbb{Z}_{10}, +)$.

Решение. Так как группа абелева, то любой ее класс сопряженных элементов состоит из одного элемента. Отсюда группа G=$(\mathbb{Z}_{10}, +)$ состоит из 10 классов сопряженности.

Ответ: 10.

Задача № 3. Какие из элементов циклической группы G=$(\mathbb{Z}_8, +)$ являются ее образующими?

Решение. Число t является образующим элементом циклической группы вычетов по модулю n в том и только том случае, когда НОД(t,n)=1. Следовательно, образующими группы G являются элементы множества 1,3,5,7.

Ответ: 1,3,5,7.

Задача № 4. Найти все собственные подгруппы группы G=$(\mathbb{Z}_7, +)$.

Решение. Любая подгруппа H циклической группы G=$(\mathbb{Z}_n, +)$ вычетов по модулю n сама является циклической, т.е. множество подгрупп группы G=$(\mathbb{Z}_n, +)$ исчерпывается множеством циклических групп $H =< g >, g \in G$. Так как 7 является простым числом, то для любого ненулевого $g \in (\mathbb{Z}_7, +)$ подгруппа $H =< g >$ совпадает со всей группой G=$(\mathbb{Z}_7, +)$. Следовательно, в группе G=$(\mathbb{Z}_7, +)$ нет собственных подгрупп.

Ответ: в группе G=$(\mathbb{Z}_7, +)$ нет собственных подгрупп.

Задача № 5. Имеется ли в группе G=$\mathbb{Z}_{24}^*(\cdot)$ мультипликативно обратимых по модулю 24 чисел элемент порядка 3?

Решение. Порядок элемента в группе G=$\mathbb{Z}_n^*(\cdot)$ чисел, мультипликативно обратимых по модулю n, является делителем порядка $|G|$ группы, который равен j(n), где $j(\cdot)$ - функция Эйлера. Так как $|\mathbb{Z}_{24}^*(\cdot)| = j(24) = 8$ и 3 не является делителем числа 8, то в группе $\mathbb{Z}_{24}^*(\cdot)$ нет элемента порядка 3.

Ответ: нет.

Задача № 6. Доказать, что группа $\mathbb{Z}_6(+)$ разлагается в прямую сумму своих подгрупп $H_1 = \{0, 2, 4\}$ и $H_2 = \{0, 3\}$.

Решение. Непосредственной проверкой убеждаемся в том, что для любого элемента g группы $\mathbb{Z}_6(+)$ существуют элементы $h_1 \in H_1$ и $h_2 \in H_2$, для которых выполнено равенство: $g = h_1 + h_2(mod6)$. Следовательно, группа $\mathbb{Z}_6(+)$ равна сумме своих подгрупп: $\mathbb{Z}_6(+) = H_1 + H_2$. Так как $H_1 \cap H_2 = \{0\}$, то группа $\mathbb{Z}_6(+)$ является прямой суммой подгрупп H_1 и H_2.

5 Кольца. Теория

5.1 Идеал кольца. Фактор-кольцо

Определение 5.1 *Множество A называется кольцом, если на нем определены две бинарные операции: + (сложение) и · (умножение), обладающие следующими свойствами:*

1. *(A, +) является абелевой группой;*
2. *умножение · ассоциативно;*
3. *операции сложения и умножения связаны дистрибутивными законами:* $(a+b)\cdot c = a\cdot c + b\cdot c, \quad c\cdot(a+b) = c\cdot a + c\cdot b, \quad \forall a,b,c \in A$

Определение 5.2 *Коммутативное ассоциативное кольцо с единицей — это кольцо, операция умножения в котором удовлетворяет ещё трём дополнительным аксиомам:*

1. *коммутативность умножения:* $ab = ba \quad \forall a,b \in A$;
2. *ассоциативность умножения:* $a(bc) = (ab)c \quad \forall a,b,c \in A$;
3. *существование единицы:* $\exists 1 \in A : \ \forall a \in A : \ 1\cdot a = a$;

Обозначается кольцо буквой $\mathbb{K}$ *(от нем. Körper) или* $\mathbb{R}$ *(от англ. Ring).*

Примечание: Мы не требуем того, что $1 \neq 0$. Однако если едница равна нулю, то кольцо A состоит только из нуля.

Определение 5.3 *Пусть A — произвольное кольцо. Подмножество* $I \subset A$ *называется идеалом, если выполнено следующее:*

1. $\forall x,y \in I, x+y \in I$;
2. $\forall x \in I, -x \in I$;
3. $\forall x \in I, a \in A, ax \in I$;

Первые две аксиомы равносильны тому, что I — подгруппа в A по сложению (в частности, $0 \in I$). На самом деле, вторая аксиома следует из третьей: т.к. $-1 \in I$, то I оказывается замкнуто по умножению на -1: то есть, если $x \in I$, то $-x \in I$.
Обратите внимание, что в третьей аксиоме требуется замкнутость I по умножению на все элементы из A (а не только из I) — это очень существенное ограничение. В частности, если $I \ni 1$, то I = A: единицу можно умножить на любой элемент кольца, и результат будет снова принадлежать I. По той же причине идеал, содержащий любой обратимый элемент, совпадает со всем кольцом.
Пример 1 В любом кольце есть два тривиальных идеала: нулевой (состоящий из одного нуля) и всё кольцо. Впрочем, некоторые авторы предпочитают считать, что $I \neq A$, и всё кольцо, таким образом, (как раз собственным) идеалом не считается — но это вопрос терминологический.

Определение 5.4 *Идеал вида* $(a) \subset A$*, т.е. порождённый одним элементом, называется главным идеалом.*

Определение 5.5 *Кольцо называется целостным (или областью целостности), если в нём произведение любых двух ненулевых элементов отлично от нуля (т.е. из того, что* $ab = 0$*, следует, что либо* $a = 0$*, либо* $b = 0$*).*

Пусть A — произвольное коммутативное кольцо, $I \subset A$ — идеал. Определим на множестве элементов из A следующее отношение: будем говорить, что $x \equiv yI$, если $x - y \in I$. Ясно, что это отношение эквивалентности. Классы эквивалентности — это множества вида $x + I = \{x + a | a \in I\}$. Иногда мы также будем обозначать класс x + I через $[x]$. Обозначим множество этих классов через A/I. На классах эквивалентности из A/I можно определить операции сложения и умножения:

$$(x+I)+(y+I)=(x+y)+I; \quad (x+I)(y+I)=xy+I.$$

Таким образом, на A/I вводятся операции сложения и умножения, что задаёт на нём структуру кольца. Полученное кольцо называется **факторкольцом** кольца A по идеалу I. Говорят, что кольцо A *факториально.*
Ясно, что нулём и единицей в A/I являются 0 + I и 1 + I соответственно.
Примеры

1. Любое из привычных нам полей $\mathbb{Q}, \mathbb{R}$,$\mathbb{C}$,$\mathbb{Z}_p$ является кольцом;
2. Самый распространенный пример кольца, не являющегося полем, — кольцо целых чисел Z.
3. Примером кольца, благодаря которому кольца именно так именуются, является кольцо вычетов по модулю n — $\mathbb{Z}_n$. Данное кольцо состоит из остатков $\{0, 1, 2, ..., n-1\}$ от деления на n, операции сложения и умножения проводятся по модулю n. Ясно, что при составном n такое кольцо не будет являться полем.

5.2 Делители нуля

Определение 5.6 *Элемент $r \neq 0$ ассоциативного кольца R (не обязательно с единицей) называется левым делителем нуля, если существует $0 \neq s \in R$ такой, что $rs = 0$. Аналогично вводятся правый и двусторонний делители нуля.*

1. В поле нет делителей нуля: если $rs = 0$ и $r \neq 0$, то существует обратный элемент 1/r. Тогда $\frac{1}{r} \cdot rs = \frac{1}{r} \cdot 0$, откуда $s = \frac{1}{r} \cdot 0$. Однако $x + x \cdot 0 = x(1+0) = x \cdot 1 = x$ откуда, $x \cdot 0 = 0$. Значит, $s = 0$, т.е. в поле нет делителей нуля.
2. В кольце целых чисел нет делителей нуля;
3. Если в кольце R не было делителей нуля, то и в кольце многочленов (от любого числа переменных) над R нет делителей нуля.
4. В кольце вычетов $\mathbb{Z}_n$ есть делители нуля, если n — не просто. Этими делителями являются любые числа в $\mathbb{Z}_n$, которые не взаимно просты с n.

5.3 Строение подколец кольца $\mathbb{Z}$ целых чисел

Определение 5.7 *Пусть $R = (S; +, \cdot)$ – кольцо, и $T \subseteq S$. Структура $K = (T; +, \cdot)$ называется подкольцом кольца R , если множество T с операциями сложения $+$ и умножения $\cdot$ является кольцом.*

Теорема 5.8 *Пусть $R = (S; +, \cdot)$ – кольцо. Множество $T \subseteq S$ с операциями сложения $+$ и умножения $\cdot$ является подкольцом кольца R тогда и только тогда, когда для любых элементов $a, b \in T$ верно $a - b \in T$.*

К главному! В кольце целых чисел все идеалы имеют вид $n\mathbb{Z}$ (порождаются одним элементом $n \in \mathbb{Z}$). Таким идеалы (порожденные одним элементом) называются главными.

- Действительно, рассмотрим некоторый ненулевой идеал I кольца Z и его минимальный положительный элемент d. Если каждый элемент идеала делится на d, то перед нами идеал $d\mathbb{Z}$.
  Если существует элемент $a \in I$, который не делится на d, то разделим a на d с остатком, получив:

  $$a = qd + r, 0 < d < r$$

  Так как $d \in I$, то $qd \in I$, а значит, $r = a - qd \in I$. Получаем противоречие в выбором d (то есть существует число меньшее d).

Такое кольцо называется *кольцом главных идеалов.*

5.4 Максимальные идеалы. Строение максимальных идеалов кольца целых чисел $\mathbb{Z}$

Определение 5.9 *Идеал $\mathfrak{m} \to A$ называется **максимальным**, если он не содержится ни в каком большем идеале (не совпадающем со всем кольцом).*

- Идеал $\mathfrak{m}$ максимален тогда и только тогда, когда $A/\mathfrak{m}$ поле.
  - Пусть $\mathfrak{m}$ максимален. Докажем, что всякий ненулевой элемент $[a] \in A/\mathfrak{m}$ обратим. Действительно, $a \notin \mathfrak{m}$. Рассмотрим идеал $a + m = \{ax + m | x \in A, m \in \mathfrak{m}\}$. Этот идеал содержит $\mathfrak{m}$ и не совпадает с ним (поскольку содержит ещё и a), значит, он совпадает со всем кольцом. Поэтому $1 =$ ax + m для некоторых $x \in A, m \in \mathfrak{m}$. Получаем, что в $A/\mathfrak{m}$ элемент [x] есть $[a]^{-1}$, так как $[1] = [a][x] + [m] = [a][x]$. Обратное утверждение доказывается аналогично.

Определение 5.10 *Идеал $\mathfrak{p} \to A$ называется простым, если для любых двух элементов $a, b \in A$, таких, что $ab \in \mathfrak{p}$, верно, что либо $a \in \mathfrak{p}$, либо $b \in \mathfrak{p}$.*

Теорема 5.11 *Простые идеалы в $\mathbb{Z}$ - это идеалы вида (p), где p простое. Они же являются и максимальными! (Доказательство очевидно)*

5.5 Строение подколец кольца $\mathbb{F}[x]$ многочленов над полем $\mathbb{F}$

В кольце многочленов все идеалы имеют вид $p(x)\mathbb{F}[x]$ (порождаются одним элементом $p(x) \in \mathbb{F}$). **Все они являются главными.**

- Рассмотрим тривиальные идеалы, которые являются главными:

$$\{0\} = 0\mathbb{F}[x] \quad \mathbb{F}[x] = 1\mathbb{F}[x]$$

Пусть I - нетривиальный идеал кольца $\mathbb{F}[x]$, а p(x) - многочлен минимальной степени в $I - \{0\}$.
Так как I - идеал. то верно: $p(x)\mathbb{F}[x] \subseteq I \subseteq \mathbb{F}[x]$
Когда $p \in \mathbb{F} - \{0\}$, $p(x)\mathbb{F}[x] = \mathbb{F}[x] = I$, тогда I - главный идеал.
Пусть $p \notin \mathbb{F}$. Возьмём такое $a \in I$, что $p \nmid a$ в $\mathbb{F}[x]$. По теореме о делении многочлена с остатком:

$$\exists q, r \in \mathbb{F}[x]$$

такое, что

$$a = pq + r \ \ \& \ \ \deg(r) < \deg(p) \ \ \& \ \ r \neq 0$$

$$a, p \in I$$
$$\Rightarrow a, pq \in I$$
$$\Rightarrow r = a - pq \in I$$

Так как $r \in I - \{0\}, \deg(r) < deg(p)$, а p - многочлен с наименьшей степенью в I, что противоречит записанному выше, значит:

$$p|a \quad \forall a(x) \in I \Rightarrow I = p(x)\mathbb{F}[x]$$

5.6 Строение максимальных идеалов в кольце $\mathbb{F}[x]$ над полем $\mathbb{F}$

Максимальными идеалами в кольце многочленов $\mathbb{F}[x]$ надо полем являются идеалы, порожденные неприводимыми многочленами (см. Определение неприводимого многочлена).

5.7 Характеристика кольца. Примеры

Определение 5.12 *Пусть $R = (S; +, \cdot)$ — кольцо. Наименьшее натуральное число n (если оно существует), что для каждого элемента $a \in S$ верно $na = 0$, называется характеристикой кольца R.*

$qa = \underbrace{a + a + ... + a}_{q\ раз} = 0$

В этом случае говорят, что кольцо R — с **положительной** характеристикой.
Если таких натуральных чисел нет, то говорят, что кольцо R — **с нулевой характеристикой**.

Теорема 5.13 *Характеристика конечного целостного кольца положительна и является простым числом.*

Доказательство

- Рассмотрим единицу e конечного целостного кольца R. Тогда в последовательности

  $$e, 2e, ..., ne, ...$$

  найдутся такие натуральные числа i и j, $i < j$, что

  $$ie = je$$

  Отсюда, $(j - i)e = 0$. Тогда для каждого элемента $a \in R$ верно

  $$(j - i)a = (j - i)(e \cdot a) = ((j - i)e) \cdot a = 0$$

  Т.е. кольцо R — с положительной характеристикой.

- Пусть n — положительная характеристика конечного целостного кольца R. Докажем от противного, что она является простым числом.
  Пусть $n = k \cdot m$, где $k, m > 1$. Тогда

  $$0 = ne = (k \cdot m)e = (ke) \cdot (me)$$

  Т.к. в целостном кольце R нет делителей нуля, верно ke = 0 или me = 0, что противоречиит тому, что n — наименьшее из таких чисел.
  ■

Примеры

1. $Char(\mathbb{Z}) = 0, Char(\mathbb{Q}) = 0, Char(\mathbb{R}) = 0, Char(C) = 0$
2. $Char(\mathbb{Z}_n) = n$, так как $x \in \mathbb{Z}_n, nx = 0$
3. Аналогично предыдущему, $Char(\mathbb{F}_q[x]/f) = f$

5.8 Условия максимальности идеала $m \cdot \mathbb{Z}_n$ кольца $\mathbb{Z}_n$

В $\mathbb{Z}_n$ идеал является **максимальным** тогда, когда m - простой делитель n или $p\mathbb{Z}_n, p|n$.

Доказательство. Предположим, что $p\mathbb{Z} \subseteq I$. Возьмём $x \in I/p\mathbb{Z}$. Тогда p не делит x, значит их НОД (p, x) = 1. По теореме Безу можно найти такое число b и a, что :

$$ap + bx = 1$$

Левая сторона равенства лежит в идеале I, это значит, что и 1 принадлежит I. $\Rightarrow I = \mathbb{Z}$. Значит, $p\mathbb{Z}$ максимальный.

5.9 Условия совпадения подкольца $m \cdot \mathbb{Z}_n$ с кольцом $\mathbb{Z}_n$

Так как $\mathbb{Z}_n$ тоже является подкольцом кольца $\mathbb{Z}_n$, то справедливо:

$$m\mathbb{Z}_n = 1\mathbb{Z}_n \iff \gcd(m, n) = \gcd(1, n) = 1,$$

то есть m и n - взаимно простые числа

5.10 Условия совпадения подкольца $m \cdot \mathbb{Z}_n$ с подкольцом $t \cdot \mathbb{Z}_n$

$$m\mathbb{Z}_n = t\mathbb{Z}_n \Longleftrightarrow \gcd(m,n) = \gcd(t,n)$$

5.11 Условие, при котором кольцо $\mathbb{Z}_n$ является полем

Определение 5.14 *Пусть R - ассоциативное коммутативное кольцо с единицей и $R \neq \{0\}$. Тогда R называется полем, если любой элемент $a \in R \setminus \{0\}$ обратим. По другому это означает, что множество $R \setminus \{0\}$ есть группа относительно умножения.*

Подполем F поля K называется подкольцо $F \subset K$, само являющееся полем.

Теорема 5.15 *Кольцо $\mathbb{Z}_n$ является полем в том случае, когда $n = p, \mathbb{Z}_p$.*

- **Доказательство.** Мы уже доказывали, что элемент $k \in \{1, 2, ..., n-1\}$ обратим в кольце $\mathbb{Z}_n$ тогда и только тогда, когда он взаимно прост с числом n. (**)
  Таким образом, кольцо $\mathbb{Z}_n$ является полем в том и только том случае, когда все числа $k \in \{1, 2, ..., n-1\}$ взаимно просты с числом n. Это, очевидно, выполняется тогда и только тогда, когда n простое.

(**) Действительно, пусть имеется $k \in \{1, 2, ..., n-1\}$ и мы хотим найти к нему обратный элемент. Это означает, что мы хотим найти такое $m \in \{1, 2, ..., n-1\}$, что $km \equiv 1n$, а более подробно — найти такие два числа $m, q \in \mathbb{Z}$, что

$$km + nq = 1$$

это возможно тогда и только тогда, когда числа k и n взаимно просты.

5.12 Гомоморфизм и изоморфизм колец

Определение 5.16 *Пусть R и S - два кольца. Гомоморфизмом из R в S называется такое отображение $f : R \to S$, что $\forall a, b \in R$ выполнено:*

$$f(a+b) = f(a) + f(b) \quad f(a \cdot b) = f(a) \cdot f(b)$$

Если кольца R и S с единицей, то естественно дополнительно потребовать
f(1) = 1. Биективные (сюръективные и инъективные) гомоморфизмы называются изоморфизмами.

Пусть $f : R \to S$ и $g : S \to T$ - гомоморфизмы колец. Тогда $g \circ f : R \to T$ так же гомоморфизм колец. Если f - изоморфизм, то отображение f^{-1} - гомоморфизм (и, следовательно, изоморфизм). Тождественное отображение гомоморфизм.

- Тождественное отображение кольца $R \to R$ есть гомоморфизм колец
- Комплексное сопряжение
- Каноническое отображение $\mathbb{Z} \to \mathbb{Z}/n$
- Гомоморфизм колец $\mathbb{Z}/nm \to \mathbb{Z}/n \cdot \mathbb{Z}/m$ является изоморфизмом,
  если (n,m) = 1
- Если дан элемент $a \in R$, то отображение $R[x] \to R[x]$, переводящее $f(x) \to f(a)$ является гомоморфизмом. Это называется **гомоморфизм подстановки**

Теорема 5.17 *Пусть R - кольцо. Тогда существует единственный гомоморфизм $Z \to R$.*

- **Доказательство.** Пусть $f : \mathbb{Z} \to R$. Тогда
  $f(1) = 1$, но тогда $f(2) = f(1+1) = f(1) + f(1)$. Аналогично для $n \in$ верно $f(n) = 1 + \cdots + 1$ n-раз. Так как $f(-n) = -f(n)$, то для отрицательных чисел тоже нет никакого выбора. Из части про единственность мы уже поняли, как выглядит гомоморфизм.

Прежде всего, эта теорема говорит, что есть единственный способ канонически определить, что такое 'целое число' в произвольном кольце. Теперь в любом кольце мы будем обозначать сумму из n единиц просто как n.

5.13 Ядро гоморфизма. Его свойства

Теорема 5.18 *Пусть R - кольцо. Рассмотрим единственный гомоморфизм $f : \mathbb{Z} \to R$. Тогда Ker(f) - это подгруппа в $\mathbb{Z}$, то есть имеет вид $n\mathbb{Z}$ для некоторого натурального n. Это число n называется характеристикой кольца. (Проще говоря, n - это наименьшее количество единиц, сумма которых равна 0 в R.)*

$$Ker(f) = \{a \in \mathbb{Z} | f(a) = 0\}$$

Ядро - это идеал
Так как $f : (R, +) \to (R', +)$ - гомоморфизм групп, то $Ker(f)$ - подгруппа в (R,+). Если $a \in Ker(f$, т. е. f(a) = 0, $r, s \in R$, то

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0,$$
$$f(as) = f(a)f(s) = 0 \cdot f(s) = 0,$$

итак, $ra \in Ker(f)$, $as \in Ker(f)$, т. е. $Ker(f) \lhd R$.
$Ker(f)(\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}) = (m)$
Любой идеал I является ядром некоторого гомоморфизма, а именно канонического гомоморфизма R/I.
Отметим ряд свойств гомоморфизмов колец $f : R \to R'$

- Гомоморфизм инъективен $\iff$ его ядро нулевое
- Так как f - гомоморфизм абелевых групп $(R, +), (R', +)$, то
  f(0)=0', f(-a)=-f(a).
- Гомоморфизм колец $f : R \to R'$ является изоморфизмом тогда и только тогда, когда $Ker(f) = \{0\}$

5.14 Условие совместности уравнения $ax \equiv b$ в кольце $\mathbb{Z}_n$

В общем случае ответ на вопрос такой:

Теорема 5.19 *Пусть $ax \equiv b \pmod n$ и $\gcd(a, n)$. Если $[x_0]$ модулю $\frac{n}{d}$ - решение такого сравнения:*

$$\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}},$$

Тогда решением $ax \equiv b \pmod n$ будут являться классы вычетов:

$$[x_0]_n,\ [x_0 + \frac{n}{d}]_n,\ [x_0 + 2\frac{n}{d}]_n, \cdots, [x_0 + (d-1)\frac{n}{d}]_n$$

- **Доказательство.** Предположим, что x решение сравнения $ax \equiv b \pmod n$. Это означает - по определению сравнения по модулю - $\exists t \in \mathbb{Z} : nt = ax - b$. Делим почленно на d: $\frac{a}{d}x - \frac{b}{d} = \frac{n}{d}t$, это приводит к сравнению:

  $$\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}},$$

  Так как $\gcd(\frac{n}{d}, \frac{a}{d}) = 1$, то существует единственное решение этого сравнения - x_0 по модулю $\frac{n}{d}$.

  – Нужно показать 2 пункта: что каждый класс вычета по модулю n
  $[c + td], 0 \le t < \frac{n}{d}$ сводится к $[c]_d$, и в обратную сторону - что каждый класс вида $[c]_d$ принадлежит множеству.
  $\Rightarrow$ Первое следует из $c + td \equiv c \pmod d, \forall t \in \mathbb{Z}$, то утверждение верно.
  $\Leftarrow$ Предположим, что $a \equiv c \pmod d$, тогда по определению $a = c + dt, t \in \mathbb{Z}$. Теперь заметим, что изменение t на $\frac{n}{d}$ не меняет $a + n\mathbb{Z}$.

По доказанному выше, $x + n\mathbb{Z}$ должен быть одним из следующих классов вычетов:

$$x_0 + n\mathbb{Z}, x_0 + \frac{n}{d} + n\mathbb{Z}, \cdots, x_0 + \frac{n}{d}(d-1) + n\mathbb{Z}$$

Решение линейного сравнения $ax \equiv b \pmod{n}$ существует тогда и только тогда, когда $gcd(a, n) \mid d$. Взаимная простота является частным случаем и очевидно, что тогда решения нет.

5.15 Неприводимые многочлены над полем. Критерий неприводимости многочленов степени 2 и 3

Определение 5.20 *Пусть $\mathbb{R}[x]$ – кольцо многочленов над кольцом $\mathbb{R}$, многочлен $f(x) \in \mathbb{R}[x]$,*

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

и элемент $c \in \mathbb{R}$. Значением многочлена f (x) в точке c называется элемент

$$f(c) = \sum_{i=0}^{n} a_i c^i \in \mathbb{R}.$$

*Если $f(c) = 0$, то элемент называется с **корнем многочлена** $f(x)$.*

Определение 5.21 *Элемент $p \neq 0, p \notin R^*$ называется неприводимым, если он не раскладывается на множители нетривиальным образом. То есть, для любых $a, b \in \mathbb{R}$: если $ab = p$, то либо a обратим, либо b обратим.*

Теорема 5.22 *Пусть $\mathbb{F}[x]$ – кольцо многочленов над полем F. Многочлен $f(x) \in \mathbb{F}[x]$ степени 2 или 3 неприводим над полем $\mathbb{F}$ тогда и только тогда, когда у него нет корней в поле $\mathbb{F}$.*

- Рассмотрим разложение
$$f(x) = g(x) \cdot h(x),$$
где $g(x), h(x) \in \mathbb{F}[x]$, $\deg g \geq 1, \deg h \geq 1$.
Т.к. степень многочлена f (x) равна 2 или 3, или $\deg g = 1$, или $\deg h = 1$.
Откуда многочлен f (x) **неприводим над полем F** тогда и только тогда когда у него нет корней в этом поле.

5.16 Производная многочлена f(x). Критерий наличия кратных корней

Определение 5.23 *Пусть R - кольцо, а $f \in R[x]$ имеет вид $f(x) = a_0 + \cdots + a_n x^n$. Тогда определим производную как*

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

Все основные свойства производных верны в этом контексте.

Определение 5.24 *Пусть R - область целостности. Будем говорить, что многочлен $f \in R[x]$ имеет $a \in R$ корнем кратности k, если*

$$f \vdots (x-a)^k \quad \& \quad f \nvdots (x-a)^{k+1}$$

Теорема 5.25 *Корень многочлена a является его k-кратным корнем тогда и только тогда, когда он является корнем k - 1 кратности его первой производной.*

- $\Rightarrow$ Пусть a — k-кратный корень многочлена f(x). Необходимо доказать, что a — корень k-1 кратности многочлена f'(x). По определению кратного корня можно записать следующее:

$$f(x) = (x-a)^k f_1(x), f_1(x) \nvdots (x-a)$$

Стоит отметить, что условия $f_1(x) \nvdots (x-a), f(a) \neq 0$ являются эквивалентными по следствию теоремы Безу.
Дифференцируя f(x), получаем:

$$f'(x) = k(x-a)^{k-1} f_1(x) + (x-a)^k f_1'(x)$$

$$f'(x) = (x-a)^{k-1}(k f_1(x) + (x-a) f_1'(x))$$

При этом слагаемое $k f_1(x) + (x-a) f_1'(x) \nvdots (x-a)$, так как в противном случае выполнялось бы условие $f_1(x) \vdots (x-a)$, что противоречит тому, что a — k-кратный корень многочлена.
Следовательно, a — корень k - 1 кратности многочлена f'(x) по определению кратного корня.

- $\Leftarrow$ Теперь пусть a — корень многочлена f(x) и корень k - 1 кратности многочлена f'(x). Тогда можно записать следующее:

$$f(x) = (x-a) f_1(x),$$

$$f'(x) = (x-a)^{k-1} g(x), g(x) \nvdots (x-a)$$

Пусть $k \geqslant 2$. Тогда продифференцируем f(x) и получим:

$$f'(x) = f_1(x) + (x-a) f_1'(x)$$

Учитывая, что $f'(x) \vdots (x-a)$, то и $f_1(x) \vdots (x-a)$, иными словами, многочлен $f_1(x)$ можно представить так:

$$f_1(x) = (x-a) f_2(x)$$

Тогда f(x) представляется в следующем виде:

$$f(x) = (x-a)^2 f_2(x)$$

Теперь продифференцируем f(x) в очередной раз, получим:

$$f'(x) = 2(x-a) f_2(x) + (x-a)^2 f_2'(x)$$

Если k = 2, тогда a — простой корень f'(x), значит $f'(x) \nvdots (x-a)^2$.
Получаем, что $f_2(x) \nvdots (x-a)$, потому a — двукратный корень f(x). Если же $k \geqslant 3$, то $f'(x) \vdots (x-a)^2$, тогда из текущего представления f'(x) видно, что $f_2(x) \vdots (x-a)$, значит $f_2(x)$ можно представить в следующем виде:

$$f_2(x) = (x-a) f_3(x)$$

Откуда f(x) представляется как:

$$f(x) = (x-a)^3 f_3(x)$$

Продолжая такой процесс, получим:

$$f(x) = (x-a)^{k-1} f_{k-1}(x)$$

Дифференцируя f(x), получаем:

$$f'(x) = (k-1)(x-a)^{k-2} f_{k-1}(x) + (x-a)^{k-1} f_{k-1}'(x)$$

По аналогии получаем, что $f_{k-1}(x) \vdots (x-a)$, откуда

$$f_{k-1}(x) = (x-a) f_k(x)$$

Тогда f(x) представляется так:

$$f(x) = (x-a)^k f_k(x)$$

Дифференцируя f(x) ещё раз, получаем следующее:

$$f'(x) = k(x-a)^{k-1} f_k(x) + (x-a)^k f_k'(x)$$

Теперь, если $f_k \vdots (x-a)$, то a — корень $f'(x)$ кратности больше чем k - 1, что противоречит условию. Значит, $f_k(x) \nvdots (x-a)$, тогда a — корень k-кратности, что и требовалось доказать. ■

5.17 Условия, при которых кольцо $\mathbb{F}[x]/f$ является полем

Пусть p — простое число и $f \in \mathbb{Z}_p[x]$ — ненулевой многочлен. Рассмотрим множество:

$$\mathbb{Z}_p[x]/(f) = \{g(x) \in \mathbb{Z}_p[x] | \deg(g) < \deg(f)\}$$

Множество Zp[x]/(f) назовем множеством многочленов из $\mathbb{Z}_p[x]$, приведенных по модулю многочлена f. Отметим, что $\mathbb{Z}_p[x]/(f)$ является множеством всех возможных остатков при делении многочленов из $\mathbb{Z}_p[x]$ на многочлен f.

Теорема 5.26 *Если p — простое число и $f(x) \in \mathbb{Z}_p[x]$ — не постоянный многочлен, то множество $\mathbb{Z}_p[x]/(f)$ с операциями сложения и умножения по модулю многочлена f является коммутативным и ассоциативным кольцом с единицей.*

- **Доказательство.** Проверим свойства кольца.

  1. Множество $\mathbb{Z}_p[x]/(f)$ с операцией сложения является коммутативной группой.
  2. Законы дистрибутивности: если для
     $g_1(x), g_2(x), h(x) \in \mathbb{Z}_p[x]/(f)$ выполняется

     $$\begin{gathered}(g_1(x)+g_2(x))\cdot h(x) = f(x)\cdot q(x) + r(x), \quad \deg(r) < \deg(f),\\ g_1(x)\cdot h(x) = f(x)\cdot q_1(x) + r_1(x) \quad \deg(r_1) < \deg(f),\\ g2(x)\cdot h(x) = f(x)\cdot q_2(x) + r_2(x) \quad \deg(r_2) < deg(f)\end{gathered}$$

     то $r(x) = r_1(x) + r_2(x)$.

Теорема 5.27 *Пусть p — простое число и $f(x) \in \mathbb{Z}_p[x], f(x) \neq const$. Кольцо $\mathbb{Z}_p[x]/(f)$ с операциями сложения и умножения по модулю многочлена f является полем тогда и только тогда, когда f(x) — неприводимый многочлен над полем $\mathbb{Z}_p$.*

- **Доказательство.**

  1. Если f (x) — неприводимый многочлен, то докажем, что кольцо $\mathbb{Z}_p[x]/(f)$ не имеет делителей нуля.
     Если для некоторых многочленов
     $g_1, g_2 \in \mathbb{Z}_p[x]/(f), g_1 \neq 0, g_2 \neq 0$, верно
     $g_1(x)\cdot g_2(x) = 0$ в этом кольце, то $g_1(x)\cdot g_2(x) = f(x)\cdot q(x)$ для какого-то многочлена
     $q \in \mathbb{Z}_p[x]$, чего не может быть.
     Следовательно, в этом случае $\mathbb{Z}_p[x]/(f)$ — конечное целостное кольцо, а значит, поле.
  2. Если f(x) — приводимый многочлен, т. е. $f(x) = f_1(x)\cdot f_2(x)$ для некоторых непостоянных многочленов $f_1, f_2 \in \mathbb{Z}_p[x]$, то покажем, что в кольце $\mathbb{Z}_p[x]/(f)$ нет обратного элемента к элементу $f_1(x)$.
     Если для некоторого многочлена $g \in \mathbb{Z}_p[x]/(f)$ верно $f_1(x)\cdot g(x) = 1$ в этом кольце, то

     $$f_1(x)\cdot g(x) = f(x)\cdot q(x) + 1 = f1(x)\cdot f2(x)\cdot q(x) + 1$$

для какого-то многочлена $q \in \mathbb{Z}_p[x]$. Поэтому в кольце $\mathbb{Z}_p[x]$ обязано выполняться равенство:

$$f_1(x)(g(x) - f_2(x) \cdot q(x)) = 1,$$

чего не может быть.
Следовательно, в этом случае Zp[x]/(f) не является полем.

ИТОГО Если f (x) — неприводимый в кольце $\mathbb{Z}_p[x]$ многочлен, где p — простое число, то кольцо $\mathbb{Z}_p[x]/(f)$ является полем.

6 Кольца. Задачи для тренировки

6.1 Кольцо вычетов

6.1.1 Вычислите количество образующих

1) $(\mathbb{Z}_{31}, \cdot) = ?$ 2) $(\mathbb{Z}_{49}, +) = ?$ 3) $(\mathbb{Z}_{48}, +) = ?$

4) $(\mathbb{Z}_{47}, +) = ?$ 5) $(\mathbb{Z}_{23}, \cdot) = ?$ 6) $(\mathbb{Z}_{17}, \cdot) = ?$

6.1.2 Возведите число в степень по модулю

1) $(\mathbb{Z}_{32}, +) : 9^6 = ?$ 2) $(\mathbb{Z}_{41}, \cdot) : 34^{10} = ?$ 3) $(\mathbb{Z}_{37}, +) : 9^4 = ?$

4) $(\mathbb{Z}_{11}, +) : 7^{12} = ?$ 5) $(\mathbb{Z}^*_{36}, \cdot) : 11^{12} = ?$ 6) $(\mathbb{Z}^*_{32}, \cdot) : 11^2 = ?$

6.1.3 Вычислите порядок элемента

1) $(\mathbb{Z}_7, \cdot) : 4 = ?$ 2) $(\mathbb{Z}_{23}, \cdot) : 16 = ?$ 3) $(\mathbb{Z}_{31}, +) : 23 = ?$

4) $(\mathbb{Z}_{41}, +) : 2 = ?$ 5) $(\mathbb{Z}^*_{26}, \cdot) : 3 = ?$ 6) $(\mathbb{Z}^*_{49}, \cdot) : 36 = ?$

6.1.4 Найдите число решений линейного сравнения

1) $12x \equiv 5 \pmod{15} \Rightarrow ?$ 2) $13x \equiv 20 \pmod{32} \Rightarrow ?$ 3) $4x \equiv 4 \pmod{5} \Rightarrow ?$

4) $12x \equiv 13 \pmod{17} \Rightarrow ?$ 5) $26x \equiv 37 \pmod{47} \Rightarrow ?$ 6) $8x \equiv 2 \pmod{9} \Rightarrow ?$

6.1.5 Решите линейное сравнение

1) $30x \equiv 5 \pmod{35} \Rightarrow ?$ 2) $13x \equiv 9 \pmod{25} \Rightarrow ?$ 3) $10x \equiv 12 \pmod{28} \Rightarrow ?$

4) $7x \equiv 29 \pmod{37} \Rightarrow ?$ 5) $9x \equiv 7 \pmod{11} \Rightarrow ?$ 6) $25x \equiv 35 \pmod{40} \Rightarrow ?$

6.1.6 Найдите число решений квадратичного сравнения по простому модулю

1) $x^2 \equiv 4 \pmod{17} \Rightarrow ?$ 2) $x^2 \equiv 11 \pmod{17} \Rightarrow ?$ 3) $x^2 \equiv 5 \pmod{41} \Rightarrow ?$

4) $x^2 \equiv 4 \pmod{7} \Rightarrow ?$ 5) $x^2 \equiv 7 \pmod{11} \Rightarrow ?$ 6) $x^2 \equiv 9 \pmod{11} \Rightarrow ?$

6.1.7 Решите квадратичные сравнения по простому модулю

1) $x^2 \equiv 7 \pmod{11} \Rightarrow ?$ 2) $x^2 \equiv 9 \pmod{17} \Rightarrow ?$ 3) $x^2 \equiv 41 \pmod{43} \Rightarrow ?$

4) $x^2 \equiv 11 \pmod{17} \Rightarrow ?$ 5) $x^2 \equiv 37 \pmod{43} \Rightarrow ?$ 6) $x^2 \equiv 23 \pmod{43} \Rightarrow ?$

6.1.8 Найдите число решений квадратичного сравнения по составному модулю

1) $x^2 \equiv 12 \pmod{14} \Rightarrow ?$ 2) $x^2 \equiv 13 \pmod{15} \Rightarrow ?$ 3) $x^2 \equiv 3 \pmod{26} \Rightarrow ?$

4) $x^2 \equiv 5 \pmod{32} \Rightarrow ?$ 5) $x^2 \equiv 6 \pmod{8} \Rightarrow ?$ 6) $x^2 \equiv 23 \pmod{26} \Rightarrow ?$

6.1.9 Решите квадратичные сравнения по составному модулю

1) $x^2 \equiv 5 \pmod{10} \Rightarrow ?$ 2) $x^2 \equiv 2 \pmod{38} \Rightarrow ?$ 3) $x^2 \equiv 6 \pmod{16} \Rightarrow ?$

4) $x^2 \equiv 4 \pmod{10} \Rightarrow ?$ 5) $x^2 \equiv 8 \pmod{12} \Rightarrow ?$ 6) $x^2 \equiv 30 \pmod{32} \Rightarrow ?$

6.1.10 Выполните операции над матрицами:

1) $\mathbb{Z}_{43}: \begin{pmatrix} 33 & 42 \\ 36 & 36 \\ 8 & 34 \end{pmatrix} + \begin{pmatrix} 37 & 35 \\ 30 & 4 \\ 0 & 3 \end{pmatrix} = ?$

2) $Z_{53}: \begin{pmatrix} 29 & 12 & 25 & 26 \\ 37 & 40 & 13 & 49 \end{pmatrix} - \begin{pmatrix} 10 & 24 & 18 & 37 \\ 52 & 1 & 46 & 43 \end{pmatrix} = ?$

3) $\mathbb{Z}_{35}: \begin{pmatrix} 6 & 31 \\ 21 & 12 \end{pmatrix} \cdot \begin{pmatrix} 26 & 5 \\ 25 & 8 \end{pmatrix} = ?$

4) $\mathbb{Z}_{44}: \begin{pmatrix} 11 & 15 \\ 22 & 1 \\ 4 & 0 \end{pmatrix} + \begin{pmatrix} 13 & 34 \\ 36 & 24 \\ 22 & 1 \end{pmatrix} = ?$

5) $\mathbb{Z}_{47}: \begin{pmatrix} 18 & 17 & 38 \\ 45 & 21 & 45 \end{pmatrix} - \begin{pmatrix} 44 & 36 & 46 \\ 32 & 16 & 26 \end{pmatrix} = ?$

6) $\mathbb{Z}_2: \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = ?$

6.1.11 Вычислите детерминант матрицы:

1) $\mathbb{Z}_{61}: \begin{vmatrix} 57 & 10 & 22 \\ 2 & 47 & 40 \\ 54 & 42 & 40 \end{vmatrix} = ?$

2) $Z_{42}: \begin{vmatrix} 29 & 6 & 31 & 24 \\ 21 & 4 & 12 & 26 \\ 30 & 12 & 4 & 35 \\ 22 & 25 & 1 & 37 \end{vmatrix} = ?$

6.2 Кольцо многочленов

6.2.1 Найдите сумму многочленов:

1) $\mathbb{Z}_{34}: (22x^5 + 6x^4 + 16x^3 + 30x + 29) + (21x^4 + 6x^3 + 17x^2 + 23x + 12) = ?$

2) $Z_{48}: (14x + 11) + (22x + 20) = ?$

3) $Z_{43}: (15x^3 + 27x^2 + 36x + 28) + (3x^2 + 7x + 21) = ?$

4) $Z_{21}: (3x^2 + 13x + 3) + (13x^4 + 3x^3 + 7x^2 + 2x + 10) = ?$

6.2.2 Найдите разность многочленов:

1) $\mathbb{Z}_{29}: (27x^5 + 18x^4 + 12x^3 + 2x^2 + 15x + 12) - (28x^3 + 27x^2 + 17x + 12) = ?$

2) $Z_7: (6x^5 + 2x^4 + 3x^2 + 1) - (3x^5 + 5x^4 + 3x^3 + 2x^2 + 6x + 2) = ?$

3) $Z_{42}: (15x + 36) - (x^3 + 40x^2 + 32x + 12) = ?$

4) $\mathrm{Z}_{51} : (32x^4 + 4x^3 + 46x^2 + 13x + 49) - (11x^2 + 11x + 46) = ?$

6.2.3 Найдите произведение многочленов:

1) $\mathbb{Z}_{47} : (43x^4 + 6x^3 + 9x^2 + 27x + 45) \cdot (27x^2 + 12x + 3) = ?$

2) $\mathrm{Z}_{10} : (2x^4 + 8x^3 + x^2 + 7x + 2) \cdot (2x^3 + 4x^2 + 6x + 1) = ?$

3) $\mathrm{Z}_{30} : (3x^4 + 11x^3 + 5x^2 + 3x + 19) \cdot (5x^5 + 22x^4 + 13x^3 + 7x^2 + 28x + 11) = ?$

4) $\mathrm{Z}_{58} : (36x^2 + 47x + 28) \cdot (40x + 26) = ?$

7 Кольца. Задачи на доказательство

В следующих задачах все кольца предполагаются коммутативными.

1) Пусть A - кольцо с $1 \neq 0$, S - его мультипликативное подмножество, не содержащее 0. Пусть, далее, μ - максимальный элемент в множестве идеалов кольца A, пересечение которых с S пусто. Показать, что μ - простой.

2) Пусть A - кольцо и μ - простой идеал. Показать, что A_μ имеет единственный максимальный идеал, состоящий из всех элементов вида as, где $a \in \mu$, $s \notin \mu$.

3) Пусть A - кольцо главных идеалов, S - его мультипликативное подмножество. Показать, что $S^{-1}A$ - кольцо главных идеалов.

4) Пусть A - факториальное кольцо, S - его мультипликативное подмножество. Показать, что $S^{-1}A$ - факториально и что простые элементы в $S^{-1}A$ - это те простые p из A, для которых $(p) \cap S$ пусто.

5) Пусть i - комплексное число $\sqrt{-1}$. Показать, что $Z[i]$ - кольцо главных идеалов и, следовательно, факториально. Каковы в нем единицы?

6) Пусть A - кольцо целых функций на комплексной плоскости. Показать, что всякий конечно порожденный идеал в A является главным. Каковы главные простые идеалы в A. Каковы единицы в A? Показать, что A не факториально.

8 Кольца. Задачи с решениями

Задача № 1. Вычислить $2^{100}(mod 7)$.

Решение. Вычисляя последовательные степени числа 2, находим, что $2^3 = 1(mod 7)$, т.е. мультипликативный порядок числа 2 в кольце $\mathbb{Z}_7$ равен 3. После этого будем иметь: $2^{100} = 2^{3 \cdot 33 + 1} = (2^3)^{33} \cdot 2 = 2(mod 7)$.

Ответ: 2.

Задача № 2. Решить в кольце $\mathbb{Z}_{23}$ уравнение: $10 \cdot x = 9$.

Решение. Так как НОД(10,23)=1, то число 10 обратимо в $\mathbb{Z}_{23}$. Поэтому для нахождения x следует вначале найти число 10^{-1}, после чего искомое решение будет вычислено по формуле: $x = 10^{-1} \cdot 9(mod 23)$. Для нахождения 10^{-1} используем алгоритм Евклида:

$$(a = 23) = 2 \cdot (b = 10) + (r_1 = 3),$$

$$b = 3 \cdot r_1 + (r_2 = 1).$$

Отсюда находим представление единицы в виде линейной комбинации исходной пары взаимно простых чисел a=23 и b=10:

$$1 = b - 3 \cdot r_1 = b - 3 \cdot (a - 2 \cdot b) = 7b - 3a = 7 \cdot 10 - 3 \cdot 23.$$

Отсюда $10^{-1} = 7(mod 23)$. Следовательно, $x = 7 \cdot 9 = 17(mod 23)$.

Ответ: x=17.

Задача № 3. Разрешимо ли уравнение $3 \cdot x = 7$ в кольце $\mathbb{Z}_{12}$?

Решение. Так как значение правой части уравнения не делится на величину НОД(12,3)=3, то уравнение не имеет решений.

Ответ: нет решений.

Задача № 4. Сколько решений имеет уравнение $18x = 6$ в кольце $\mathbb{Z}_{30}$?

Решение. Так как правая часть уравнения делится на величину НОД(18,30)=6, то уравнение разрешимо в кольце $\mathbb{Z}_{30}$, при этом число решений совпадает с числом решений однородного уравнения 18x=0 (mod 30), которое имеет ровно НОД(18,30)=6 решений в кольце $\mathbb{Z}_{30}$.

Ответ: 6 решений.

Задача № 5. Решить уравнение 11x=7 в кольце $\mathbb{Z}_{60}$.

Решение. Учитывая возможность разложения кольца $\mathbb{Z}_{60}$ в прямое произведение колец

$$\mathbb{Z}_{60} = \mathbb{Z}_3 * \mathbb{Z}_4 * \mathbb{Z}_5,$$

заключаем, что каждому решению исходного уравнения соответствует единственное решение системы уравнений

$$\begin{cases} 2x = 1(mod 3) \\ 3x = 3(mod 4) \\ x = 2(mod 5) \end{cases}$$

или

$$\begin{cases} x = 2(mod 3) \\ x = 1(mod 4) \\ x = 2(mod 5) \end{cases}$$

Отсюда по китайской теореме об остатках решение исходного уравнения может быть вычислено по формуле

$x = 1 \cdot 3 \cdot 5 \cdot [(3^{-1} \cdot 5^{-1})(mod 4)] + 2 \cdot 4 \cdot 5 \cdot [(4^{-1} \cdot 5^{-1})(mod 3)] + 2 \cdot 4 \cdot 3 \cdot [(4^{-1} \cdot 3^{-1})(mod 5)] = 15 \cdot 3 + 40 \cdot 2 + 24 \cdot 3 = 45 + 80 + 72 = 17(mod 60)$.

Ответ: x=17.

Задача № 6. Сколько решений имеет уравнение $x^2 - 1 = 0$ в кольце $\mathbb{Z}_{60}$?

Решение. Непосредственной проверкой легко проверить, что данное уравнение имеет по два решения в каждом из колец Z3, Z4 и Z5. Отсюда, учитывая разложение

$$\mathbb{Z}_{60} = \mathbb{Z}_3 \cdot \mathbb{Z}_4 \cdot \mathbb{Z}_5,$$

получаем, что в кольце $\mathbb{Z}_{60}$ исходное уравнение имеет 2*2*2=8 решений.

Ответ: 8 решений.

Задача № 7. Найти мультипликативный порядок числа 7 в кольце $\mathbb{Z}_{60}$.

Решение. Так как $\mathbb{Z}_{60} = \mathbb{Z}_3 \cdot \mathbb{Z}_4 \cdot \mathbb{Z}_5$, то

$$ord(7)_{mod60} = \text{НОК}\{ord(7)_{mod3}, ord(7)_{mod4}, ord(7)_{mod5}\} = (1, 2, 4) = 4.$$

Ответ: 4.

Задача № 8. Найти остаток от деления многочлена $f(x) = x^{100} + 1, f(x) \in \mathbb{F}_7[x]$ на многочлен x-2.

Решение. По теореме Безу остаток r(x) от деления многочлена f(x) на многочлен x-2 равен значению многочлена f(x) в точке x=2. Отсюда: $r(x) = f(2) = 2^{100} + 1(mod7) = (2^3)^{33}2 + 1 = 2 + 1 = 3(mod7)$.

Ответ: 3.

Задача № 9. Является ли кольцо $\mathbb{F}_2[x]/x2 + 1$ полем?

Решение. Кольцо $\mathbb{F}_q[x]/f(x)$ является полем в том и только том случае, когда многочлен f(x) неприводим над полем $\mathbb{F}_q$. Так как в кольце $\mathbb{F}_2[x]$ справедливо равенство $x^2+1 = (x+1)^2$, то кольцо $\mathbb{F}_2[x]/x2+1$ не является полем.

Ответ: нет.

Задача № 10. Имеет ли многочлен $f(x) = x^{17}+2x+1, f(x) \in \mathbb{F}_{17}[x]$ кратные корни в поле разложения?

Решение. Производная многочлена f(x) равна $f'(x) = 17x^{16} + 2 = 2$. Так как НОД(f(x), f'(x))=1, то у многочлена f(x) кратных корней нет.

Ответ: нет.

Задача № 11. Решить в кольце $\mathbb{F}_3[x]/x^3 + 1$ уравнение: $f(x)(x^2 + 1) = 1$.

Решение. Используя алгоритм деления с остатком, имеем:

$$(a = x^3 + 1) = x(b = x^2 + 1) + (r_1 = 2x + 1),$$

$$b = (2x + 2)r_1 + 2.$$

Отсюда получаем, что НОД($x^2 + 1$, $x^3 + 1$)=1, и, следовательно, уравнение имеет в кольце $\mathbb{F}_3[x]/x^3 + 1$ единственное решение $f(x) = (x^2 + 1)^{-1}$.

Для вычисления $(x^2 + 1)^{-1}$ необходимо на основе приведенных выше результатов деления с остатком представить наибольший общий делитель многочленов $x^2 + 1$ и $x^3 + 1$ в виде их линейной комбинации

$$1 = ((2^{-1})_{mod3} = 2)b - (x + 1)r_1 = 2b - (x + 1)(a - xb) = -(x + 1)a + (2 + x + x^2)b.$$

Отсюда $(x^2 + 1)^{-1} = x^2 + x + 2$.

Ответ: $f(x) = x^2 + x + 2$.

Задача № 12. Найти мультипликативный порядок многочлена x-4 в кольце $\mathbb{F}_5[x]/(x-1)(x-2)(x-3)$.

Решение. Так как многочлены x-1, x-2, x-3 попарно взаимно просты, то справедливо разложение кольца $\mathbb{F}_5[x]/(x-1)(x-2)(x-3)$ в прямое произведение колец $\mathbb{F}_5[x]/x-b, b = 1, 2, 3$. Отсюда мультипликативный порядок многочлена x-4 в кольце $\mathbb{F}_5[x]/(x-1)(x-2)(x-3)$ равен наименьшему общему кратному порядков этого многочлена в кольцах $\mathbb{F}_5[x]/x-b, b = 1, 2, 3$. Имеем

$$ord(x-4)_{mod(x-1)} = ord(-3)_{mod(5)} = 4,$$

$$ord(x-4)_{mod(x-2)} = ord(-2)_{mod(5)} = 4,$$

$$ord(x-4)_{mod(x-3)} = ord(-1)_{mod(5)} = 2$$

Отсюда получаем

$$ord(x-4) = (4, 4, 2) = 4.$$

Ответ: 4.

Задача № 13. Найти мультипликативный порядок многочлена $x^2 + x + 1$ в кольце $\mathbb{F}_2[x]/x^3 + x + 1$.

Решение. Многочлен $x^3 + x + 1$ неприводим над полем F_2, следовательно, кольцо $F_2[x]/x^3 + x + 1$ является полем. Так как число элементов в данном поле равно $2^3 = 8$, то мультипликативный порядок любого ненулевого элемента в нем является делителем числа $2^3 - 1 = 7$. Многочлен $x^2 + x + 1$ отличен от единичного элемента поля, значит, его порядок равен 7.

Ответ: 7.

Задача № 14. Найти период многочлена $f(x) = x^2 + 1, f(x) \in F_3[x]$.

Решение. Непосредственной проверкой убеждаемся в том, что многочлен f(x) не имеет корней в поле F_3=0,1,2, следовательно, он неприводим над данным полем. В таком случае период многочлена f(x) будет делителем числа $3^2 - 1 = 8$ ненулевых элементов поля $F_3[x]/x^2 + 1$. Далее непосредственной проверкой получаем:

$$x \neq 1(mod\ x^2 + 1),$$

$$x2 \neq 1(mod\ x^2 + 1),$$

$$x4 = x2 \cdot x^2 = (-1)(-1) = 1(mod\ x^2 + 1).$$

Таким образом, период данного многочлена равен 4.

Ответ: w(f)=4.

Задача № 15. Найти период многочлена $f(x) = x^5 + x + 1$ принадлежит $F_2[x]$.

Решение. Разложение многочлена на неприводимые множители имеет вид:

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

следовательно, период многочлена $f(x) = x^5 + x + 1$ равен наименьшему общему кратному периодов его множителей:

$$w(x^2 + x + 1) = 3,$$

$$w(x^3 + x^2 + 1) = 7,$$

$$w(f(x)) = \text{НОК}(3, 7) = 21.$$

Ответ: w(f)=21.

Задача № 16. Найти период многочлена $f(x) = (x^2 + x + 1)^{10}(x^3 + x^2 + 1)^{20}$ принадлежит $F_2[x]$.

Решение. Многочлены $x^2 + x + 1$ и $x^3 + x^2 + 1$ являются неприводимыми, и их периоды равны сответственно 3 и 7. Далее, наименьшее целое t такое, что $2t \geq max\{10, 20\}$, равно t=5. Отсюда

$$w(f) = 25\text{НОК}(3, 7) = 32 \cdot 21.$$

Ответ: $w(f) = 32 \cdot 21$.

Задача № 17. Найти мультипликативный порядок многочлена g(x) в кольце $F_q[x]/f(x)$

Пример: g=x, q=3, f=(x+1)(x+2).

Решение. Так как многочлены x+1 и x+2 взаимно просты, то кольцо $F_q[x]/f(x)$ изоморфно декартову произведению колец $F_q[x]/x+1$ и $F_q[x]/x+2$. При этом любое кольцо вида $F_q[x]/x+b$ совпадает с полем F_q. При указанном изоморфизме многочлен g=x соответствует вектору $(x_{mod(x+1)}, x_{mod(x+2)}) = (2, 1)$. Отсюда

$$ord(x) = \text{НОК}(ord(2), ord(1)) = \text{НОК}(2, 1) = 2.$$

Ответ: ord(x)=2.

Задача № 18. Найти мультипликативный порядок элемента a в кольце Z_n

Пример: a=23, n=420.

Решение. Так как $420 = 3 \cdot 4 \cdot 5 \cdot 7$, то имеет место изоморфизм кольцаZ_{420} декартову произведению

$$Z_{420} \approx Z_3 \cdot Z_4 \cdot Z_5 \cdot Z_7$$

Тогда мультипликативный порядок элемента a=23 в кольце Z_{420} равен наименьшему общему кратному порядков этого элемента в кольцах Z_3, Z_4, Z_5 и Z_7 , т.е.

$$ord(a) = \text{НОК}(r_1, r_2, r_3, r_4),$$

где

$$r_1 = ord(a_{mod3}) = ord(2) = 2$$
$$r_2 = ord(a_{mod4}) = ord(3) = 2$$
$$r_3 = ord(a_{mod5}) = ord(3) = 4$$
$$r_4 = ord(a_{mod7}) = ord(2) = 3$$

Примечание: При вычислении величин r_j число a=23 рассматривается как элемент соответствующей компоненты разложения (т.е. кольца Z_3, Z_4, Z_5, Z_7)

Отсюда получаем ord(23)=НОК(2,2,4,3)=12

Ответ: 12.

Задача № 19. Является ли кольцо $K = F_q[x]/f(x)$ полем?

Пример: q=2, $f = x^2 + x + 1$.

Решение. Кольцо $K = F_q[x]/f(x)$ является полем. Многочлен f(x) неприводим над полем F_q. Многочлен $f = x^2 + x + 1$ неприводим над полем F_2, так как у него нет корней в поле F_2 и его степень равна 2.

Ответ: рассматриваемое кольцо является полем.

Задача № 20. Обратим ли многочлен g(x) в кольце $F_q[x]/f(x)$?

Пример: g(x)=x-4, q=5 (т.е. $F_q = Z_5$), f(x)=(x-1)(x-2)(x-3)

Решение. Многочлен g(x) обратим в кольце $F_q[x]/f(x)$, НОД(g(x),f(x))=1. В нашем случае многочлен g(x)=x-4 взаимно прост с многочленом f(x)=(x-1)(x-2)(x-3), так как корень x=4 многочлена g(x) не является корнем многочлена f(x). Значит, НОД(g(x),f(x))=1 и многочлен g(x) обратим.

Ответ: обратим.

Задача № 21. Сколько решений имеет уравнение $a \cdot x = b$ в кольце Z_n?

Пример № 1: 18x=6 в кольце Z_{30}.

Решение. Уравнение $a \cdot x = b$ имеет в кольце Z_n решения b=0 (mod(НОД(a,n)), т.е.когда правая часть уравнения делится на НОД(a,n). При этом (в случае совместности) число решений совпадает с числом решений однородного уравнения $a \cdot x = 0$ (mod(n)) и равно НОД(a,n). В нашем случае НОД(18,30)=6 и правая часть делится на 6. Значит, уравнение имеет 6 решений в кольце Z_{30}.

Ответ: 6 решений.

Пример № 2: $x^2 - 1 = 0$ в кольце Z_{60}.

Решение. Так как имеет место изоморфизм кольца Z_{60} и прямого произведения колец Z_3, Z_4 и Z_5

$$Z_{60} \approx Z_3 \cdot Z_4 \cdot Z_5$$

то число решений исходного уравнения в кольце Z_{60} равно произведению чисел решения этого уравнения в каждой из компонент разложения. Непосредственной проверкой легко проверить, что данное уравнение имеет по два решения в каждом из колец Z_3, Z_4 и Z_5. Отсюда получаем, что в кольце Z_{60} исходное уравнение имеет $2 \cdot 2 \cdot 2 = 8$ решений.

Ответ: 8 решений.

Задача № 22. Найти число решений уравнения $a \cdot f(x) = b$ в кольце $F_q[x]/g(x)$

Пример: a=x+1, b=x, q=2, $g = x^3 + x + 1$

Решение. Уравнение $a \cdot f(x) = b$ совместно в кольце $F_q[x]/g(x)$, правая часть делится без остатка на НОД(a,g), т.е. b=0(mod(НОД(a,g)). Так как у многочлена $g = x^3 + x + 1$ нет корней в поле $F_q = F_2$ и его степень равна 3, то этот многочлен неприводим над полем F_2 и кольцо $F_q[x]/g(x)$ является полем. Так как НОД(a,g)=1, то указанное уравнение в поле $F_2[x]/g(x)$ будет иметь одно решение ($f(x) = a^{-1}b$).

Ответ: одно решение.

Задача № 23. Найти число мультипликативно-обратимых элементов кольца Z_n.

Пример: Z_{60}

Решение (1 способ). Так как $Z_{60} \approx Z_3 \cdot Z_4 \cdot Z_5$, то число мультипликативно обратимых элементов в кольце Z_{60} равно f(60)=f(3)f(4)f(5)=$2 \cdot 2 \cdot 4$=16.

Решение (2 способ). Через Z_n^* обозначим множество всех мультипликативно обратимых элементов кольца Z_n. Тогда $|Z_n^*| = f(n)$, где f(n) – функция Эйлера.

В нашем случае $|Z_n^*| = f(n) = f(60) = f(3 \cdot 4 \cdot 5) = f(3) \cdot f(4) \cdot f(5) = 2 \cdot 2 \cdot 4 = 16$

Ответ: 16.

Задача № 24. Найти число необратимых элементов в кольце $K = F_2[x]/f(x)$, $f(x) = x^4 + 1$.

Решение. Так как $x^4 + 1 = (x + 1)^4$, то в K необратимые элементы имеют вид: $g(x) = (x + 1) \cdot h(x)$, $deg(h) \leq 2$. Число таких многочленов равно 8.

Ответ: 8.

Задача № 25. Найти число мультипликативно обратимых элементов в кольце $F_q[x]/f(x)$.

Пример: $F_q = Z_5$, f(x)=(x-1)(x-2)(x-3)

Решение. Имеет место изоморфизм колец

$$Z_5[x]/f(x) \approx Z_5[x]/(x-1) \ \cdot \ Z_5[x]/(x-2) \ \cdot \ Z_5[x]/(x-3)$$

Тогда число мультипликативно обратимых элементов в исходном кольце равно произведению чисел обратимых элементов в каждом из колец разложения.

Так как каждое из колец $Z_5[x]/x-b$ является полем Z_5, в котором имеется ровно 4 обратимых элемента, то число обратимых элементов в исходном кольце составит $4 \cdot 4 \cdot 4 = 64$ элемента.

Ответ: 64.

Задача № 26. Указать характеристику кольца $K \in \{Z_n, Z_q[x]/f(x), m \cdot Z_n\}$, q-простое.

Решение. Характеристика кольца Z_n равна n. Характеристика кольца $Z_q[x]/f(x)$ равна q т.е. совпадает с характеристикой кольца $Z_q[x]$ и кольца Z_q. Пусть НОД(m,n)=d. Так как $m \cdot Z_n = \text{НОД}(m, n) \cdot Z_n = \{0, d, 2d, \ldots, (n/d - 1)d\} \rightarrow char = n/\text{НОД}(m, n)$.

9 Конечные поля

9.1 Теоретическое введение

- $\mathbb{Z}$ — кольцо целых чисел евклидово (целостное унитальное + возможно деление с остатком $\Rightarrow$ существование НОД!),
- p — простое число
- $(p) = \{np \mid n \in \mathbb{Z}\} = p\mathbb{Z} = \{0, \pm p, \pm 2p, ...\}$ — идеал
- $\mathbb{Z}/(p) = \{\bar{0}, \bar{1}, \cdots, \overline{p-1}\}$ — кольцо вычетов по модулю этого идеала = классы остатков от деления на p:

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

  Черту над символами классов вычетов часто не ставят.

- Поскольку p — простое, то $\mathbb{Z}/(p)$ — не просто кольцо, а **поле** (возможно деление без остатка на любой ненулевой элемент). Это ***простейшее поле Галуа***, обозначается как $\mathbb{F}_p$ или $GF(p)$; все операции в нём совершаются по модулю p.

Теорема 9.1 *В поле характеристики $p > 0$ выполнено тождество:*

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

Доказательство. В любом коммутативном кольце верна формула для бинома:

$$(a+b)^p = a^p + C_p^1 a^{p-1} b + ... + C_p^{p-1} a b^{p-1} + b^p$$

Но при $i = 1, ..., p-1$ числитель коэффициента $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p, а знаменатель — нет.
$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F} \setminus \{0\}$ - **мультипликативная группа поля** $\mathbb{F}_p$

- $\mathbb{F}_p^*$ — циклическая группа порядка $p-1$ по умножению.
- Как конечная циклическая группа, F_p^* содержит генератор = примитивный элемент α:
  - любой элемент $\beta \in F_p$ является некоторой его натуральной степенью: $\beta = \alpha^i, i \in \{1, ..., p-1\}$;
  - причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

Функция Эйлера
$\varphi(n)$ - функция Эйлера — количество чисел из интервала $[1, ..., n-1]$, взаимно простых с n.

- $\varphi(n) \leqslant n-1 \quad \& \quad \varphi(p) = p-1$;
- $\varphi(n^m) = n^{m-1}\varphi(n) \quad \Rightarrow \quad \varphi(p^m) = p^{m-1}(p-1)$;
- $\varphi(m^n) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)} \ : \ d = \gcd(m,n)$
  откуда: если m и n взаимно просты, то
  $\varphi(mn) = \varphi(m)\varphi(n)$ ($\varphi(\cdot)$ — мультпликативная функция).

Примитивные элементы поля $\mathbb{F}_p$
Если примарное разложение $(p-1)$ известно - элемент $\alpha \in \mathbb{F}_p$ будет примитивным, if $\alpha^k \not\equiv_p 1$, для каждого делителя k числа $p-1$.

9.2 Ограничения на количество элементов поля GF(q)

Если $f(x)$ — неприводимый в кольце $\mathbb{Z}_p[x]$ многочлен, где p — простое число, то кольцо $\mathbb{Z}_p[x]/(f)$ является полем.
Элементы этого поля — всевозможные остатки при делении на многочлен f(x).
Пусть $\deg(f) = n$, т. е.

$$f(x) = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$$

Тогда при делении на *f(x)* каждый остаток *g(x)* имеет вид:

$$g(x) = \sum_{j=0}^{n-1} b_j x^j$$

где $b_0, b_1, \cdots, b_{n-1}$ — какие-то элементы поля $\mathbb{Z}_p$. Когда коэффициенты $b_0, b_1, \cdots, b_{n-1} \in \mathbb{Z}_p$ пробегают все свои возможные значения, мы получаем все возможные остатки при делении на многочлен *f(x)*. Возможных остатков найдется p^n. А значит, столько же элементов в поле $\mathbb{Z}_p[x]/(f)$.
Пример. Построим поле из $4 = 2^2$ элементов. В кольце $\mathbb{Z}_2[x]$ многочлен $f(x) = x^2+x+1$ — неприводим. Элементами поля $\mathbb{Z}_2[x]/(f)$ являются остатки при делении на $f(x)$:

$$0,\ 1,\ x,\ x+1,$$

где 0 — нулевой и 1 — единичный элементы.

9.3 Характеристика поля $GF(q)$

Характеристика каждого конечного поля является простым числом. Пусть $\mathbb{F}$ — конечное поле. Тогда оно состоит из p^n элементов, где p — характеристика поля $\mathbb{F}$, а натуральное число n — степень поля $\mathbb{F}$ над его простым подполем.
Согласно теореме о существовании и единственности конечных полей, для каждого простого числа p и натурального числа n существует конечное поле из p^n элементов и любое конечное поле из $q = p^n$ элементов изоморфно полю разложения многочлена $x^q - x$ над полем $\mathbb{F}_p$. Данная теорема позволяет говорить о вполне определённом поле данного порядка q (то есть о поле Галуа из q элементов).
Пример. Построим поле из $4 = 2^2$ элементов. В кольце $\mathbb{Z}_2[x]$ многочлен $f(x) = x^2+x+1$ — неприводим. Элементами поля $\mathbb{Z}_2[x]/(f)$ являются остатки при делении на $f(x)$, $(GF(4)) = 2$

9.4 Описание подполей $GF(q)$. Простые поля

$GF(q_1) \subset GF(q_2) \iff \exists k : q_2 = (q_1)^k$

Определение 9.2 *Поле, не имеющее подполей, отличных от него самого, называется* ***простым****.*

Примерами простых полей могут служить поле рациональных чисел и поля вычетов по простому модулю p.
$\mathbb{F}_p$ является простым полем. Действительно, всякое подполе F_p вместе с мультипликативной единицей 1 обязано содержать также элементы $1+1,\ 1+1+1,$ ..., т. е. совпадать с $\mathbb{F}_p$.

9.5 Алгебраические элементы поля над заданным подполем

Поле K называется *расширением* поля κ, если выполнено $\kappa \subset K$.

Определение 9.3 *Пусть $\kappa \subset K$ - расширение полей. Элемент $\alpha \in K$ называется* ***алгебраическим****, если :*
$\exists p(x) \in \kappa, p \neq 0\ :\ p(\alpha) = 0.$
Иначе α называется ***трансцендентным*** *над κ.*

Примеры.

- Числа $\sqrt{2}, \sqrt{3} \in \mathbb{R}$ алгебраичны над $\mathbb{Q}$, они суть корни многочленов x^2-2 и x^2-3 соответственно. Число $\alpha = \sqrt{2}+\sqrt{3}$ так же алгебраично. Чтобы это заметить, напишем:

$$\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6},\ (\alpha^2 - 5)^2 = 24,$$

  значит α обнуляет многочлен вида $(x^2-5)-24$

- $GF(4) = \mathbb{F}_2[y]/y^2+y+1 = \{0, 1, y, y+1\} \to$ y + 1 является корнем многочлена $g(x) = x^2+x+1$:

$$(y+1)^2 + y + 1 + 1 = y^2 + y + 1 = 0 \to (y+1)$$

  - алгебраический элемент поля $GF(4)$ над полем $\mathbb{F}_2$.

9.6 Минимальный многочлен алгебраического элемента и его свойства

Определение 9.4 *Пусть α - алгебраический над к элемента в K. Минимальным многочленом α над к называется ненулевой многочлен $f \in \kappa[x]$ минимальной степени такой, что $f(\alpha) = 0$. ($g(x) \in GF(q)[x]$ - минимальный, если он нормированный и имеет минимальную степень среди всех многочленов, имеющих α в качестве корня). Степенью алгебраического элемента называется степень его минимального многочлена, обозначение:* $\deg \alpha$ *или* $\deg_\kappa \alpha$.

Все многочлены, равные нулю на α, кратны минимальному многочлену.
Пример. Пусть $\alpha \in \mathbb{C}$ - первообразный корень степени 6 из единицы, тогда α обнуляет многочлен $x^6 - 1$. Разложим:

$$x^6 - 1 = (x^3-1)(x^3+1) = (x^3-1)(x+1)(x^2-x+1),$$

видим, что α обнуляет $x^2 - x + 1$. Так как $\alpha \notin \mathbb{Q}$, это и есть минимальный многочлен, и $\deg \alpha = 2$.
Свойства

- $g(x)$ - неприводимый
- $g(\alpha) = 0 \iff f(x) \equiv 0 \pmod{g(x)}$

9.7 Простые расширения $K(\omega)$ поля K, образующим элементом которых является некоторый корень ω неприводимого многочлена $g(x) \in K[x], g(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_nx^n$

Используя неприводимые многочлены, можно строить новые конечные поля — расширения простых полей $\mathbb{F}_p$:

- Выбираем простое p и фиксируем поле:

$$\mathbb{F}_p = \langle\ \{\bar{0},\ \bar{1},\ ...,\ \overline{p-1},\ +_p,\ \cdot_p\}\ \rangle$$

- Рассматриваем кольцо $\mathbb{F}_p[x]$ многочленов над ним
- Выбираем натуральное n и неприводимый многочлен

$$P(x) = a_nx^n + ... + a_1x + a_0 \in \mathbb{F}_p[x]$$

- Идеал $(P(x))$ порождает факторможество $\mathbb{F}_p[x]/(P(x))$, элементы которого суть совокупность $\{R(x)\}$ остатков от деления многочленов $f \in \mathbb{F}_p[x]$ на P (x):

$$f(x) = Q(x) \cdot P(x) + \mathbf{R(x)}$$

Множество $\{R(x)\}$ является полем Галуа $GF(p^n)$.

- **Доказательство.** Кольцо многочленов $\mathbb{F}_p[x]$ евклидово, идеал $(P(x))$ — максимальный $\Rightarrow \{R(x)\}$ — поле.
  Его мощность $|\{R(x)\}|$ = число многочленов над $\mathbb{F}_p$ степени не выше $n-1$, т.е. $|\{R(x)\}| = p^n$.

Поле $\{R(x)\} = GF(p^n)$ называется расширением n-й степени поля $\mathbb{F}_p$;
альтернативное обозначение — F_p^n .
Любое конечное поле изоморфно какому-нибудь полю Галуа F_p^n.
Пример. Выберем неприводимый многочлен в $\mathbb{F}_3[x] : x^2+1$. Искомое поле есть:

$$\begin{aligned}\mathbb{F}_3^2 &\cong \mathbb{F}_3[x]/(x^2+1)\\ &= \{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}.\end{aligned}$$

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

$$\begin{array}{ll}(x+1)+(x+2)=2x, & (x)\cdot(2x)=1,\\ (2x+1)+x=1, & (2x+1)\cdot x = x+1,\end{array}$$

Заметим, что, например,

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

Это значит, что $x+1$ — примитивный элемент (мультипликативной группы) поля F_2^3.

1. Поле $K(\omega)$ изоморфно полю многочленов $K[x]/g(x)$
2. $b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \Longleftrightarrow b_0 + b_1\omega + \cdots b_{n-1}\omega^{n-1}, b_j \in K$
3. $K(\omega) = K[\omega]/g(\omega)$

9.8 Свойства полей разложения заданного многочлена

Определение 9.5 *Поле $K \subset \mathbb{F}_p$ называется полем разложения многочлена f(x), если над полем K многочлен f(x) раскладывается на линейные множители, и при этом он не раскладывается на линейные множители ни над каким собственным подполем поля K, содержащим $\mathbb{F}_p$.*

Для всякого поля $\mathbb{F}_p$ и многочлена $f(x) \in \mathbb{F}_p[x]$ существует расширение $K/\mathbb{F}$, являющееся полем разложения для f(x).

- Поле разложения существует, и оно единственно с точностью до изоморфизма
- Если f(x) неприводим над полем $\mathbb{F}_p$, и его степень равна n, то его полем разложения является поле $GF(p^n)$.

Примеры.

1. Поле комплексных чисел $\mathbb{C}$ служит полем разложения многочлена x^2+1 над полем K вещественных чисел.
2. Любое конечное поле $GF(q)$, где $q = p^n$, есть поле разложения многочлена многочлена $x^q - x$ над простым подполем $GF(p) \subset GF(q)$.

9.9 Теорема о существовании и единственности конечного поля с заданным числом элементов

Теперь можно вернуться к вопросу о существовании

1. конечного поля $\mathbb{F}_q$ размера q, показав, что всегда $q = p^n$;
2. неприводимого многочлена степени n над $\mathbb{F}_p$ (везде p — простое, n — натуральное).

Это можно сделать двумя способами.

- 1) $\Rightarrow$ 2) доказать существование поля из p^n элементов, откуда вывести существование неприводимого многочлена степени n над $\mathbb{F}_p$;
- 1) $\Leftarrow$ 2) становить существование неприводимого многочлена f степени n над $\mathbb{F}_p$, откуда уже следует существование поля из p^n как факторкольца по идеалу (f).

Мы пойдём вторым путём.
Докажем существование нормированного неприводимого многочлена в полях Галуа.
Для таких многочленов выполняется аналог основной теоремы арифметики: **каждый нормированный многочлен однозначно разлагается на произведение степеней неприводимых многочленов**.
Действительно:

- разложение в евклидовом кольце однозначно (с точностью до умножения на обратимые элементы — делители);
- в случае кольца многочленов над полем обратимые элементы — ненулевые константы (многочлены степени 0);
- выбор старшего коэффициента 1 однозначно определяет сомножители.

Докажем вторую часть основной теоремы о конечных полях: любые два поля с одинаковым числом элементов изоморфны.

Теорема 9.6 *Пусть m — минимальный многочлен элемента $\alpha \in \mathbb{F}_p^n$ и d — её степень. Тогда поле $\mathbb{F}_p[x]/(m)$ изоморфно подполю $\mathbb{F}_p^d$, порожденному степенями α.*

Теорема 9.7 *Если d_n — число неприводимых нормированных многочленов степени n над $\mathbb{F}_p$, то*

$$\sum_{m|n} m \cdot d_m = p^n$$

9.10 Связь конечного поля $GF(q = p^n)$ с полем разложения многочлена $x^q - x \in \mathbb{F}_q[x]$

- Поле разложения многочлена $x^q - x \in \mathbb{F}_q[x], q = p^n$ состоит в точности из q элементов;
- $\forall \alpha \in \mathbb{F}_q[x], \alpha^q = \alpha$
- Все элементы поля F_p^n , не исключая нуля, являются корнями многочлена $x^{p^n} - x$.

Вынесем x за скобку:

$$x^{p^n} - x = x(x^{p^n-1} - 1)$$

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

9.11 Малая теорема Ферма

Теорема 9.8 $\forall \alpha \in \mathbb{F}_p \ : \ \alpha^p \equiv \alpha \pmod p$
$\forall \alpha \in \mathbb{F}_p, \alpha \neq 0 \ : \ \alpha^{p-1} = 1$

Альтернативное доказательство с помощью теории групп.
Одно из самых простых доказательств Малой теоремы Ферма основано на следствии теоремы Лагранжа из теории групп, утверждающей, что порядок элемента конечной группы делит порядок группы.
Напомним, что порядком конечной группы G называется число её элементов, а порядком элемента $g \in G$ — наименьший натуральный показатель его степени, равной единичному элементу $e \in G$.
Пусть G — конечная группа порядка n. Из того, что порядок элемента $g \in G$ делит n, следует, что $g^n = e$.
Рассмотрим поле $\mathbb{Z}_p$ вычетов по модулю p. Вычет целого числа a будем обозначать через a. Ненулевые элементы поля $\mathbb{Z}_p$ образуют группу относительно умножения.
Порядок этой группы, очевидно, равен $p-1$. Её единичным элементом является 1. Отсюда следует, что для каждого числа a, не делящегося на $a^{p-1} = 1$, но это как раз означает сравнение $a^{p-1} \equiv 1 \pmod p$

9.12 Условия существования и оценка числа подполей с заданным числом элементов

Пусть E/F конечное расширение поля, где $|E| = p^n$, $|F| = p^m$. Тогда E/F расширение Галуа. $n \vdots m$, причём $Gal(E/F)$ циклическая, порождённая автоморфизмом $\theta(x) = x^{p^m}, x \in E$. Более того, F - единственное подполе поля E размера p^m.
Примеры.

- Укажите, в каких полях $\{GF(8), GF(16), GF(32), GF(64)\}$ содержится подполе $GF(4)$.
  - Преобразуем: $\{GF(2^3), GF(2^4), GF(2^5), GF(2^6)\}$, а $GF(2^2)$. $4 \vdots 2$ & $6 \vdots 2$, то есть $GF(4)$ является подполем только полей: $\{GF(2^4), GF(2^6)\}$
- Найти число собственных подполей в поле $GF(64)$
  - Преобразуем: $GF(64 = 2^6)$. Только 3 и 2 делят 6, тогда собственные подполя данного поля $\{GF(4), GF(8)\}$

9.13 Мультипликативная группа поля $GF(q)$. Свойства

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F} \setminus \{0\}$ - **мультипликативная группа поля** $\mathbb{F}_p$

- $\mathbb{F}_p^*$ — циклическая группа порядка $p-1$ по умножению.
- Как конечная циклическая группа, F_p^* содержит генератор = примитивный элемент α:
  - любой элемент $\beta \in F_p^*$ является некоторой его натуральной степенью: $\beta = \alpha^i, i \in \{1, ..., p-1\}$;
  - причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

9.14 Примитивные элементы поля. Вычисление через степени одного из них

- $\mathbb{F}_p^*$ — циклическая группа порядка $p-1$ по умножению.
- Как конечная циклическая группа, F_p^* содержит генератор = примитивный элемент α:

– любой элемент $\beta \in F_p^*$ является некоторой его натуральной степенью:
$\beta = \alpha^i, i \in \{1, ..., p-1\}$;

– причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

Пример.
α корень многочлена $x^3 + x + 1$ над $GF(2)$, то есть $1 + x + x^3 \in GF(2)[x]$. Следовательно, $GF(8) = GF(2)[\alpha]$. Порядок α есть делитель 8-1=7. Поэтому $\text{ord}(\alpha) = 7$ и α – примитивный элемент.
Элементы поля $\mathbb{F}_8$:

$$0 = 0 \quad 1 = \alpha^7 = \alpha^0 \quad \alpha = \alpha^1$$
$$\alpha^2 = \alpha^2 \quad 1 + \alpha = \alpha^3 \quad \alpha + \alpha^2 = \alpha^4$$
$$1 + \alpha + \alpha^2 = \alpha^5 \quad 1 + \alpha^2 = \alpha^6$$

Тогда:
$\alpha^3 + \alpha^6 = (1 + \alpha) + (1 + \alpha^2) = \alpha + \alpha^2 = \alpha^4 \quad \alpha^3\alpha^6 = \alpha^9 = \alpha^2$
Ещё пример. Элементы 3 и 5 поля $GF(7)$ являются примитивными, тогда как остальные ненулевые элементы непримитивны. Действительно, $p\breve{}1 = 6$ степеней элемента 3 различны: $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 3^0 = 1$. Для непримитивного элемента поля, например 2, подобные вычисления дают $2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2, 2^5 = 4, 2^6 = 1$, так что возведением 2 в различные степени можно получить лишь некоторые (но не все!) ненулевые элементы GF(7).

9.15 Алгоритм проверки примитивности заданного элемента поля $GF(q)$

Если примарное разложение $(p-1)$ известно - элемент $\alpha \in \mathbb{F}_p$ будет примитивным, if $\alpha^k \not\equiv_p 1$, для каждого делителя k числа $p-1$.
Пример. Выберем неприводимый многочлен в $\mathbb{F}_3[x] : x^2 + 1$. Искомое поле есть:

$$\begin{aligned}\mathbb{F}_3^2 &\cong \mathbb{F}_3[x]/(x^2+1) \\ &= \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.\end{aligned}$$

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

$$\begin{aligned}(x+1) + (x+2) &= 2x, & (x) \cdot (2x) &= 1, \\ (2x+1) + x &= 1, & (2x+1) \cdot x &= x+1,\end{aligned}$$

Заметим, что, например,

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

Это значит, что $x+1$ — примитивный элемент (мультипликативной группы) поля $\mathbb{F}_2^3$.
f(x) — примитивный элемент (генератор) группы $\mathbb{F}_p^{n*}$, если

1. $(f(x))^{p^n-1} = 1 \;\; \& \;\; (f(x))^i \neq 1, 0 < i < p^n - 1$
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что
$g(x) = (f(x))^i, i \in \{0, 1, ..., p^n - 1\}$.

Если α — примитивный элемент поля $GF(q)$, то любой другой примитивный элемент может быть получен как степень α^k, где k — целое взаимно простое с $q-1 \Rightarrow$ количество примитивных элементов поля $\mathbb{F}_p^n$ равно $\varphi(p^n - 1)$.
Например, в 9-элементном поле $\mathbb{F}_3^2$ имеется $\varphi(8) = 4$ примитивных элемента, образованных степенями

1, 3, 5, 7 (числа, взаимно простые с 8) уже найденного генератора:

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

9.16 Поле разложения неприводимого многочлена $f \in F_q[x]$

Теорема 9.9 *Все неприводимые многочлены n-й степени из $\mathbb{F}_p[x]$ делят многочлен $x^{p^n} - x$.*

Доказательство.

- **n = 1:**
  - Убеждаемся,что $(x-a)|(x^p - x)$,где $a \in \mathbb{F}_p$:при $a = 0$ это очевидно, а в остальных случаях доказано, что a — корень многочлена $x^{p-1} - 1 = (x^p - x)/x$.
- **n > 1:**
  - Строим по неприводимому и (без ограничения общности — нормированному) многочлену f(x) степени n поле $\mathbb{F}_p^n$. В этом поле x — корень и $f(x)$, и $x^{p^n-1} - 1$, причём $f(x)$ — м.м. для него. По свойствам м.м. $x^{p^n-1} - 1$ делится на $f(x)$.

Пример. разложение $x^{15} + 1 \in \mathbb{F}_2[x]$
Проверяем степени 2 :

$$2^4 - 1 = 15|15, \quad 2^3 - 1 = 7 \not| 15, \quad 2^2 - 1 = 3|15, \quad 2^1 - 1 = 1|15$$

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

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

2. $x(x^3+1) = x^{2^2} + x$, откуда все неприводимые многочлены 2-й степени будут делителями $x^4 + x$ и, следовательно, $x^3 + 1$. Такой многочлен только один: $x^2 + x + 1$.
3. $x(x^1+1) = x^{2^1} + x$, откуда (тривиально) единственный неприводимый многочлен 1-й степени $x+1$ делит $x^2 + x$.

Итого: разложение $x^{15} - 1$ на неразложимые над $\mathbb{F}_2$ многочлены —

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

9.17 Строение и свойства множества корней неприводимого многочлена в поле разложения

Определение 9.10 *Пусть $\mathbb{F}$–поле. Многочлен $P_n(x) = a_0x^n + a_1x^{n-1} + ... + a_n$, где все $a_i \in \mathbb{F}$, называется неприводимым над полем $\mathbb{F}$, если его нельзя представить в виде произведения многочленов меньшей степени с коэффициентами из поля $\mathbb{F}$.*

- Многочлен $P_2(x) = x^2 - 2$ является неприводимым над полем $\mathbb{F}_5$, так как в $\mathbb{F}_5$ уравнение $P_2(x) = x^2 - 2 = 0$ не имеет решения, так как нет элементов, квадрат которых равен 2. Многочлен $P_2(x) = x^2 + 4$ является приводимым в этом поле $x^2 + 4 = (x+1)(x+4)$.

Свойства множества корней неприводимых многочленов:

- Множество всех корней неприводимого многочлена образует циклическую группу, то есть найдется примитивный корень θ, такой что все другие корни являются степенями этого элемента.

$$(\theta_1)^q = \theta_2, \cdots, (\theta_{n-1})^q = \theta_n$$

- Поле разложения неприводимого многочлена $f \in \mathbb{F}_q[x]$ степени n равно $GF(q^n)$.
- В поле разложения неприводимый многочлен f имеет в точности $n = \deg(f)$ различных корней.

Примерчик. Найти корни неприводимого над $\mathbb{F}_2$ многочлена:

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

Один корень получаем немедленно: **x** (или $\bar{x}$). По только что доказанной теореме можно выписать остальные:

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

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

$$\begin{aligned} f(x^2) = x^4 + x^3 + 1|_{x \to x^2} &= x^{4\cdot 2} + x^4 + 2 + 1|_{x^4 \to x^3+1} = \\ &= (x^3+1)^2 + (x^3+1)x^2 + 1 = x^6 + \not{1} + x^5 + x^2 + \not{1} = \\ &= x^6 + x^5 + x^2 = x^2(x^4 + x^3 + 1) = x^2 \cdot 0 = 0. \end{aligned}$$

9.18 Функция $tr(x)$ как отображение поля $GF(p^n)$ в поле $GF(p)$. Свойства

отображение элементов конечного расширения поля $GF(p^n) \supset GF(p)$ в исходное поле $GF(p)$, определяемое следующим образом:

$$tr(x) = \sum_{i=0}^{n-1} x^{p^i}$$

Свойства

- $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$
- $\mathrm{Tr}(c\alpha) = c\mathrm{Tr}(\alpha)$ при $c \in K$

Примеры:

- $\mathrm{Tr}(1) = \sum_{i=0}^{2-1} x^{2^i} = 1 + 1 = 0 | GF(2^2)$
- $\mathrm{Tr}(1) = \sum_{i=0}^{3-1} x^{2^i} = 1 + 1 + 1 = 1 | GF(2^3)$
- $\mathrm{Tr}(1) = \sum_{i=0}^{2-1} x^{3^i} = 1 + 1 = 2 | GF(3^2)$

9.19 Период многочлена. Примеры.

Определение 9.11 ***Периодом(экспонентой)*** *многочлена $f(x) \in \mathbb{F}_q[x], f(0) = 0$ называется такое наименьшее число $j \in \mathbb{N}$, что*

$$x^j - 1 \ \vdots \ f(x)$$

Если же $f(0) = 0$, то многочлен $f(x)$ однозначно представим в виде $f(x) = x^n \cdot g(x), n \in \mathbb{N}, g(x) \in \mathbb{F}_q[x]$ и $g(0) = 0$, тогда $\mathrm{ord}(f(x))$ *определяется как* $\mathrm{ord}(g(x))$.

ИЛИ

Из определения порядка многочлена $f(x)$ следует, что - это наименьшее натуральное число, удовлетворяющее сравнению:

$$x^e \equiv 1 \pmod{f(x)},$$

т.к. это сравнение означает, что $f(x)$ делит $x^e - 1$.

Примеры будут потом.

9.20 Свойства периода неприводимого многочлена

Если $f(x), \deg(f) = m$ над $GF(q)$, то период $f(x)$ равен наименьшему общему кратному мультипликативных порядков его корней (то есть ооно делит $q^m - 1$). Это следствие, вытекающее из следующей теоремы.

- Пусть с – натуральное число. Многочлен $f(x) \in \mathbb{F}_q[x]$, удовлетворяющий условию $f(0) \neq 0$ делит двучлен $x^c - 1$ тогда и только тогда, когда $\mathrm{ord}(f(x))$ делит число с.
- Если e_1 и e_2 натуральные числа, то НОД многочленов $(x^{e_1} - 1)$ и $(x^{e_2} - 1)$ в $\mathbb{F}_q[x]$ равен $(x^d - 1)$, где $d = \gcd(_1, _2)$.

9.21 Связь между периодом неприводимого многочлена $f(x) \in \mathbb{F}_q[x]$ и порядком его корня в поле разложения

Теорема 9.12 *Пусть $f(x) \in \mathbb{F}_q[x]$ неприводимый многочлен степени m, удовлетворяющий условию $f(0) \neq 0$. Порядок этого многочлена совпадает с порядком любого корня этого многочлена в мультипликативной группе $\mathbb{F}^*$ поля F_q^m.*

9.22 Пусть f разлагается в произведение $f = f_1 \cdot f_2 \cdots f_t$ попарно взаимно простых многочленов. Указать связь между периодом многочлена f и периодами множителей f_i

Теорема 9.13 *Пусть $g_1(x), ..., g_k(x)$ – попарно взаимно простые ненулевые многочлены над полем $\mathbb{F}_q$, и пусть $f(x) = g_1(x) \cdot g_2(x) \cdots g_K(x)$, тогда*

$$\mathrm{ord}(f(x)) = \mathrm{ord}(g_1(x)) \cdot \mathrm{ord}(g_K(x)) = \mathrm{lcm}(\mathrm{ord}(g_1(x), ..., ord(g_K).$$

Иными словами, порядок произведения попарно взаимно простых ненулевых многочленов равен наименьшему общему крат- ному порядков его сомножителей (многочленов).

9.23 Пусть $f = g^m$, где g - неприводимый многочлен над полем $GF(q = p^n)$. Связь между периодами f и g.

Теорема 9.14 *Пусть $\mathbb{F}_q$ конечное поле характеристики p. Если $f = a \cdot f_1^{n_1} \cdot ... \cdot f_n^{n_K}$ каноническое разложение в кольце $\mathbb{F}_q[x]$ многочлена $f(x) \in \mathbb{F}_q[x]$ положительной степени, такого что $f(0) \neq 0$, то*

$$\mathrm{ord}(f(x)) = \mathrm{ord}(af_1^{n_1} \cdot ... \cdot f_n^{n_K}) = p^t \,\mathrm{lcm}(\mathrm{ord}(f_1), ..., \mathrm{ord}(f_n)),$$

где t – наименьшее целое число, удовлетворяющее неравенству $p^t \geqslant \max\{n_1, ..., n_K\}$.

Пример. $f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.
Каноническое разложение $f(x)$ над полем $\mathbb{F}_2$ имеет вид $f(x) = (x^2 + x + 1)^3(x^4 + x + 1)$. Т.к. $\mathrm{ord}(x^2 + x + 1) = 3$ и имея $\mathrm{ord}(g^n(x) = p^t \,\mathrm{ord}(g(x))$, получаем, что $\mathrm{ord}((x^2 + x + 1)^3) = 2^2 \cdot 3 = 12$ т.к. у нас $\mathbb{F}_2$ т.е. $p = 2$ и $t = 2$ чтобы $2^2 > 3$). Далее $\mathrm{ord}(x^4 + x + 1) = 15$. Тогда $\mathrm{ord}(f(x)) = \mathrm{lcm}(12, 15) = 60$.

9.24 Примитивные многочлены

Определение 9.15 *Многочлен $f(x) \in \mathbb{F}_q[x]$степени $m \geqslant 1$ называется примитивным многочленом над полем $\mathbb{F}_q$, если он является минимальным многочленом над $\mathbb{F}_q$ некоторого примитивного элемента расширения $\mathbb{F}_q^m$ поля F.*
Многочлен $f(x) \in \mathbb{F}_q[x]$ степени m является примитивным тогда и только тогда, когда он нормирован и, такой,что

$$f(0) \neq 0 \quad \& \quad \mathrm{ord}(f(x)) = q^m - 1.$$

$f(x)$ — примитивный элемент (генератор) группы $\mathbb{F}_p^{n*}$, если

- $(f(x))^{p^n-1} = 1, (f(x))^i \neq 1 \ : \ 0 < i < p^n - 1$
- $\forall g(x) \in \mathbb{F}_p^{n*} \ \exists \, i : g(x) = (f(x))^i, i \in \{0, 1, ..., p^n - 1\}$

Если α — примитивный элемент поля $GF(q)$, то любой другой примитивный элемент может быть получен как степень α^k, где k — целое взаимно простое с $q-1 \Rightarrow$ количество примитивных элементов поля F_p^n равно $\varphi(p^n - 1)$.

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 $F = F_2[x]/(x^3 + x + 1) \cong F_2^3$; оно содержит все полиномы из F2[x] степени не выше 2.
4. Многочлен $P(x) = x^2 + x$ — приводим в любом кольце, в т.ч. в $\mathbb{F}_2[x]$, и он принадлежит F.
   Является ли $P(x)$ — примитивным элементом поля F?
5. 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**!

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 $F = \mathbb{F}_5[x]/(x^2 + x + 1) \cong F_5^2$; 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 ?
5. 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**!

9.25 Структура примитивных многочленов степени n над полем GF(q) в случае простоты числа $q^m - 1$

1. $q^m - 1$ НЕ является простым, если $q = p^n, p > 2$.
2. $2^m - 1$ НЕ является простым, если m - НЕ простое число.

$$2^6 - 1 = 63 \vdots 7$$

3. $2^p - 1$ - ПРОСТЫЕ (**числа Мерсенна**).

$$2^5 - 1 = 31 = p$$

9.26 Функция Мебиуса

Для функции Мебиуса, заданной на множестве натуральных чисел, справедливо выражение:

$$\left.\begin{array}{r}1, n = 1\\ (-1)^k, n = \underbrace{p_1 + p_2 + ... + p_k}_{\text{k}}, p_i \neq p_j\\ 0, n \vdots p^2\end{array}\right\} = \mu(n)$$

9.27 Квадратичные вычеты по модулю простого числа

Определение 9.16 *Пусть m - натуральное число, $a_0, a_1, a_2 \in \mathbb{Z}, a_2 \neq 0$. Рассмотрим квадратичное сравнение $a_2x^2 + a_1x + a_0 \equiv 0 \pmod p$ относительно переменной x с помощью выделения полного квадрата, применения теоремы Эйлера и китайской теоремы об остатках может быть приведено к виду*

$$x^2 \equiv a \pmod p,$$

где $a \in \mathbb{Z}$.
Если сравнение $x^2 \equiv a \pmod m$ имеет решение, то a называется ***квадратичным вычетом по модулю*** *m, иначе число a называется* ***квадратичным невычетом*** *по модулю m.*

Для $a = 3$ и $m = 4$. Квадратичное сравнение $x^2 \equiv 3 \pmod 4$ не имеет решений. В чем несложно убедиться небольшим перебором. (3 - квадратичный невычет по модулю 4).
$x^2 \equiv 2 \pmod 7$ (3 - квадратичный вычет по модулю 7).

9.28 Описание множества квадратичных вычетов через степени примитивного элемента поля GF(q)

Пусть p - нечётное простое число, b - произвольный примитивный элемент поля $\mathbb{Z}_p$. Тогда элемент поля $a \neq 0 \in \mathbb{Z}_p$ является квадратичным вычетом по модулю p тогда и только тогда, когда

$$a \in V = \{b^{2t} | t = 1, 2, ..., \frac{p-1}{2}\}$$

9.29 Символ Лежандра. Формула Эйлера для символа Лежандра

Назовём символом Лежандра следующее выражение:

$$\left.\begin{array}{r}1, \text{ если a - кв. вычет по модулю p}\\ -1, \text{ если a - кв. невычет по модулю p}\\ 0, (a, p) \neq 1.\end{array}\right\} = \left(\frac{a}{p}\right)$$

Теорема 9.17 ***(Критерий Эйлера)****. Пусть $p > 2$ - простое. Число a, взаимнопростое с p, является квадратичным вычетом тогда и только тогда, когда*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p \quad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

Доказательство. Пусть a является квадратичным вычетом по модулю p. Тогда $x^2 \equiv a \pmod p$. Следовательно, $a^{p-1/2} \equiv x^{p-1} \equiv 1 \pmod p$.
Рассмотрим многочлен $x^{(p-1)/2} - 1 \pmod p$. Как показано выше, любой квадратичный вычет является его корнем. Так как p - простое, то данный многочлен имеет не более $(p-1)/2$ корней. С другой стороны

количество квадратичных вычетов равно $(p-1)/2$. Следовательно, это корни многочлена $x^{(p-1)/2}-1 \pmod p$. Таким образом теорема выполнена.
Пример. Крошка-сын к отцу пришел, и спросила кроха: "Будет ли число 5 квадратом по модулю 7 ?". Гигант-отец тут же сообразил:

$$\left(\frac{5}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{5-1}{2}} \cdot \left(\frac{7}{5}\right) = 1 \cdot \left(\frac{2}{5}\right) = (-1)$$

т.е. сравнение $x^2 \equiv 5 \pmod 7$ решений не имеет и 5 - квадратичный невычет по модулю 7. Кроха-сын, расстроенный, пошел на улицу делиться с друзьями полученной информацией.

9.30 Мультипликативное свойство символов Лежандра и Якоби

Определение 9.18 *Пусть n—нечетное, большее единицы $n = p_1^{k_1}...p_s^{k_s}$,где $p_1, ..., p_s$ — простые числа. Тогда символ Якоби $\left(\frac{a}{n}\right)$ определяется следующим равенством:* $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \cdot \cdot \cdot \cdot \cdot \left(\frac{a}{p_s}\right)^{k_s}$

Символ Якоби является обобщением символа Лежандра, а символ Лежандра является частным случаем символа Якоби.
Мультипликативное свойства символа Лежандра (и символа Якоби соответственно)

$$\left(\frac{a\cdot b\cdot ...\cdot k}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\cdot ...\cdot\left(\frac{k}{p}\right)$$

По критерию Эйлера,

$$\left(\frac{a\cdot b\cdot ...\cdot k}{p}\right) = (a\cdot b\cdot ...\cdot k)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} ...k^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\cdot ...\cdot\left(\frac{k}{p}\right)$$

10 Конечные поля. Задачи для тренировки

10.1 Какие из следующих множеств образуют кольцо, а какие - поле:

1) множество $\{0\}$;
2) множество $\mathbb{N}$ натуральных чисел;
3) множество целых неотрицательных чисел;
4) множество целых неположительных чисел;
5) множество $\mathbb{Z}$ целых чисел;
6) множество $2\mathbb{Z}$ четных чисел;
7) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n \neq 0$;
8) множество $\mathbb{Q}$ рациональных чисел;
9) множество иррациональных чисел;
10) множество $\mathbb{R}$ вещественных чисел;
11) множество C комплексных чисел;
12) множество $\mathbb{Z}[i]$ целых гауссовы чисел, т. е. комплексных чисел с целыми действительной и мнимой частями;
13) множество комплексных чисел с рациональными действительной и мнимой частями?

10.2 Какие из следующих множеств образуют кольцо, а какие - поле:

1) множество чисел $a + b\sqrt{2}$, где a, b - целые;
2) множество чисел $a + b\sqrt{2}$, где a, b - рациональные;
3) множество чисел $a + b\sqrt[3]{2}$, где a, b - целые;

4) множество чисел $a + b\sqrt[3]{2}$, где a, b - рациональные;
5) множество чисел $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c - целые;
6) множество чисел $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c - рациональные;

10.3 Пусть K — кольцо, а $\mathbb{F}$ — поле. Какие из следующих множеств являются полугруппами, а какие группами:

1) множество $K[x]$ многочленов с коэффициентами из К относительно сложения;
2)$K[x]$ относительно умножения;
3)$K[x]$ относительно суперпозиции: $fg = f(g(x))$;
4)$K[x]$ относительно умножения?

10.4 Символ Лежандра

Вычислите символ Лежандра:

1) $\left(\frac{-88}{3}\right) = ?$ 2) $\left(\frac{90}{97}\right) = ?$ 3) $\left(\frac{30}{31}\right) = ?$ 4) $\left(\frac{70}{3}\right) = ?$ 5) $\left(\frac{46}{61}\right) = ?$

6) $\left(\frac{49}{67}\right) = ?$ 7) $\left(\frac{57}{59}\right) = ?$ 8) $\left(\frac{25}{97}\right) = ?$ 9) $\left(\frac{63}{67}\right) = ?$ 10) $\left(\frac{-13}{89}\right) = ?$

10.5 Символ Якоби

Вычислите символ Якоби:

1) $\left(\frac{-74}{33}\right) = ?$ 2) $\left(\frac{62}{81}\right) = ?$ 3) $\left(\frac{65}{93}\right) = ?$ 4) $\left(\frac{97}{9}\right) = ?$ 5) $\left(\frac{16}{33}\right) = ?$

6) $\left(\frac{-53}{99}\right) = ?$ 7) $\left(\frac{51}{9}\right) = ?$ 8) $\left(\frac{39}{85}\right) = ?$ 9) $\left(\frac{70}{51}\right) = ?$ 10) $\left(\frac{-10}{45}\right) = ?$

10.6 Функция Мёбиуса

Вычислите функцию Мёбиуса:

1) $\mu(91) = ?$ 2) $\mu(57) = ?$ 3) $\mu(62) = ?$ 4) $\mu(94) = ?$ 5) $\mu(70) = ?$

6) $\mu(30) = ?$ 7) $\mu(96) = ?$ 8) $\mu(24) = ?$ 9) $\mu(16) = ?$ 10) $\mu(52) = ?$

10.7 Матрицы

10.7.1 Вычислите сумму матриц

1) $\mathbb{Z}_{13}: \begin{pmatrix} 8 & 7 & 8 & 0 \\ 5 & 2 & 0 & 7 \end{pmatrix} + \begin{pmatrix} 0 & 11 & 11 & 11 \\ 7 & 9 & 4 & 5 \end{pmatrix} = ?$

2) $\mathbb{Z}_{11}: \begin{pmatrix} 0 & 9 & 2 & 3 \\ 9 & 7 & 3 & 6 \\ 7 & 5 & 2 & 8 \end{pmatrix} + \begin{pmatrix} 5 & 4 & 5 & 7 \\ 6 & 5 & 3 & 2 \\ 5 & 6 & 7 & 1 \end{pmatrix} = ?$

10.7.2 Найдите разность матриц

1) $\mathbb{Z}_{41}: \begin{pmatrix} 27 & 29 \\ 17 & 22 \\ 2 & 5 \\ 16 & 9 \end{pmatrix} - \begin{pmatrix} 34 & 10 \\ 37 & 25 \\ 18 & 22 \\ 2 & 24 \end{pmatrix} = ?$

2) $\mathbb{Z}_{43}: \begin{pmatrix} 4 & 7 & 25 & 20 \\ 32 & 18 & 27 & 37 \\ 0 & 23 & 33 & 19 \\ 16 & 4 & 36 & 2 \end{pmatrix} - \begin{pmatrix} 23 & 1 & 25 & 18 \\ 30 & 31 & 39 & 14 \\ 20 & 16 & 26 & 35 \\ 9 & 39 & 12 & 3 \end{pmatrix} = ?$

10.7.3 Найдите произведение матриц

1) $\mathbb{Z}_{41}: \begin{pmatrix} 3 & 26 & 30 & 30 \\ 19 & 5 & 23 & 2 \end{pmatrix} \cdot \begin{pmatrix} 23 & 5 \\ 12 & 32 \\ 12 & 33 \\ 27 & 28 \end{pmatrix} = ?$

2) $\mathbb{Z}_{31}: \begin{pmatrix} 6 & 7 & 27 \\ 26 & 28 & 13 \\ 21 & 11 & 24 \end{pmatrix} \cdot \begin{pmatrix} 26 & 2 & 14 \\ 11 & 27 & 5 \\ 19 & 1 & 1 \end{pmatrix} = ?$

10.7.4 Вычислите детерминант матрицы

1) $\mathbb{Z}_{23}: \begin{vmatrix} 22 & 11 \\ 21 & 22 \end{vmatrix} = ?$

2) $\mathbb{Z}_{53}: \begin{vmatrix} 25 & 28 & 42 \\ 15 & 16 & 23 \\ 50 & 52 & 33 \end{vmatrix} = ?$

10.7.5 Найдите сумму многочленов:

1) $\mathbb{Z}_{29}: (24x + 14) + (13x^3 + 28x^2 + 2x + 2) = ?$

2) $\mathbb{Z}_{7}: (x^3 + 5x^2 + 4x + 5) + (x + 2) = ?$

10.7.6 Найдите разность многочленов:

1) $\mathbb{Z}_{31}: (3x + 19) - (24x^4 + 28x^3 + 25x^2 + 2x + 23) = ?$

2) $\mathbb{Z}_{43}: (3x + 28) - (5x + 36) = ?$

10.7.7 Найдите произведение многочленов:

1) $\mathbb{Z}_{43}: (39x^5 + 34x^4 + 10x^3 + 9x^2 + 21x + 17) \cdot (13x^2 + 16x + 10) = ?$

2) $\mathbb{Z}_{29}: (24x^5 + 9x^4 + 6x^3 + 8x^2 + 21x + 21) \cdot (10x^2 + 21x + 26) = ?$

10.7.8 Вычислите целую часть от деления многочленлов:

1) $\mathbb{Z}_{11}: (7x + 10)/(8x^4 + 8x^3 + 3x^2 + 2) = ?$

2) $\mathbb{Z}_{59}: (21x^4 + 28x^3 + 37x^2 + 46x + 36)/(8x^2 + 27x + 44) = ?$

10.7.9 Разделите многочлен с остатком:

1) $\mathbb{Z}_{5}: (4x^4 + 4x^3 + 3x^2 + x + 3)\ mod\ (x^4 + 3x^3 + x^2 + 2x + 1) = ?$

2) $\mathbb{Z}_{47}: (20x + 2)\ mod\ (28x + 26) = ?$

10.7.10 Найдите НОД многочленов:

1) $\mathbb{Z}_{59}: (19x^3 + 42x^2 + 53, 16x^5 + 11x^4 + 50x^3 + 12x^2 + 47x + 8) = ?$

2) $\mathbb{Z}_{17}: (15x^4 + 7x^3 + 8x^2 + 9x + 6, 15x^2 + 3x + 5) = ?$

10.7.11 Выписать для поля $\mathbb{F}_4$:

- Таблицы **сложения** и **умножения**;
- Таблицы **противоположных** и **обратных** элементов;
- Таблицу, представляющую все элементы $a \in \mathbb{F}_4^*$ как **степени** $a = a^k; k \in \{0, 1, 2\}$ одного из них $a \in \mathbb{F}_4^*$.

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

Таблица 1: Сложение.

a	**0**	**1**	**x**	**x+1**
$-a$				

Таблица 2: Противоположные элементы.

$\cdot$	**0**	**1**	**x**	**x+1**
0				
1				
x				
x+1				

Таблица 3: Умножение.

a	**0**	**1**	**x**	**x+1**
a^{-1}				

Таблица 4: Обратные элементы.

a	**0**	**1**	**x**	**x+1**
a^k				

Таблица 5: Степенное представление.

Решение

1.Сложение:

+	**0**	**1**	**x**	**x+1**
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

Таблица 1: Сложение.

2.Противоположные элементы:

a	**0**	**1**	**x**	**x+1**
$-a$	0	1	x	x+1

Таблица 2: Противоположные элементы.

Пояснения:

$$2x \equiv 0 \mod 2; -x \equiv x \mod 2$$

3.Умножение:

·	**0**	**1**	**x**	**x+1**
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

Таблица 3: Умножение.

Пояснения:

$$x \cdot x = x^2 \equiv x^2 - f(x) \equiv (-x-1) \mod f(x) \equiv (x+1) \mod 2;$$
$$x \cdot (x+1) = x^2 + x \equiv x^2 + x - f(x) \equiv -1 \mod f(x) \equiv 1 \mod 2.$$
$$(x+1)^2 = x^2 + 2x + 1 \equiv (x^2+1) \mod 2 \equiv x^2 + 1 - f(x) \equiv -x \mod f(x) \equiv -x \mod 2.$$

4.Обратные элементы:

a	**0**	**1**	**x**	**x+1**
a^{-1}	-	1	x+1	x

Таблица 4: Обратные элементы.

Пояснения:

$$x \cdot (x+1) = 1 \Rightarrow x^{-1} = x + 1;$$

5.Степенное представление:

a	**0**	**1**	**x**	**x+1**
a^k	-	a^0	a^1	a^2

Таблица 5: Степенное представление.

Пояснения:

$$a = x; a^2 = x^2 = x + 1; a^3 = x^3 = x^2 \cdot x = (x + 1) \cdot x = 1;$$

Замечание. Группа $\mathbb{F}_4^*$ является циклической третьего порядка. В качестве порождающего элемента можно взять любой из неединичных элементов:

$\mathbb{F}_4^* = \mathbb{F}_4 \backslash \{0\} = \{1, x, x + 1\} = \langle x \rangle = \langle x + 1 \rangle \cong C_3$, здесь и далее C_i - циклическая группа порядка i.
В табл. 5 в качестве порождающего элемента выбран $a = x$

Предостережение:

$$\mathbb{F}_4 \ncong \mathbb{Z}_4.$$

$Z_4 = \{0, 1, 2, 3\}$ - не поле, и даже не целостное кольцо: $2 \cdot 2 = 0$; можно считать, что $\mathbb{F}_p = \mathbb{Z}_p$, лишь для простых p.

10.7.12 Выписать для поля $\mathbb{F}_8$:

- Таблицы **сложения** и **умножения**;
- Таблицы **противоположных** и **обратных** элементов;
- Таблицу, представляющую все элементы $a \in \mathbb{F}_8^*$ как **степени** $a = a^k; k \in \{0, 1, 2, 3, 4, 5, 6\}$ одного из них $a \in \mathbb{F}_8^*$.

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0								
1								
x								
$x+1$								
x^2								
x^2+1								
x^2+x								
x^2+x+1								

Таблица 1: Сложение.

a	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
$-a$								

Таблица 2: Противоположные элементы.

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0								
1								
x								
$x+1$								
x^2								
x^2+1								
x^2+x								
x^2+x+1								

Таблица 3: Умножение.

a	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
a^{-1}								

Таблица 4: Обратные элементы.

a	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
a^k								

Таблица 5: Степенное представление.

Решение

1.Сложение:

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Таблица 1: Сложение.

2.Противоположные элементы:

a	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
$-a$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

Таблица 2: Противоположные элементы.

3.Умножение:

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Таблица 3: Умножение.

4.Обратные элементы:

a	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
a^{-1}	-	1	x^2+1	x^2+x	x^2+x+1	x	$x+1$	x^2

Таблица 4: Обратные элементы.

5.Степенное представление:

a	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
a^k	-	a^0	a^1	a^3	a^2	a^6	a^4	a^5

Таблица 5: Степенное представление.

Пояснения:

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

10.7.13 Выписать для поля $\mathbb{F}_9$:

- Таблицы **сложения** и **умножения**;
- Таблицы **противоположных** и **обратных** элементов;
- Таблицу, представляющую все элементы $a \in \mathbb{F}_9^*$ как **степени** $a = a^k; k \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ одного из них $a \in \mathbb{F}_9^*$.

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

Таблица 1: Сложение.

a	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$-a$									

Таблица 2: Противоположные элементы.

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0									
1									
2									
x									
$x+1$									
$x+2$									
$2x$									
$2x+1$									
$2x+2$									

Таблица 3: Умножение.

a	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
a^{-1}									

Таблица 4: Обратные элементы.

a	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
a^k									

Таблица 5: Степенное представление.

Решение

1.Сложение:

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

Таблица 1: Сложение.

Противоположные элементы:

a	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$-a$	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$

Таблица 2: Противоположные элементы.

Умножение:

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	$2x+1$	1	$x+1$	$x+2$	$2x+2$	2
$x+1$	0	$x+1$	$2x+2$	1	$x+2$	$2x$	2	x	$2x+1$
$x+2$	0	$x+2$	$2x+1$	$x+1$	$2x$	2	$2x+2$	1	x
$2x$	0	$2x$	x	$x+2$	2	$2x+2$	$2x+1$	$x+1$	1
$2x+1$	0	$2x+1$	$x+2$	$2x+2$	x	1	$x+1$	2	$2x$
$2x+2$	0	$2x+2$	$x+1$	2	$2x+1$	x	1	$2x$	$x+2$

Таблица 3: Умножение.

Обратные элементы:

a	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
a^{-1}	-	1	2	$x+1$	x	$2x+1$	$2x+2$	$x+2$	$2x$

Таблица 4: Обратные элементы.

Степенное представление:

a	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
a^k	-	a^0	a^4	a^1	a^7	a^6	a^5	a^2	a^3

Таблица 5: Степенное представление.

Замечание. Группа $\mathbb{F}_9^*$ является циклической восьмого порядка. В данном случае **не любой** неединичный элемент является порождающим. Однако обычный выбор $a = x$ снова дает порождающий элемент. В то же время, скажем, $a^2 = 2x + 1$ уже порождает не всю группу $\mathbb{F}_9^* = \langle a \rangle \cong C_8$, а лишь ее подгруппу $\langle a^2 \rangle = \{1, a^2, a^4, a^6\} \cong C_4$.

10.7.14 Найти порядки всех ненулевых элементов поля $\mathbb{F}_7$

Решение
В поле $\mathbb{F}_7$ имеется 6 ненулевых элементов По теореме Лагранжа порядком элемента могут быть только делители 6, т.е. числа $Del(6) = \{1, 2, 3, 6\}$. Порядок 1 имеет только $a = 1$, а порядок 2 имеет наибольший элемент поля $a = 6$. Все остальные элементы имеют порядок 3 или 6. Будем вычислять значение $a^3 \mod 7$ для всех a от 2 до 5. Если $a^3 \mod 7 = 1$, то порядок a равен 3, иначе, 6:

a	2	3	4	5
$\operatorname{ord} a$	3	6	3	6

Элементами максимального порядка являются $a = 3$ и $a = 5$. Они и являются примитивными элементами поля $\mathbb{F}_7$.

11 Конечные поля. Задачи на доказательство

1) (а) Показать, что многочлены $x^4 + 1$ и $x^6 + x^3 + 1$ неприводимы над полем рациональных чисел.

(б) Показать, что многочлен степени 3 над полем либо неприводим, либо имеет корень в этом поле. Является ли многочлен $x^3 - 5x^2 + 1$ неприводимым над полем рациональных чисел?

(в) Показать, что многочлен от двух переменных x^2+y^2-1 неприводимым над полем рациональных чисел. Неприводим ли он над полем комплексных чисел?

2) Пусть $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ - многочлен с целыми коэффициентами, $a_0 \neq 0$. Показать, что если f имеет корень в поле рациональных чисел, то этот корень должен быть целым рациональным числом, делящим a_0. Обобщить это утверждение на любое факториальное кольцо и поле его частных.

3) Доказать, что существует поле, состоящее из двух элементов.
Примечание: очевидно, что один из этих элементов должен быть нулем поля, а другой - его единицей.

4) Доказать теорему 9.7.

12 Поля. Задачи с решениями

Задача № 1. Указать характеристику поля GF(8).

Решение. Конечное поле GF(q) из q элементов существует только в том случае, когда число q является степенью простого числа: $q = p^m$, при этом характеристика поля $GF(p^m)$ равна p. Так как $8 = 2^3$, то характеристика поля GF(8) равна 2.

Ответ: 2.

Задача № 2. Является ли поле GF(4) подполем поля GF(8)?

Решение. Поле $GF(q_1 = (p_1)^m)$ является подполем поля $GF(q = p^n)$ в том и только том случае, когда характеристики p_1 и p полей равны, а число m является делителем числа n.

Имеем: $4 = 2^2$, $8 = 2^3$. Однако число 2 не делит число 3. Следовательно, поле GF(4) не является подполем поля GF(8).

Ответ: нет.

Задача № 3. В каком из полей Fq принадлежит $\{F_8, F_{16}, F_{32}\}$ многочлен $f(x) = x^2+x+1$, $f(x) \in F_2[x]$ полностью разлагается на линейные множители?

Решение. Многочлен x^2+x+1 неприводим над полем F_2, следовательно, его полем разложения является поле F_4. Поле F_4 содержится в поле F_{16} и не содержится в полях F_8 и F_{32}. Таким образом, многочлен f(x) полностью разлагается на линейные множители только в поле F_{16}.

Ответ: в F_{16}.

Задача № 4. Найти число различных решений уравнения $y^3 + y + 1 = 0$ в поле $F_2[x]/x^3 + x^2 + 1$.

Решение. Так как многочлен $y^3 + y + 1$ имеет степень 3 и неприводим над полем F_2, то поле $GF(2^3) = F_2[x]/x^3+x^2+1$ является его полем разложения. В этом поле он имеет в точности 3 различных решения.

Ответ: 3.

Задача № 5. Сколько различных решений имеет уравнение $x^9 - x = 0$ в поле GF(9)?

Решение. Каждый элемент поля GF(q) является решением уравнения $x^q - x = 0$. Значит, в поле GF(9) уравнение $x^9 - x = 0$ имеет ровно 9 различных решений.

Ответ: 9.

Задача № 6. Доказать, что $(p-1)! \equiv_p -1$ для простого p. Решение. $p = 2$: - решение тривиально.
$p > 2$: эдементы $\mathbb{F}_p$ являются корнями уравнения $x^{p-1} - 1 = 0$ и других корней у этого уравнения нет. По т. Виета их произведение равно свободному члену -1.

Задача № 7. Найти $x \equiv_{17} 1^{2006} + 2^{2006} + ... + 16^{2006}$.

Решение. $\mathbb{F}_{17}^* = \{1, 2, ..., 16\} = \langle 3 \rangle$:
$3^1 = 1, 3^2 = 9, 3^3 = 27 \equiv_{17} 10, 30_{17}13, 39 \equiv_{17} 5, ...;$
$G = \{1^{2006}, 2^{2006}, ..., 16^{2006}\}$ - циклическая группа порядка k группы $\mathbb{F}_{17}^*$.
Элементы G - корни уравнения: $x^k - 1 = 0$ *(*)*
Их сумма по т. Виета есть коэффициент при x^{k-1} в *(*)*, т.е. 0.

Задача № 8. Построить поле из 4 элементов.

Решение. Это поле F_2^2, оно может быть построено как фактор-кольцо $F_2[x]/(a(x))$, где a(x) - неприводчмый многочлен из $F_2[x]$ степени 2. Но такой многочлен только один: $x^2 + x + 1$.
Следовательно, $F_2^2 = \{0, 1, x, x + 1\}$.

Задача № 9. Производная многочлена $f \neq 0$ над полем характеристики p тождественно равна 0. Доказать, что этот многочлен приводимый.

Решение. Производная монома $(x^n)' = nx^{n-1}$ тождественно равна 0 iff $n \equiv_p 0 \leftrightarrow p|n$;
$f' = 0 \rightarrow$ показатели степеней всех мономов многочлена f делятся на p; поэтому $f(x) = g(x^p) = g^p(x)$.

Задача № 10. Многочлен $x^5 + x^3 + x^2 + 1$ разложить на неприводимые множители над полем вычетов по мудулю 2.

Решение.

1. $f(x) = x^5 + x^3 + x^2 + 1, f(1) = 0 \rightarrow 1 -$ корень f
2. Делим f 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 № 11. Многочлен $f = x^3 + 2x^2 + 4x + 1$ разложить на неприводимые множители над полем $\mathbb{F}_5$.

Решение.

1. $f(2) = 25 \equiv_5 0, (x - 2) \equiv_5 (x + 3)$
2. $\frac{f}{x+3} = x^2 + 4x + 2$
3. $x^2 + 4x + 2$ - неприводимый многочлен над полем $\mathbb{F}_5$

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

Задача № 12. Многочлен $f = x^4 + x^3 + x + 2$ разложить на неприводимые множители над полем вычетов по модулю 3.

Решение.

1. 0,1,2 - не корни f. Значит, f не содержит линейных делителей.
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. $f(x) = (x^2 + 1)(x^2 + x + 2)$.

Задача № 13. Многочлен $f = x^4 + 3x^3 + 2x^2 + x + 4$ разложить на неприводимые множители над полем вычетов по модулю 5.

Решение.

1. 0,1,2,3,4 - не корни f, поэтому линейных делителей нет.
2. Перебирая неприводимые многочлены степени 2 над полем $\mathbb{F}_5$, получаем $f(x) = (x^2 + x + 1)(x^2 + 2x + 4)$

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

Задача № 14. Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены второй степени от x.

Решение.

- $f_1(x) = x^2 = x \cdot x$
- $f_2(x) = x^2 + 1 = (x + 1)^2$
- $f_3(x) = x^2 + x = x \cdot (x + 1)$
- $f_4(x) = x^2 + x + 1$ - неприводим

Задача № 15. Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены третьей степени от x.

Решение.

- $f_1(x) = x^3$
- $f_2(x) = x^3 + 1 = (x + 1)(x^2 + x + 1)$
- $f_3(x) = x^3 + x = x \cdot (x + 1)^2$
- $f_4(x) = x^3 + x^2 = x^2(x + 1)$
- $f_5(x) = x^3 + x + 1$ - неприводим
- $f_6(x) = x^3 + x^2 + 1$ - неприводим
- $f_7(x) = x^3 + x^2 + x = x(x^2 + x + 1)$
- $f_8(x) = x^3 + x^2 + x + 1 = (x + 1)^3$

Задача № 16. Найти все нормированные многочлены второй степени от x, неприводимые над полем вычетов по модулю 3.

Решение. Должно быть: $f(0) \neq 0, f(1) \neq 0, f(2) \neq 0$. Перебором коэффициентов в выражении x^2+bx+c находим подходящие многочлены:

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

Задача № 17. Найти все нормированные многочлены третьей степени от x, неприводимые над полем вычетов по модулю 3.

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

1. $f_1(x) = x^3 + 2x + 1$
2. $f_2(x) = x^3 + 2x + 2$
3. $f_3(x) = x^3 + x^2 + 2$
4. $f_4(x) = x^3 + 2x^2 + 1$

5. $f_5(x) = x^3 + x^2 + x + 2$
6. $f_6(x) = x^3 + x^2 + 2x + 1$
7. $f_7(x) = x^3 + 2x^2 + x + 1$
8. $f_8(x) = x^3 + 2x^2 + 2x + 2$

Задача № 18. Проверить, что $F = \mathbb{F}_7[x]/x^2 + x - 1$ является полем. Выразить обратный к $1 - x$ в F в базисе $\{\overline{1}, \overline{x}\}$.

Решение.

1. $f(x) = x^2 + x - 1, f(0) = 6, f(1) = 1, f(2) = 5, f(3) = 4, f(4) = 6, f(5) = 1, f(6) = 6 \rightarrow$ многочлен $f(x)$ - неприводим в $\mathbb{F}_7$ и F - поле $(= \mathbb{F}_7^2)$.
2. $\mathbb{F}_7^2 = \{ax + b | a, b \in \mathbb{F}_7, x^2 = 1 - x = 6x + 1\}$
   $(ax + b)(6x + 1) = ... = (2a + 6b)x + (6a + b) = 1$

$$\begin{cases} 6a+b=1 \\ a+3b=0 \end{cases} \rightarrow \begin{cases} a=1 \\ b=2 \end{cases} \quad (1)$$

Проверка. (6x+1)(x+2)=$6x^2 + 13x + 2 = 1 + 7x = 1$.

Задача № 19. Найти количество неприводимых многочленов: 1) степени 7 над полем $\mathbb{F}_2$; 2) степени 6 над полем $\mathbb{F}_5$; 3) степени 24 над полем $\mathbb{F}_3$.

Решение.

$$\sum_{m|n} m d_m = p^n$$

1. $\underline{d_7\text{-?}}$ $\sum\limits_{m|7} m d_m = 2^7 = 1 \cdot d_1 + 7 \cdot d_7 = 128.$
   $d_1 = 2$ $(x, x + 1) \rightarrow d_7 = (128 - 2)/7 = 126/7 = 18.$

Задача № 20. Чему равно произведение всех ненулевых элементов поля $\mathbb{F}_2^6$?

Решение. Все ненулевые элементы поля $\mathbb{F}_2^6$ являются корнями уравнения

$$x^{2^6-1} - 1 = x^{63} - 1 = 0. (*)$$

По т. Виета их произведение равно свободному члену, т.е. $-1 \equiv_2 1$.

Ответ. 1.

Задача № 21. Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(-2x^2+x+2)$ построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов. С помощью данной таблицы вычислить выражение: $\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}$

Решение. char $\mathbb{F}_3^2 = 3$, поэтому $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = f(x)$. $\mathbb{F}_3^2*$ содержит $3^2 - 1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1, 8}$ примитивног элемента α. Если элемент x окажется примитивным, то положим $\alpha = x$ и, поскольку вычисления в $\mathbb{F}_3^2$ проводятся по mod f(x), будем иметь $x^2 + x + 2 = 0 \rightarrow x^2 = -x - 2 = 2x + 1$.
$x^2 = 2x + 1$,
$x^3 = x \cdot x^2 = 2x^2 + x = 2(2x + 1) + x = 2x + 2$,

$x^4 = x \cdot x^3 = x(2x+2) = 2x^2 + 2x = 2(2x+1) + 2x = 2,$
$x^5 = x \cdot x^4 = 2x,$
$x^6 = x \cdot x^5 = 2x^2 = 2(2x+1) = x+2,$
$x^7 = x \cdot x^6 = x^2 + 2x = 2x + 1 + 2x = x+1,$
$x^8 = x \cdot x^7 = x2 + x = 2x + 1 + x = 1.$
- т.е. x - примитивный элемент; теперь вычислим значение выражения ($2^8 = 256 \equiv_3 1$) :

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} - \frac{x^7}{x^9x^6} = \frac{x^8}{x^2} - \frac{x^7x^8}{x^{15}} = x^6 - 1 = x + 2 - 1 = x + 1.$$

Ответ. $x+1$.

Задача № 22. Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(x^2+1)$ построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов поля.

Решение. В данном поле $x^2 + 1 = 0 \ \rightarrow x^2 = -1 \equiv_3 2$.
1) Найдем порядок элемента $x \rightarrow$ проверим степени, являющиеся делителями $3^2 - 1 = 8$, т.е. 2 и 4:

$$x^2 = 2, x^4 = 1.$$

Следовательно, элемент $degx = 4$ и x не является примитивынм элементом. Также не являются примитивынми все степени элемента $x : x^2 = 2, x^3 = 2x, x^4 = 1$.
2) Найдем порядок элемента $x+1$:

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

т.е. $(x+1)$ оказался примитивным элементом. Его степени:
$\alpha = x+1,$
$\alpha^2 = 2x,$
$\alpha^3 = 2x(x+1) = 2x+1,$
$\alpha^4 = (\alpha^2)^2 = 2,$
$\alpha^5 = 2(x+1) = 2x+2,$
$\alpha^6 = \alpha^2 \cdot \alpha^4 = x,$
$\alpha^7 = x(x+1) = x+2,$
$\alpha^8 = (\alpha^4)^2 = 1.$

Задача № 23. Чему равна сумма всех элементов поля $\mathbb{F}_3^7$?

Решение. Все элементы поля $\mathbb{F}_3^7$ являются корнями уравнения

$$x^{3^7} - x = x^{2187} - x = 0. (*)$$

По т. Виета их сумма равна коэффициенту перед x^{2186}, т.е. 0.

Ответ. 0.

Задача № 24. В поле $\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3)$ найти обратный элемент для $x^2 + x + 3$.

Решение. Проще всего обратный элемент можно найти путем решения уравнения:

$$(x^4 + x^3 + x^2 + 3) \cdot a(x) + (x^2 + x + 3) \cdot b(x) = 1 \quad (*)$$

с помощью расширенного алгоритма Евклида - тогда $b(x)$ будет искомым обратным элементом.
Замечание. Вычислять коэффициент при $x^4+x^3+x^2+3$ ($x_i(x)$) нет необходимости (нас интересует коэффициент только при x^2+x+3, т.е. $y_i(x)$).

1. $r_{-2}(x) = x^4+x^3+x^2+3$, //Инициализация
   $r_{-1}(x) = x^2+x+3$,
   $y_{-2}(x) = 0$,
   $y_{-1}(x) = 1$.
2. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,
   // Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком.
   $q_0(x) = x^2+5$,
   $r_0(x) = 2x+2$,
   $y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -x^2-5$.
3. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
   // 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:

$$(x^2+x+3)(4x^3+6x+1) = r_1(x) = 3.$$

Чтобы найти $b(x)$ нужно домножить $y_1(x)$ на $3^{-1} = 5$:

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

Проверка: $b(x)(x^2+x+3) = (6x^3+2x+5)(x^2+x+3) = 6x^5+6x^4+6x^3+4x+1 = 6x(-x^3-x^2-3) + 6x^4+6x^3+4x+1 = 1$.

Задача № 25. 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 $\mathbb{F}_2$:

$$f(0) = 1, f(1) = 1.$$

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

$$f(x) = (x^2+x+1)(x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1).$$

Продолжаем дальше делить на x^2+x+1:

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

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

$$g(x) = x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = (x^3+x+1)(x^6+x^5+x^3+x^2+1).$$

Производя далее попытки деления $h(x) = x^6 + x^5 + x^3 + x^2 + 1$, получаем

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

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

Так как многочлен $h(x)$ не имеет делителей 3-й и меньших степеней, то он является неприводимым. Т.к. при наличии, например, делителя степени 4, так же найдется и делитель степени 2.
В итоге $f(x)$ имеет разложение в $\mathbb{F}_2[x]$:

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

Задача № 26. Найти минимальное 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. Найдем разложение многочлена $f(x)$ на неприводимые множители над $\mathbb{F}_3$:

- Проверяем корни: $f(0) = 2, f(1) = 1, f(2) = 0$.
  Т.к. $(x - 2) \equiv_3 (x + 1)$, то $f(x) = (x + 1)(x^2 + 2x + 2)$.
- Найдем разложение многочлена $g(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$.
  Он не имеет корней, его степень $= 2 \ \rightarrow$ он неприводим.
- Окончательно $f(x) = (x + 1)(x^2 + 2x + 2)$.

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

- в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей -

  $$g(x) = (x - \alpha)(x - \alpha^p)(x - \alpha^{p^2}) \cdot \ldots \cdot (x - \alpha^{p^{n-1}}),$$

  где α - произвольный корень $g(x)$ в F.
- не имеет корней ни в каком конечном поле, содержащем менее, чем p^n элементов.

3. Рассмотрим поел $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2 + 2x + 2$. В этом поле если α - корень $g(x)$, то

- $\alpha^2 = -2\alpha - 2 = \alpha + 1$;
- $\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1$ - тоже корень $g(x)$.

Действительно (подчеркиваем слагаемые, дающие в сумме 0):

$(x-\alpha)(x-2\alpha-1) = (x+2\alpha)(x+\alpha+2) = x^2+\underline{\alpha x}+2x+\underline{2\alpha x}+2\alpha^2+4\alpha = x^2+2x+\underline{2\alpha}+2+\underline{4\alpha} = x^2+2x+2.$

Построенное расширение - поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ - содержит нацденный 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 $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ легко:
всегда можно взять $\alpha = x$,
откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.
5. Такимо образом, в поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ многочлен $f(x) = x^3 + x + 2$ имеет корни:

$$2, x \text{ и } 2x + 1.$$

13 Ответы

2.1.1. 1) полугруппа, но не группа; 2) полугруппа, но не группа; 3) полугруппа, но не группа; 4) группа; 5) группа; 6) группа; 7) группа; 8) не является полугруппой; 9) группа; 10) группа. **2.1.2.** 1) полугруппа, но не группа; 2) полугруппа, но не группа; 3) не является полугруппой; 4) полугруппа, но не группа; 5) полугруппа, но не группа; 6) полугруппа, но не группа; 7) группа; 8) группа; 9) не является полугруппой; 10) полугруппа, но не группа; 11) группа; 12) группа; 13) полугруппа, но не группа; 14) группа; 15) группа; 16) группа; 17) группа. **2.1.3.** 1) полугруппой не является; 2) полугруппой не является; 3) полугруппой не является; 4) полугруппа с единицей, но не группа. **2.1.4.** 1) полугруппой не является, 2) полугруппой не является. **2.1.5.** 1) Полугруппа, но (при $X \neq \varnothing$) не группа. Нейтральный элемент $\varnothing$. 2) Полугруппа, но (при$X \neq \varnothing$) не группа. Нейтральный элемент X. 3) Группа. Нейтральный элемент $\varnothing$. **2.1.6.** 1) группа; 2) группа; 3) операция не алгебраическая; 4) не является полугруппой.

2.2.1. 1) $\left(\begin{smallmatrix}1&2&3&4\\2&3&4&1\end{smallmatrix}\right)$, 2) $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\3&2&7&6&4&1&8&9&5\end{smallmatrix}\right)$, 3) (5,3,7,4,8,6,1), 4) (4,2,1)(6,5). **2.2.2.** 1) $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\4&9&8&1&10&6&3&5&7&2\end{smallmatrix}\right)$, 2) $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\8&9&7&4&10&1&2&3&6&5\end{smallmatrix}\right)$, 3) (2,1), 4) 4,3,7,6,2,1. **2.2.3.** 1) $[1^2, 6^1]$, 2) $[9^1]$, 3) $[1^2, 2^2, 4^1]$, 4) $[1^1, 3^1]$. **2.2.4.** 1) Нечетная, 2) Четная, 3) Нечетная, 4) Четная. **2.2.5.** 1) 23, 2) 19, 3) 20, 4) 1. **2.2.6.** 1) 3, 2) 4, 3) 7, 4) 4. **2.2.7.** 1) (3,2)(3,1)(3,5)(3,4), 2) (3,5)(3,2)(3,1)(3,4), 3) (5,13)(5,7)(5,11)(5,4)(6,1)(6,8)(6,12)(6,2)(6,10)(6,3)(6,9),
4) (7,8)(7,3)(7,5)(7,10)(7,6)(7,9)(7,4)(7,1)(7,2). **2.2.8.** 1) (3,4)(2,3)(3,4)(2,3)(4,5)(3,4)(2,3)(3,4)(4,5), 2) (2,3), 3) (1,2)(2,3)(1,2)(2,3), 4) (2,3)(4,5)(3,4)(4,5)(2,3)(1,2)(2,3)(3,4)(5,6)(4,5)(3,4)(4,5)(5,6). **2.2.9.** 1) 40, 2) 16, 3) 88, 4) 70, 5) 8, 6) 54, 7) 4, 8) 20, 9) 12, 10) 40. **2.2.10.** 1) $n!$; 2) $\frac{n!}{2}$, если $n \geq 2$.

6.1.1. 1) 8, 2) 42, 3) 16, 4) 46, 5) 10, 6) 8. **6.1.2.** 1) 22, 2) 9, 3) 36, 4) 7, 5) 1, 6) 25. **6.1.3.** 1) 3, 2) 11, 3) 31, 4) 41, 5) 3, 6) 7. **6.1.4.** 1) 0, 2) 1, 3) 1, 4) 1, 5) 1, 6) 1. **6.1.5.** 1) 6, 13, 20, 27, 34, 2) 18, 3) 4, 18, 4) 20, 5) 2, 6) 3, 11, 19, 27, 35. **6.1.6.** 1) 2, 2) 0, 3) 2, 4) 2, 5) 0, 6) 2. **6.1.7.** 1) Нет корней, 2) 3,14, 3) 16,27, 4) Нет корней, 5) Нет корней, 6) 18,25. **6.1.8.** 1) 0, 2) 0, 3) 2, 4) 0, 5) 0, 6) 2. **6.1.9.** 1) 5, 2) Нет корней, 3) Нет корней, 4) 2,8, 5) Нет корней, 6) Нет корней. **6.1.10.** 1) $\left(\begin{smallmatrix}27&34\\23&40\\8&37\end{smallmatrix}\right)$, 2) $\left(\begin{smallmatrix}19&41&7&42\\38&39&20&6\end{smallmatrix}\right)$, 3) $\left(\begin{smallmatrix}21&33\\6&26\end{smallmatrix}\right)$, 4) $\left(\begin{smallmatrix}24&5\\14&25\\26&1\end{smallmatrix}\right)$, 5) $\left(\begin{smallmatrix}21&28&39\\13&5&19\end{smallmatrix}\right)$, 6) $\left(\begin{smallmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&1&0&0\end{smallmatrix}\right)$. **6.1.11.** 1) 50, 2) 35. **6.2.1.** 1) $22x^5+27x^4+22x^3+17x^2+19x+7$, 2) $36x+31$, 3) $15x^3+30x^2+6$, 4) $13x^4+3x^3+10x^2+15x+13$. **6.2.2.** 1) $27x^5+18x^4+13x^3+4x^2+27x+7$, 2) $3x^5+4x^4+4x^3+x^2+x+6$, 3) $41x^3+2x^2+25x+24$, 4) $32x^4+4x^3+35x^2+2x+3$. **6.2.3.** 1) $33x^6+20x^5+21x^4+9x^3+15x^2+10x+41$, 2) $4x^7+4x^6+6x^5+8x^4+6x^3+x^2+9x+2$, 3) $15x^9+x^8+6x^7+19x^6+27x^5+23x^4+19x^3+2x^2+25x+29$, 4) $48x^3+25x^2+22x+32$.

10.1. 1) Кольцо, но не поле, 2) Не является кольцом, 3) Не является кольцом, 4) Не является кольцом, 5) Кольцо, но не поле, 6) Кольцо, но не поле, 7) Кольцо, но не поле, 8) Поле, 9) Не является кольцом, 10) Поле, 11) Поле, 12) Кольцо, но не поле, 13) Поле. **10.2.** 1) Кольцо, но не поле, 2) поле, 3) не является кольцом, 4) не является кольцом, 5) кольцо, но не поле, 6) поле. **10.3.** 1) группа; 2) полугруппа, но (если $K_6 = \{0\}$) не группа; 3) полугруппа, но (если $K_6 = \{0\}$) не группа; 4) полугруппа, но не группа. **10.4.** 1) -1, 2) -1, 3) -1, 4) 1, 5) 1, 6) 1, 7) 1, 8) 1, 9) -1, 10) -1. **10.5.** 1) 1, 2) 1, 3) 1, 4) 1, 5) 1, 6) -1, 7) 0, 8) -1, 9) 1, 10) 0. **10.6.** 1) 1, 2) 1, 3) 1, 4) 1, 5) -1, 6) -1, 7) 0, 8) 0, 9) 0, 10) 0. **10.7.1.** 1) $\left(\begin{smallmatrix}8&5&6&11\\12&11&4&12\end{smallmatrix}\right)$, 2) $\left(\begin{smallmatrix}5&2&7&10\\4&1&6&8\\1&0&9&9\end{smallmatrix}\right)$. **10.7.2.** 1) $\left(\begin{smallmatrix}34&19\\21&38\\25&24\\14&26\end{smallmatrix}\right)$, 2) $\left(\begin{smallmatrix}24&6&0&2\\2&30&31&23\\23&7&7&27\\7&8&24&42\end{smallmatrix}\right)$. **10.7.3.** 1) $\left(\begin{smallmatrix}34&12\\7&4\end{smallmatrix}\right)$, 2) $\left(\begin{smallmatrix}2&11&22\\22&15&21\\7&22&1\end{smallmatrix}\right)$. **10.7.4.** 1) 0, 2) 5. **10.7.5.** 1) $13x^3+28x^2+26x+16$, 2) x^3+5x^2+5x. **10.7.6.** 1) $7x^4+3x^3+6x^2+x+27$, 2) $41x+35$. **10.7.7.** 1) $34x^7+34x^6+32x^5+15x^4+x^3+2x^2+9x+41$, 2) $8x^7+14x^6+3x^5+5x^4+12x^3+18x^2+x+24$. **10.7.8.** 1) 0, 2) $10x^2+14x+13$. **10.7.9.** 1) $2x^3+4x^2+3x+4$, 2) 17. **10.7.10.** 1) 2, 2) 3.

14 Список литературы

1) Э.Б.Винберг КУРС АЛГЕБРЫ 2-е изд., испр. и доп. — М.: Изд-во «Факториал Пресс», 2001. — 544 с.

2) Ленг С. Алгебра. - М., Мир, 1968. - 572 с.

3) Глухов, М. М. Алгебра : учебник / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 608 с.

4) Федоровский, Константин Юрьевич. Алгебра [Электронный ресурс] : введение в теорию групп : курс лекций по дисциплине "Алгебра" : электронное учебное издание / К. Ю. Федоровский ; Московский гос. технический ун-т им. Н. Э. Баумана, Фак. "Фундаментальные науки", Каф. "Прикладная математика". - Москва : МГТУ им. Н. Э. Баумана, 2012. - 1 электрон. опт. диск (CD-ROM); 12 см.

5.1) Видео лекций по теории групп. Богданов И.И.

5.2) Конспект лекций по теории групп. Богданов И.И., Васильев А.

6) Вавилов Н. Конкретная теория групп.

7) Основы теории конечных групп, колец, полей : учебное пособие / М. И. Рожков ; Московский государственный институт электроники и математики (Технический университет). - Москва : Моск. гос. ин-т электроники и математики, 2009. - 82 с.

8) Сборник задач по алгебре / И. В. Аржанцев и др. Под ред. С23 А. И. Кострикина: Учеб. пособ. для вузов.-—Новое издание, исправленное. —М.: МЦНМО, 2009. —408 с.

9) Группы, кольца, поля. Н. Ю. Золотых, С. В. Сидоров. Электронное учебно-методическое пособие. — Нижний Новгород: Нижегородский госуниверситет, 2012. — 52 с.

10) Р. Лидл, Г. Нидеррайтер. Конечные поля. В 2-х томах. Том 1. - М., 1988, с. 430.

11) Ишмухаметов Ш.Т., Рубцова Р.Г. Вычисления в конечных полях: Учебно-методическое пособие/ Ш.Т. Ишмухаметов, Р.Г. Рубцова.– Казань: Казанский ун-т, 2019.– 23 с.

12) Анашкин А.В. Видео-лекции по теории групп, колец, полей