МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"МИРЭА - Российский технологический университет"
РТУ МИРЭА

Институт Кибернетики
Базовая кафедра №252 - Информационной безопасности

КУРСОВАЯ РАБОТА

По дисциплине: «Алгебраические модели в информационной безопасности»
Тема курсовой работы: **«Общая теория полей»**

Студент группы ККСО-03-19	Никишина А.А.	____________ (подпись)
Руководитель курсовой работы	Кожухов П.В.	____________ (подпись)

Работа представлена к защите «____» __________ 2021 г.
Допущен к защите «____» __________ 2021 г.

Москва 2021

Содержание

1. Кольца

1.1. Задача №1

Вариант №53

(Разложение)

Задание:

1) Найдите компоненты элементов a_1 , b_1 , c_1 кольца R.
2) Постройте изоморфизм f: $\mathbb{Z}/n$->.... как в следствии к Теореме 32 в ГЕН.

Следствие. $n = p_1^{\alpha_1}...p_k^{\alpha_k} - n \in \mathbb{N}$,
$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{\alpha_1} \oplus ... \oplus \mathbb{Z}/p_k^{\alpha_k}$$

а) Найдите f(a_2), f(b_2), f(c_2).

б) Найдите f^{-1}((a_3), (b_3), (c_3)).

Дано:

$a_1 = 80, b_1 = 345, c_1 = 171, R = \mathbb{Z}_{406}$

$n = 765,$

$a_2 = 131, b_2 = 445, c_2 = 353$

$a_3 = 7, b_3 = 2, c_3 = 16$

Решение:

1) Рассмотрим утверждение №29 параграфа №7

Утверждение. $R - |R||R| = p_1^{\alpha_1} \dots p_k^{\alpha_k}, k > 1, RI_s|I_s| = p_s^{\alpha_s}, s \in \overline{1,k}, R:$ $R = I_1 \dot{+} \dots \dot{+} I_k$

$\mathbb{Z}_{406}$ - конечное кольцо и $|\mathbb{Z}_{406}| = 2^1 \cdot 7^1 \cdot 29^1$. В кольце $\mathbb{Z}_{406}$ существует единственный идеал I_s порядка $|I_s| = p_s^{\alpha_s}$, где $p_s^{\alpha_s} \in 2^1, 7^1, 29^1, s \in \overline{1,3}$ и кольцо $\mathbb{Z}_{406}$ разложимо: $\mathbb{Z}_{406} = I_1 \dot{+} I_2 \dot{+} I_3$

$I_s = \{r \in R : p_s^{\alpha_s} r = 0\}$

$I_1 = \{0,\ 203\}$

$I_2 = \{0,\ 58,\ 116,\ 174,\ 232,\ 290,\ 348\}$

$I_3 = \{0, 14, 28, 42, 56, 70, 84, 98, 112, 126, 140, 154, 168, 182, 196, 210, 224, 238, 252, 266, 280, 294, 308, 322, 336, 350, 364, 378, 392\}$

Так как $(|I_1|, |I_2|, |I\ 3\ |) = 1$ по критерию взаимной простоты существуют $a, b, c \in \mathbb{Z}_{406} : 1 = 203a + 58b + 14c$

a = 1, b = -3, c = -2 - данные значения получены через расширенный алгоритм Евклида.

$1 = 203\cdot 1 + 58\cdot(-3) + 14\cdot(-2) \mod (406)$

$1 = 203 + 232 + 378 \mod (406)$

Находим остальные компоненты элементов кольца.

Умножаем полученное сверху выражение на элемент кольца и приводим по модулю 406.

80 = 0 + 290 + 196

345 = 203 + 58 + 84

171 = 203 + 290 + 84

2) $n = 765 = 3^2\cdot 5^1\cdot 17^1$

Введём отображение $f : \mathbb{Z}/765 \to \mathbb{Z}/9 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/17$ по правилу

$f([x]_{765}) = ([x]_9, [x]_5, [x]_{17})$

Проверим на условие гомоморфизма:

$f([a]765\cdot [b]765) = f([a\cdot b]765) = ([a\cdot b]9, [a\cdot b]5, [a\cdot b]17) =$

$= ([a]9\cdot [b]9, [a]5\cdot [b]5, [a]17\cdot [b]17) = ([a]9, [a]5, [a]17)\cdot ([b]9, [b]5, [b]17) =$

$= f([a]765)\cdot f([b]765)$

Так как (9, 5, 17) = 1, то применима китайская теорема об остатках, а значит, существует единственное отображение в $\mathbb{Z}/765$, следовательно, отображение является инъективным и так как: $|\mathbb{Z}/765| = |\mathbb{Z}/9 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/17|$, то биективным. То отображение является изоморфным.

$f(a_2) = f(131) = ([131]_9, [131]_5, [131]_{17}) = ([5]_9, [1]_5, [12]_{17})$

$f(b_2) = f(445) = ([445]_9, [445]_5, [445]_{17}) = ([4]_9, [0]_5, [3]_{17})$

$f(c_2) = f(353) = ([353]_9, [353]_5, [353]_{17}) = ([2]_9, [3]_5, [13]_{17})$

Необходимо решить систему сравнений:

$$\begin{cases} x \equiv 7 \mod (9) \\ x \equiv 2 \mod (5) \\ x \equiv 16 \mod (17) \end{cases}$$

а) $x \equiv 7 \mod (9) \Rightarrow [7]_9 = 7 + 9t_1 | t_1 \in \mathbb{Z}$

б) $x \equiv 2 \mod (5) \Rightarrow 7 + 9t_1 \equiv 2 \mod (5) \Rightarrow 4t_1 \equiv 0 \mod (5) \Rightarrow$
$t_1 \equiv 0 \mod (5) = \{7 + 9t_1\} = \{7 + 9(5t_2) | t_2 \in \mathbb{Z}\} = \{7 + 45t_2 | t_2 \in \mathbb{Z}\}$

в) $x \equiv 16 \mod (17) \Rightarrow 7{+}45t_2 \equiv 16 \mod (17) \Rightarrow 11t_2 \equiv 9 \mod (17) \Rightarrow$
$t_2 \equiv 7 \mod (17) = \{7 + 45(7 + 17t_3) | t_3 \in \mathbb{Z}\} = \{322 + 765t_3 \in \mathbb{Z}\} =$
$[322]_{765}$
$f^{-1}(7, 2, 16) = [322]_{765}$

1.2. Задача №2

Вариант №21

(Факторкольца)

Задание:

Построить факторкольца P[x]/f_1(x), P[x]/f_2(x). Определить являются ли они полями. Если факторкольца конечны, то выписать таблицы Кэли, если бесконечны, то описать элементы факторколец. Указать делители нуля и обратимые элементы (с обратными элементами).

Дано:

$\mathrm{P} = \mathrm{GF}(3) = \{0, e, \alpha\}$, $\quad f_1(x) = x^2 + e$, $\quad f_2(x) = x^2 + x + e$

Решение:

P = GF(3) - это поле Галуа из трёх элементов и так как оно является полем простого порядка, то изоморфно кольцу вычетов $\mathbb{Z}/3$.

1) Найдём корни f_1(x).
$GF(3)[x] \cong \mathbb{Z}_3/x^2 + e$ поэтому строим таблицы Кэли.

$+$	0	e	α
0	0	e	α
e	e	α	0
α	α	0	e

$\cdot$	0	e	α
0	0	0	0
e	0	e	α
α	0	α	e

По таблицам Кэли не находим ни одного корня многочлена, значит по критерию неприводимости многочленов, $f_1(x)$ неприводим над полем, поэтому факторкольцо GF(3)[x]/f$_1(x)$ будет изоморфно полю GF(3^2)=GF(9).
$P[x]/f_1(x) =$
$\{[0]_{f_1(z)}, [e]_{f_1(z)}, [\alpha]_{f_1(z)}, [ex]_{f_1(z)}, [ex{+}e]_{f_1(z)}, [ex{+}\alpha]_{f_1(z)}, [\alpha x]_{f_1(z)}, [\alpha x{+}e]_{f_1(z)},$ $[\alpha x + \alpha]_{f_1(z)}, \}$, у поля нет делителей нуля.

$+$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$
$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$
$[e]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$
$[\alpha]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$
$[ex]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$
$[ex+e]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$
$[ex+\alpha]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$
$[\alpha x]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$
$[\alpha x+e]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$
$[\alpha x+\alpha]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$

$+$	$[ex+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$
$[0]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$
$[e]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$
$[\alpha]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$
$[ex]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$
$[ex+e]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$
$[ex+\alpha]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$
$[\alpha x]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$
$[\alpha x+e]_{f_1(z)}$	$[0]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$
$[\alpha x+\alpha]_{f_1(z)}$	$[e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$

$\cdot$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$
$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[0]_{f_1(z)}$
$[e]_{f_1(z)}$	$[0]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$
$[\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$
$[ex]_{f_1(z)}$	$[0]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$
$[ex+e]_{f_1(z)}$	$[0]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$
$[ex+\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[e]_{f_1(z)}$
$[\alpha x]_{f_1(z)}$	$[0]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$
$[\alpha x+e]_{f_1(z)}$	$[0]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$
$[\alpha x+\alpha]_{f_1(z)}$	$[0]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[ex]_{f_1(z)}$

$\cdot$	$[ex+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$
$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[0]_{f_1(z)}$	$[0]_{f_1(z)}$
$[e]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$
$[\alpha]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[ex+e]_{f_1(z)}$
$[ex]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[e]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$
$[ex+e]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha x+e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$
$[ex+\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$
$[\alpha x]_{f_1(z)}$	$[ex+e]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[\alpha]_{f_1(z)}$
$[\alpha x+e]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$	$[\alpha x+\alpha]_{f_1(z)}$	$[ex]_{f_1(z)}$	$[e]_{f_1(z)}$
$[\alpha x+\alpha]_{f_1(z)}$	$[ex+\alpha]_{f_1(z)}$	$[\alpha]_{f_1(z)}$	$[e]_{f_1(z)}$	$[\alpha x]_{f_1(z)}$

Обратимые элементы:

α, обратный: α;

ex, обратный: αx;

$\alpha x + e$, обратный: $\alpha x + \alpha$.

2) Многочлен f_2(x) приводим, следовательно, GF(3)[x]/f_2(x) будет кольцом, а не полем.
P[x]/f_2(x) $= \{[0]_{f_1(z)}, [e]_{f_1(z)}, [\alpha]_{f_1(z)}, [ex]_{f_1(z)}, [ex{+}e]_{f_1(z)}, [ex{+}\alpha]_{f_1(z)}, [\alpha x]_{f_1(z)}, [\alpha x + e]_{f_1(z)}, [\alpha x + \alpha]_{f_1(z)}, \}$.

$\cdot$	$[0]_{f_2(z)}$	$[e]_{f_2(z)}$	$[\alpha]_{f_2(z)}$	$[ex]_{f_2(z)}$	$[ex+e]_{f_2(z)}$
$[0]_{f_2(z)}$	$[0]_{f_2(z)}$	$[0]_{f_2(z)}$	$[0]_{f_2(z)}$	$[0]_{f_2(z)}$	$[0]_{f_2(z)}$
$[e]_{f_2(z)}$	$[0]_{f_2(z)}$	$[e]_{f_2(z)}$	$[\alpha]_{f_2(z)}$	$[ex]_{f_2(z)}$	$[ex+e]_{f_2(z)}$
$[\alpha]_{f_2(z)}$	$[0]_{f_2(z)}$	$[\alpha]_{f_2(z)}$	$[e]_{f_2(z)}$	$[\alpha x]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$
$[ex]_{f_2(z)}$	$[0]_{f_2(z)}$	$[ex]_{f_2(z)}$	$[\alpha x]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$	$[\alpha]_{f_2(z)}$
$[ex+e]_{f_2(z)}$	$[0]_{f_2(z)}$	$[ex+e]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$	$[\alpha]_{f_2(z)}$	$[ex]_{f_2(z)}$
$[ex+\alpha]_{f_2(z)}$	$[0]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$
$[\alpha x]_{f_2(z)}$	$[0]_{f_2(z)}$	$[\alpha x]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$	$[ex+e]_{f_2(z)}$	$[e]_{f_2(z)}$
$[\alpha x+e]_{f_2(z)}$	$[0]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[ex]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$
$[\alpha x+\alpha]_{f_2(z)}$	$[0]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$	$[ex+e]_{f_2(z)}$	$[e]_{f_2(z)}$	$[\alpha x]_{f_2(z)}$

$\cdot$	$[ex+\alpha]_{f_2(z)}$	$[\alpha x]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$
$[0]_{f_2(z)}$	$[0]_{f_2(z)}$	$[0]_{f_2(z)}$	$[0]_{f_2(z)}$	$[0]_{f_2(z)}$
$[e]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[\alpha x]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$
$[\alpha]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[ex]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[ex+e]_{f_2(z)}$
$[ex]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[ex+e]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[e]_{f_2(z)}$
$[ex+e]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[e]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[\alpha x]_{f_2(z)}$
$[ex+\alpha]_{f_2(z)}$	$[0]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[0]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$
$[\alpha x]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[\alpha x+\alpha]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[\alpha]_{f_2(z)}$
$[\alpha x+e]_{f_2(z)}$	$[0]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[0]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$
$[\alpha x+\alpha]_{f_2(z)}$	$[ex+\alpha]_{f_2(z)}$	$[\alpha]_{f_2(z)}$	$[\alpha x+e]_{f_2(z)}$	$[ex]_{f_2(z)}$

По таблицам Кэли найдём обратимые элементы:

α, обратный: α;

ex, обратный: $\alpha x+\alpha$.

Также, с помощью таблиц Кэли найдём делители нуля:

$ex+\alpha$ и $\alpha x+e$.

1.3. Задача №3

Вариант №12

(Изучение структур)

Задание:

Являются ли R_1 , R_2 полями или кольцами (выполняется ли коммутативность, есть ли единица, какие элементы не обратимы)?

Если да, то в R_1 , R_2 найти (не менее 3, если возможно) собственные идеалы и (не менее 3, если возможно) собственные подкольца, не являющиеся идеалами (если идеалы и такие подкольца существуют). Являются ли данные кольца кольцами главных идеалом?

(необходимо все обосновать и доказать)

Дано:

$R_1 = 8\mathbb{Z}$, $R_2 = \mathbb{Z}_2[x]$

Решение:

Определение. *Кольцом называется множество R с бинарными операциями сложения $+$ и умножения $\cdot$, удовлетворяющими условиям:*

1) $(R; +)$ — абелева группа,

2) $(R; \cdot)$ — полугруппа,

3) операция умножения дистрибутивна относительно сложения.

При этом группа $(R; +)$ называется аддитивной группой кольца R, а ее нейтральный элемент 0 — нулем кольца R.

Кольцо $(R; +)$ называется коммутативным, если операция умножения коммутативна, и кольцом с единицей, если $(R; \cdot)$ — полугруппа с единицей.

Определение. *Полем называют коммутативное кольцо с единицей, отличной от нуля, в котором каждый ненулевой элемент обратим.*

1) Рассмотрим структуру $R_1 = 8\mathbb{Z}$ - данная структура является множеством целых чисел, кратных 8.

   Проверим, является ли она кольцом:

а) Замкнутость относительно сложения:
$\forall 8a, 8b \in R_1 : 8a + 8b = 8c \in R_1$

б) Замкнутость относительно умножения:
$\forall 8a, 8b \in R_1 : 8a \cdot 8b = 8c \in R_1$

в) Коммутативность сложения:
$\forall 8a, 8b \in R_1 : 8a + 8b = 8b + 8a$

г) Ассоциативность сложения:
$\forall 8a, 8b, 8c \in R_1 : (8a + 8b) + 8c = 8a + (8b + 8c)$

д) Существование нейтрального элемента:
$\exists 0 \in R_1 : \forall 8a \in R_1 : 0 + 8a = 8a$

е) Существование противоположного элемента:
$\forall 8a \in R_1 \exists (-8a) \in R_1 : 8a + (-8a) = 0$

ж) Ассоциативность умножения:
$\forall 8a, 8b, 8c \in R_1 : (8a \cdot 8b) \cdot 8c = 8a \cdot (8b \cdot 8c)$

з) Правая дистрибутивность умножения относительно сложения:
$\forall 8a, 8b, 8c \in R_1 : (8a + 8b) \cdot 8c = 8ac + 8bc$

и) Левая дистрибутивность умножения относительно сложения:
$\forall 8a, 8b, 8c \in R_1 : 8a \cdot (8b + 8c) = 8ab + 8ac$

Значит, R_1 - кольцо. Проверим, является ли структура R_1 полем.

а) Коммутативность умножения:
$\forall 8a, 8b \in R_1 : 8a \cdot 8b = 8b \cdot 8a$

б) Существование единицы:
$\nexists e \in R_1 : \forall 8a \in R_1 \setminus \{0\} : 8a \cdot e = e \cdot 8a = 8a$

Так как условия поля не выполнены, то R_1 не является полем. Так как $8\mathbb{Z} \cong \mathbb{Z}$, а в $\mathbb{Z}$ идеалами являются , то в нашем случае идеалы будут выглядеть как $(8n) \cdot \mathbb{Z}, n \in \mathbb{Z}$.

Найдём 3 собственных идеала:
$(8 \cdot 2)\mathbb{Z} = 16\mathbb{Z}$
$(8 \cdot 3)\mathbb{Z} = 24\mathbb{Z}$

$(8\cdot 4)\mathbb{Z} = 32\mathbb{Z}$

Данные идеалы являются главными, так как они порождены элементом 8n.

Собственных подколец, не являющихся идеалами – нет.

Следовательно, R_1 является кольцом главных идеалов.

2) Рассмотрим структуру $R_2 = \mathbb{Z}_2[x]$

Данная структура является множеством многочленов по модулю 2.

Проверим, является ли она кольцом.

а) Замкнутость относительно сложения:
$\forall f_1(x), f_2(x) \in R_2 : f_1(x) + f_2(x) = f_3(x) \in R_2$

б) Замкнутость относительно умножения:
$\forall f_1(x), f_2(x) \in R_2 : f_1(x)\cdot f_2(x) = f_3(x) \in R_2$

в) Коммутативность сложения:
$\forall f_1(x), f_2(x) \in R_2 : f_1(x) + f_2(x) = f_2(x) + f_1(x)$

г) Ассоциативность сложения:
$\forall f_1(x), f_2(x), f_3(x) \in R_2 : (f_1(x) + f_2(x)) + f_3(x) = f_3(x) + (f_2(x) + f_3(x))$

д) Существование нейтрального элемента:
$\exists 0 \in R_2 : \forall f(x) \in R_2 : 0 + f(x) = f(x)$

е) Существование противоположного элемента:
$\forall f(x) \in R_2 \exists (-f(x)) \in R_2 : f(x) + (-f(x)) = 0$

ж) Ассоциативность умножения:
$\forall f_1(x), f_2(x), f_3(x) \in R_2 : (f_1(x)\cdot f_2(x))\cdot f_3(x) = f_1(x)\cdot (f_2(x)\cdot f_3(x))$

з) Правая дистрибутивность умножения относительно сложения:
$\forall f_1(x), f_2(x), f_3(x) \in R_2 : (f_1(x) + f_2(x))\cdot f_3(x) = f_1(x)\cdot f_3(x) + f_2(x)\cdot f_3(x)$

и) Левая дистрибутивность умножения относительно сложения:
$\forall f_1(x), f_2(x), f_3(x) \in R_2 : f_1(x)\cdot (f_2(x) + f_3(x)) = f_1(x)\cdot f_2(x) + f_1(x)\cdot f_3(x)$

Значит, R_2 - кольцо. Проверим, является ли структура R_2 полем.

а) Коммутативность умножения:
$\forall f_1(x), f_2(x) \in R_2 : f_1(x)\cdot f_2(x) = f_2(x)\cdot f_1(x)$

б) Существование единицы:
$\exists e \in R_2 : \forall f(x) \in R_2 \setminus \{0\} : f(x)\cdot e = e\cdot f(x) = f(x)$

в) Обратимость эл-тов:
$\sqsupset\ f_1(x) = x \in R_2 : \forall f_2(x) \in R_2 : f_1(x)\cdot f_2(x) \neq 1 \Rightarrow R_2$ не является полем

У $R_2\quad \exists$ подкольца вида $[\alpha_n x^n + \ldots + \alpha_1 x]_2, n \in \mathbb{N}\setminus\{0\}, \alpha_n \in \mathbb{Z}_2$ и подкольцо $\mathbb{Z}_2$. Не собственных идеалов не существует.

1.4. Задача №4

Вариант №39

Задачник Шишкова А.Б. задача № 4.8 пункт «в».

Задание:

Пусть $a_1, ..., a_k \in \mathbb{Z}$. Докажите, что $a_1\mathbb{Z} \cap ... \cap a_k\mathbb{Z} = m\mathbb{Z}$, где $m = [a_1, ..., a_k]$ - наименьшее общее кратное чисел $a_1, ..., a_k$.

Решение:

Для доказательства воспользуемся определением пересечения множеств (определение №2 §2 главы 1), согласно которому:

Определение. *Пересечением множеств A, B называется множество $A \cap B$, состоящее из всех тех элементов, которые содержатся в обоих множествах A, B : $A \cap B = m : m \in A$ и $m \in B$.*

По аналогии можем определить пересечение семейства множеств:
$\{a_i : i \in A\}$, где А - любое множество индексов.
$\underset{i\in A}{\cap} a_i = \{b : b \in a_i,$ для всех $i \in A\}$.
Если при пересечении множеств каждый элемент итогового множества должен принадлежать ко всем пересекаемым множествам, то с помощью ММИ докажем, что в нашем случае так как множества $a_i\mathbb{Z}$ представляют собой бесконечный набор чисел кратных a_i, справедливо утверждать, что элементы должны

принадлежать к $[a_1, ..., a_k]$.
При k=2: $2\mathbb{Z} \cap 3\mathbb{Z} = \{\ldots, -6, 0, 6, 12, 18, 24, 30, 36, 42, 48, \ldots\} = 6\mathbb{Z} = [2, 3]\mathbb{Z}$.
Предположим, что при k=n справедливо: $a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z} = [a_1, ..., a_n]\mathbb{Z}$.
При k=n+1: $a_1\mathbb{Z}\cap\ldots\cap a_n\mathbb{Z}\cap a_{n+1}\mathbb{Z} = [a_1, ..., a_n]\mathbb{Z}\cap a_{n+1}\mathbb{Z} = [[a_1, ..., a_n], a_{n+1}]\mathbb{Z} =$
$= [a_1, ..., a_{n+1}]\mathbb{Z}$.
Следовательно, $a_1\mathbb{Z} \cap ... \cap a_k\mathbb{Z} = [a_1, ..., a_k]\mathbb{Z} = m\mathbb{Z}$.

1.5. Задача №5

Вариант №8
Общая теория колец
Задание:
$I_\alpha \lhd R, \alpha \in A \Rightarrow \bigcap\limits_{\alpha\in A} I_\alpha \lhd R$
Решение:
Воспользуемся утверждением №12 §3 главы 20.

Утверждение. *Если $\{I_\alpha : \alpha \in A\}$ — произвольное семейство идеалов кольца R, то $T = \bigcap\limits_{\alpha\in A} I_\alpha$ — идеал кольца R.*

Докажем это с помощью утверждения №6 §1 главы 20.

Утверждение. *Если $\{S_\alpha : \alpha \in A\}$ — произвольное семейство подколец кольца R, то $T = \bigcap\limits_{\alpha\in A} S_\alpha$ — подкольцо кольца R.*

Так как согласно определению идеала, (определение №3 §3 главы 20)

Определение. *Идеалом кольца R называют любое его подкольцо I, удовлетворяющее условию: $\forall i \in I, \forall r \in R(ir \in I, ri \in I)$, т. е. выдерживающее умножение на элементы кольца R (обозначение: $I \lhd (R, +,)$ или $I \lhd R$).*

идеалы являются подкольцами кольца R следует, что для них справедливо утверждение №6.
$\sqsupset I_i = \{i{\cdot}\, a : \forall a \in R, \forall i \in R\} \lhd R \wedge I_j = \{j{\cdot}\, a : \forall a \in R, \forall j \in R\} \lhd R :$
$I_i{\cap}I_j = \{[i, j]{\cdot}\, a : \forall a \in R\, [i, j]{\cdot}\, a \in I_i{\cap}I_j\} = H \lhd R \Rightarrow$, а значит и утверждение №11 выполняется соответственно.
Исходя из этого мы можем доказать, что $I_\alpha \lhd R, \alpha \in A \Rightarrow \bigcap\limits_{\alpha\in A} I_\alpha \lhd R$.

2. Поля

2.1. Задача №1

Вариант №21

Задание:

1) Найти минимальный многочлен $m_{a,P[x]}$

2) Найти минимальный многочлен $m_{b,H[x]}$, где H - простое подполе поля T

Дано:

$a = 7, P = Z_2$

$b = 4y + 1, T = \mathbb{Z}_7[y]/y^2 + 5y + 3$

Решение:

Рассмотрим определение №9 §5 главы 21

Определение. *Если P' , P - поля, $P \subset$ P' и $\alpha \in$P' - алгебраический над P элемент, то единственный унитарный неприводимый над полем P многочлен, корнем которого является α, называют минимальным многочленом элемента α над полем P и обозначают через $m_{a,P[x]}$.*

1) $7 = 111_2 = y^2 + y + 1$

   $y^2 + y + 1 \in GF(8) = \mathbb{Z}_2[y]/y^3 + y + 1$

   $m_{a,\mathbb{Z}_2[y]} = y^3 + \alpha y^2 + \beta y + \gamma$

   $(y^2 + y + 1)^3 + \alpha(y^2 + y + 1)^2 + \beta(y^2 + y + 1) + \gamma \equiv 0 \mod (y^3 + y + 1)$

   $y^6+3y^5+(\alpha+6)y^4+(2\alpha+7)y^3+(3\alpha+\beta+6)y^2+(2\alpha+\beta+3)y+\alpha+\beta+\gamma+1 \equiv 0 \mod (y^3 + y + 1)$

   $y^6+3y^5+(\alpha)y^4+y^3+(\alpha+\beta)y^2+(\beta+1)y+\alpha+\beta+\gamma+1 \equiv 0 \mod (y^3+y+1)$

   $\alpha y^4 + (\alpha + \beta)y^2 + (\beta + 1)y + \alpha + \beta + \gamma \equiv 0 \mod (y^3 + y + 1)$

   $\beta y^2 + (\alpha + \beta + 1)y + \alpha + \beta + \gamma \equiv 0 \mod (y^3 + y + 1) \quad \Rightarrow$

   $\Rightarrow \quad \beta = 0, \quad \alpha+\beta+1 = 0, \quad \alpha+\beta+\gamma = 0 \quad \Rightarrow \quad \beta = 0, \quad \alpha = 1, \quad \gamma = 1.$

   $m_{a,\mathbb{Z}_2[y]} = y^3 + y^2 + 1.$

2) Пусть $m = x^2 + \alpha x + \beta$, посчитаем $m_{b,H[x]} = (4y+1)^2 + \alpha(4y+1) + \beta$
$(4y+1)^2 + \alpha(4y+1) + \beta \equiv 0 \mod (y^2+5y+3)$
$16y^2 + y(8+4\alpha) + 1 + \alpha + \beta \equiv 0 \mod (y^2+5y+3)$
$2y^2 + (1+4\alpha)y + 1 + \alpha + \beta \equiv 0 \mod (y^2+5y+3)$
$2(y^2 + (4+2\alpha)y + 4(1+\alpha+\beta)) \equiv \mod (y^2+5y+3) \Rightarrow$
$\Rightarrow 4 + 2\alpha = 5, \quad 4(1+\alpha+\beta) = 3 \quad \Rightarrow \quad \alpha = 4, \quad \beta = 1.$
$m_{b,H[x]} = x^2 + 4x + 1$; Простое подполе в Т есть $H = \mathbb{Z}_7$

2.2. Задача №2

Вариант №17

Задание:

1) Найти минимальное поле разложение T многочлена $f(x) \in P[x]$.

2) Разложить $f(x)$ над полем .

3) Найти $[T : P]$

Дано:

$f(x) = x^3 + x^2 + 3x + 6, \qquad P = Z_7$

Решение:

1) Разложим многочлен по $\mathbb{Z}_7$ (подставим элементы поля).
f(0)=6; f(1)=4; f(2)=3; f(3)=2; f(4)=0; f(5)=3; f(6)=3.
$f(x) = x^3 + x^2 + 3x + 6 = (x+3)(x^2+5x+2)$
Аналогично разложим $x^2 + 5x + 2$ в P.
f(0)=2; f(1)=1; f(2)=2; f(3)=5; f(4)=3; f(5)=3; f(6)=5.
Все значения ненулевые – многочлен является неприводимым. $\mathbb{Z}_7$ не является минимальным полем разложения этого многочлена:
$f(x) = (x+3)(x^2+5x+2)$
Пусть $[y]_{y^2+5y+2}$ это корень многочлена $f_1(x)$ в поле $\mathbb{Z}[x]([y]_{y^2+5y+2})$. По теореме о корнях неприводимого многочлена получаем:
Так как $f_1(x) = x^2 + 5x + 2$ неприводимый многочлен степени 2 над полем $P = \mathbb{Z}_7$ и $[y]_{y^2+5y+2} \in \mathbb{Z}_7/f_1(x)$ - это корень многочлена $f_1(x)$ в поле

$\mathbb{Z}_7([y]_{y^2+5y+2})$, тогда $S = P([y]_{y^2+5y+2}) = \mathbb{Z}[x]([y]_{y^2+5y+2})$ - расширение поля P, порождённое корнем $[y]_{y^2+5y+2}$ многочлена $f_1(x)$. Тогда $S = T$ - минимальное поле разложения многочлена $f_1(x)$ над $P = \mathbb{Z}_3[x]$, причём $f_1(x)$ имеет в S 2 корня:
$([y]_{y^2+5y+2})^{2^0}, ([y]_{y^2+5y+2})^{2^1}$:

а) $([y]_{y^2+5y+2})^{2^0} = [y]_{y^2+5y+2}$

б) $([y]_{y^2+5y+2})^{2^1} = [y+1]_{y^2+5y+2}$

Тогда $f_1(x)$ представим в поле T как
$f_1(x) = (x - ([y]_{y^2+5y+2})^{2^0})(x - ([y]_{y^2+5y+2})^{2^1}) =$
$= (x - [y]_{y^2+5y+2})(x - [y+1]_{y^2+5y+2}) = (x + 6[y]_{y^2+5y+2})(x + 6[y+1]_{y^2+5y+2})$
А значит, $f(x)$ можно разложить над полем T:
$f(x) = (x + [6y]_{y^2+5y+2})(x + [6y+6]_{y^2+5y+2})$
По утверждению о степени простого расширения поля, порождённого алгебраическим элементом $[T : P] = deg(m_{\alpha,P(x)})$. Отметим, что $f_1(x)$ является минимальным многочленом элемента $[y]_{y^2+5y+2}$ над полем $\mathbb{Z}_3(x)$ по определению, так как он унитарный, неприводимый, $[y]_{y^2+5y+2}$ - его корень $\Rightarrow deg(f_1(x)) = 2$, значит $[T : P] = 2$.

2.3. Задача №3

Вариант №14
(Изоморфизм полей)
Задание:

1) Приводимы или неприводимы многочлены $f_1(x)$ и $f_2(x)$ в $\mathbb{Z}_k[x]$

2) Если оба многочлена неприводимы, то постройте в явном виде изоморфизм полей $\mathbb{Z}_k[x]/f_1(x) \longrightarrow \mathbb{Z}_k[x]/f_2(x)$

Дано:
$f_1(x) = x^4 + 4x^3 + 3x^2 + 3, \qquad f_2(x) = x^4 + x^3 + x + 3, \qquad k = 5$
Решение:

1) Докажем неприводимость многочленов.

а) Проверим приводимость многочлена $f_1(x)$
$f_1(x) = x^4 + 4x^3 + 3x^2 + 3$
$f_1(0) = 3; f_1(1) = 1; f_1(2) = 3; f_1(3) = 4; f_1(4) = 3.$
Так как многочлен не обнуляется при подстановке всех элементов поля $\mathbb{Z}/5$, он неприводим над $\mathbb{Z}/5$.

б) Проверим приводимость многочлена $f_1(x)$
$f_2(x) = x^4 + x^3 + x + 3$
$f_1(0) = 3; f_1(1) = 1; f_1(2) = 4; f_1(3) = 4; f_1(4) = 2$
Так как многочлен $f_2(x)$ не зануляется при подстановке всех элементов поля $\mathbb{Z}/5$, он неприводим над $\mathbb{Z}/5$.

2) $\varphi : \mathbb{Z}_k[x]/f_1(x) \longrightarrow \mathbb{Z}_k[x]/f_2(x)$
Оба многочлена раномощны и их мощность равна $5^4 = 625$. Факторизунм $625 - 1 = 624 = 2^4 \cdot 3 \cdot 13$.
$P_1 = \mathbb{Z}_5/f_1(x), P_2 = \mathbb{Z}_5/f_2(x)$
Проверим будет ли $x \in P_1$ являться примитивным элементом.
$x^{\frac{624}{2}} = x^{312} \qquad x^{\frac{624}{3}} = x^{208} \qquad x^{\frac{624}{13}} = x^{48}$
$x^{312} \mod (x^4 + 4x^3 + 3x^2 + 3) = 4$
$x^{208} \mod (x^4 + 4x^3 + 3x^2 + 3) = x^3 + 4x + 3$
$x^{48} \mod (x^4 + 4x^3 + 3x^2 + 3) = 3x^3 + 4x^2 + x$
Следовательно, $x \in P_1$ является примитивным элементом и так же, можно сказать, что x^α, где $(\alpha, 624) = 1$. Так же их количество будет равно $\phi(624) = 192$.

Далее проверим, является ли $x \in P_2$ примитивным
$x^{312} \mod (x^4 + x^3 + x + 3) = 4$
$x^{208} \mod (x^4 + x^3 + x + 3) = 4x^3 + x^2 + 2$
$x^{48} \mod (x^4 + x^3 + x + 3) = 2x^3 + x^2$

Построим минимальный многочлен $f(x) = x^3 + 2x^2 + 1$
Проверим приводим он или нет.
f(0)=1; f(1)=4; f(2)=2; f(3)=1; f(4)=2.

По критерию неприводимости - многочлен неприводим.
$m_{x,\mathbb{Z}_5[x]}(x) = x^3 + 2x^2 + 1$
$\phi : P_1 \longrightarrow P_2$: примитивные многочлены в степени n равны и $\phi(a\cdot b) = \phi(a)\cdot \phi(b) \Rightarrow \phi$ - изоморфизм.

2.4. Задача №4

Вариант №21

Задание:
(Неприводимый многочлен большой степени)
Постройте неприводимый многочлен над P степени k. (с конструктивным алгоритмом построения)
Дано:
$P = \mathbb{Z}_3, k = 30$
Решение:
Степень k=30 не подходит для построения по алгоритму, так как, согласно условию алгоритма, $deg(f(x)) = 3^n - 1$.
Поэтому рассмотрим элементы поля для подбора степеней многочлена.

- 0, при возведении в любую степень остаётся неизменным.
- 1, также не меняется при возведении в степень.
- 2, остаётся неизменным в нечётных степенях и превращается в 1 в чётных.

Многочлен степени n является неприводимым над $P = \mathbb{Z}_p$, когда $\forall k \in \overline{1, m}$, $m = [\frac{n}{2}] \Rightarrow d(x) = (f(x), u^{p^k}) \mod (f(x) - x) = 1$
Допустим $x^{30} + x + 2$ - неприводимый многочлен.
$x^3 \mod (x^{30} + x + 2) = x^3$
$x^9 \mod (x^{30} + x + 2) = x^9$
$x^{27} \mod (x^{30} + x + 2) = x^{27}$
$x^{81} \mod (x^{30} + x + 2) = x^{23} + x^{22} + x^{21}$
$x^{243} \mod (x^{30} + x + 2) = x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3$
$x^{729} \mod (x^{30} + x + 2) = x^{27} + x^{24} + x^{21} + x^{18} + x^{15} + x^{12} + x^9 + 2x^4 + x^3 + 2x + 1$

Далее, согласно выше описанному условию, посчитаем НОД многочленов, производя проверку с помощью WolframAlpha :

1) $(x^{30}+x+2, x^3+2x)=1$

2) $(x^{30}+x+2, x^9+2x)=1$

3) $(x^{30}+x+2, x^{27}+2x)=1$

4) $(x^{30}+x+2, x^{23}+x^{22}+x^{21}+2x)=1$

5) $(x^{30}+x+2, x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+2x)=1$

6) $(x^{30}+x+2, x^{27}+x^{24}+x^{21}+x^{18}+x^{15}+x^{12}+x^9+2x^4+x^3+x+1)=1$

Таким образом, многочлен $f(x)=x^{30}+x+2$ - является неприводимым в $\mathbb{Z}_3$.

2.5. Задача №5

Вариант №12

Задание:

$\sigma : P \to F$ - изоморфизм колец, введем $\sigma` : P[x] \to F[x]$. Доказать, что $\sigma`$ изоморфизм колец.

Решение:

Пусть $f(x) = f_0 + \ldots + f_m x^m$ и $g(x) = g_0 + \ldots + g_l x^l$ - произвольные многочлены из P[x]. Ввиду того, что мы работаем в кольцах, $\sigma`(f(x)+g(x)) = \sigma`(f(x))+\sigma`(g(x))$, т. е. $\sigma`$ - гомоморфизм относительно операции сложения. А также, эпиморфизм относительно умножения $\sigma`(f(x)g(x)) = \sigma`(f(x))\sigma`(g(x))$.
$\sigma`(f(x))\sigma`(g(x)) = (\sigma(f_0)+\ldots+\sigma(f_m)x^m)(\sigma(g_0)+\ldots+\sigma(g_m)x^l) =$
$= \prod\limits_{i=0}^{i=m}(\sigma(f_i)x^i \cdot \sum\limits_{j=0}^{j=l}\sigma(g_j)x^j) = \sigma(f_0)\sigma(g_0)+\ldots+\sigma(f_0)\sigma(g_l)x^l+\sigma(f_1)x\sigma(g_0)+$
$\ldots+\sigma(f_1)x\sigma(g_l)x^l+\ldots\ldots+\sigma(f_m)x^m\cdot\sigma(g_0)+\ldots+\sigma(f_m)x^m\cdot\sigma(g_l)x^l =$
$= \sigma(f_0g_0)+\ldots+\sigma(f_0g_l)x^l+\sigma(f_1g_0)x+\ldots+\sigma(f_1g_l)x^{l+1}+\ldots\ldots+\sigma(f_mg_0)x^m+$
$\ldots+\sigma(f_mg_l)x^{l+m} = \sigma`(f(x)g(x))$.
Следовательно, $\sigma`$ - изоморфизм колец.

3. ЛРП

3.1. Задача №1

Вариант №15

Задание:

1) Определите над каким полем последовательность u. Является ли последовательность u ЛРП?
    - Если да, то каков её характеристический многочлен минимальной степени, общий u(i), а также Ann(u).
2) Если ЛРП, то является ли периодической?
    - Если да, то вычислите период и длину подхода ЛРП.

Дано:

$u = 1, 2, 1, 1, 1, 2, 0, 2, 1, 2, 2, 1, 2, 0, 1, 1, 0, 2, 0, 0, 0, 0, 1, 2, 0, 0, 1, 1, 2, 2, 1, 0, 2, 1, 1, 1,$
$0, 2, 2, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 2, 2, 2, 2, 0, 0, 2, 2, 0, 2, 2, 0, 0, 1, 0, 0, 2, 1, 2, 1, 2, 2, 0,$
$0, 0, 1, 0, 2, 0, 1, 2, 0, 1, 0, 1, 2, 0, 2, 2, 1, 2, 1, 0, 1, 0, 0, 1, 2, 2, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 0, 2,$
$1, 2, 2, 1, 2, 0, 1, 1, 0, 2, 0, 0, 0, 0, 1, 2, 0, 0, 1, 1, 2, 2, 1, 0, 2, 1, 1, 1, 0, 2, 2, 1, 0, 0, 0, 1, 1, 1,$
$0, 1, 0, 1, 0, 2, 2, 2, 2, 0, 0, 2, 2, 0, 2, 2, 0, 0, 1, 0, 0, 2, 1, 2, 1, 2, 2, 0, 0, 0, 1, 0, 2, 0, 1, 2, 0, 1,$
$0, 1, 2, 0, 2, 2, 1, 2, 1, 0, 1, 0, 0, 1, 2, 2, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 0, 2, 1, 2, 2, 1, 2, 0, 1, 1, 0, 2,$
$0, 0, 0, 0, 1, 2, 0, 0, 1, 1, 2, 2, 1, 0, 2, 1, 1, 1, 0, 2, 2, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 2, 2, 2, 2, 0,$
$0, 2, 2, 0, 2, 2, 0, 0, 1, 0, 0, 2, 1, 2, 1, 2, 2, 0, 0, 0, 1, 0, 2, 0, 1, 2, 0, 1, 0, 1, 2, 0, 2, 2, 1, 2, 1, 0,$
$1, 0, 0, 1, 2, 2, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 0, 2, 1, 2, 2, 1, 2, 0, 1, 1, 0, 2, 0, 0, 0, 0, 1, 2, 0, 0, 1, 1,$
$2, 2, 1, 0, 2, 1, 1, 1, 0, 2, 2, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 2, 2, 2, 2, 0, 0, 2, 2, 0, 2, 2, 0, 0, 1, 0,$
$0, 2, 1, 2, 1, 2, 2, 0, 0, 0, 1, 0, 2, 0, 1, 2, 0, 1, 0, 1, 2, 0 \ldots$

Решение:

Степень характеристического многочлена 5. Потому что для 4 и меньше, совпадения не будут совпадать с началом нового цикла.

Т.к. значения последовательностей не превышает 2, то $P = \mathbb{Z}_3$.

Нужно решить систему из 4 уравнений:

$$\begin{cases} 1\cdot f_{n-1}+1\cdot f_{n-2}+1\cdot f_{n-3}+2\cdot f_{n-4}+1\cdot f_{n-5}=2\\ 2\cdot f_{n-1}+1\cdot f_{n-2}+1\cdot f_{n-3}+1\cdot f_{n-4}+2\cdot f_{n-5}=0\\ 2\cdot f_{n-2}+1\cdot f_{n-3}+1\cdot f_{n-4}+1\cdot f_{n-5}=2\\ 2\cdot f_{n-1}+2\cdot f_{n-3}+1\cdot f_{n-4}+1\cdot f_{n-5}=1\\ 1\cdot f_{n-1}+2\cdot f_{n-2}+2\cdot f_{n-4}+1\cdot f_{n-5}=2 \end{cases} \Rightarrow \left(\begin{array}{ccccc|c} 1&1&1&2&1&2\\ 2&1&1&1&2&0\\ 0&2&1&1&1&2\\ 2&0&2&1&1&1\\ 1&2&0&2&1&2 \end{array}\right) \Rightarrow$$

$$\Rightarrow \left(\begin{array}{ccccc|c} 1&1&1&2&1&2\\ 0&2&2&0&0&2\\ 0&2&1&1&1&2\\ 0&1&0&0&2&0\\ 0&1&2&0&0&0 \end{array}\right) \Rightarrow \left(\begin{array}{ccccc|c} 1&1&1&2&1&2\\ 0&2&2&0&0&2\\ 0&0&2&1&1&0\\ 0&0&2&0&2&2\\ 0&0&1&0&0&2 \end{array}\right) \Rightarrow \left(\begin{array}{ccccc|c} 1&1&1&2&1&2\\ 0&2&2&0&0&2\\ 0&0&2&1&1&0\\ 0&0&0&2&1&2\\ 0&0&0&1&1&2 \end{array}\right) \Rightarrow$$

$$\Rightarrow \left(\begin{array}{ccccc|c} 1&1&1&2&1&2\\ 0&2&2&0&0&2\\ 0&0&2&1&1&0\\ 0&0&0&2&1&2\\ 0&0&0&0&2&1 \end{array}\right) \Rightarrow \begin{cases} 1\cdot f_{n-1}+1\cdot f_{n-2}+1\cdot f_{n-3}+2\cdot f_{n-4}+1\cdot f_{n-5}=2\\ 2\cdot f_{n-2}+2\cdot f_{n-3}=2\\ 2\cdot f_{n-3}+1\cdot f_{n-4}+1\cdot f_{n-5}=0\\ 2\cdot f_{n-4}+1\cdot f_{n-5}=2\\ 2\cdot f_{n-5}=1 \end{cases} \Rightarrow$$

$\Rightarrow f_{n-1}=2; \quad f_{n-2}=2; \quad f_{n-3}=2; \quad f_{n-4}=0; \quad f_{n-5}=2.$

$F(x)=x^5-2x^4-2x^3-2x^2-2=x^5+x^4+x^3+x^2+1$

$u(i)=2\cdot u(i-1)+2\cdot u(i-2)+2\cdot u(i-3)+0\cdot u(i-4)+2\cdot u(i-5)$

Согласно теореме №7 §3 главы 25: $Ann(u)=P[x]G(x)$.

Воспользовавшись данной формулой получим:

$Ann(u)=F[x]P=(x^5+x^4+x^3+x^2+1)\mathbb{Z}_3$.

u является периодической ЛРП т.к. $\lambda=0, \quad \forall i\geq\lambda: \quad u(i+312)=u(i)$ длина подхода равна 0 и период равен 312.

3.2. Задача №2

Вариант №2

Задание:

(Найти определенный член последовательности)

f(x) – характеристический многочлен ЛРП u. deg f(x) = n

Найдите:

1) u(i), u(i+1), u(i+2),. . . , u(i+n);

2) u(j), u(j+1), u(j+2),. . . , u(j+n).

Дано:

$P = \mathbb{Z}_5$

$f[x] := 1 + 3x + 2x^3 + 2x^4 + 3x^6 + x^7$

$u[\overline{1,7}] = (0, 4, 3, 4, 2, 0, 4)$

i=1742, j=989

Решение:

$f(1) = 2, \quad f(2) = 0, \quad f(3) = 0, \quad f(4) = 0, \quad f(5) = 4$

$f'(2) = 0, \quad f'(3) = 0, \quad f'(4) = 0$

$f''(2) = 4, \quad f''(3) = (3), \quad f''(4) = 0$

$f^{(3)}(4) = 4$

Таким образом многочлен раскладывается $f(x) = (x + 3)^2(x + 2)^2(x + 1)^3$

$k_1 = 1, \quad k_2 = 1, \quad k_3 = 2$

$a_1 = 2, \quad a_2 = 3, \quad a_3 = 4$

$u(i) = a_{10}a_1^{<0>} + a_{11}a_1^{<1>} + a_{20}a_2^{<0>} + a_{21}a_2^{<1>} + a_{30}a_3^{<0>} + a_{31}a_3^{<1>} + a_{32}a_3^{<2>}$

$u(i) = a_{10}2^i + a_{11}2^i\binom{i}{1} + a_{20}3^i + a_{21}3^i\binom{i}{1} + a_{30}4^i + a_{31}4^i\binom{i}{1} + a_{32}4^i\binom{i}{2}$

$a_1^{<0>} = (2^0 2^0, 2^0\binom{1}{0}2^1, 2^0\binom{2}{0}2^2, 2^0\binom{3}{0}2^3, 2^0\binom{4}{0}2^4, 2^0\binom{5}{0}2^5, 2^0\binom{6}{0}2^6) = (1, 2, 4, 3, 1, 2, 4, \ldots)$

$a_1^{<1>} = (2^1 0, 2^1 2^0, 2^1\binom{2}{1}2^1, 2^1\binom{3}{1}2^2, 2^1\binom{4}{1}2^3, 2^1\binom{5}{1}2^4, 2^1\binom{6}{1}2^5) = (0, 2, 3, 4, 4, 0, 4, \ldots)$

$a_2^{<0>} = (3^0 3^0, 3^0\binom{1}{0}3^1, 3^0\binom{2}{0}3^2, 3^0\binom{3}{0}3^3, 3^0\binom{4}{0}3^4, 3^0\binom{5}{0}3^5, 3^0\binom{6}{0}3^6) = (1, 3, 4, 2, 1, 3, 4, \ldots)$

$a_2^{<1>} = (3^1 0, 3^1 3^0, 3^1\binom{2}{1}3^1, 3^1\binom{3}{1}3^2, 3^1\binom{4}{1}3^3, 3^1\binom{5}{1}3^4, 3^1\binom{6}{1}3^5) = (0, 3, 3, 1, 4, 0, 4, \ldots)$

$a_3^{<0>} = (4^0 4^0, 4^0\binom{1}{0}4^1, 4^0\binom{2}{0}4^2, 4^0\binom{3}{0}4^3, 4^0\binom{4}{0}4^4, 4^0\binom{5}{0}4^5, 4^0\binom{6}{0}4^6) = (1, 4, 1, 4, 1, 4, 1, \ldots)$

$a_3^{<1>} = (4^1 0, 4^1 4^0, 4^1\binom{2}{1}4^1, 4^1\binom{3}{1}4^2, 4^1\binom{4}{1}4^3, 4^1\binom{5}{1}4^4, 4^1\binom{6}{1}4^5) = (0, 4, 2, 2, 4, 0, 1, \ldots)$

$a_3^{<2>} = (4^2 0, 4^2 0, 4^2 4^0, 4^2\binom{3}{2}4^1, 4^2\binom{4}{2}4^2, 4^2\binom{5}{2}4^3, 4^2\binom{6}{2}4^4) = (0, 0, 1, 2, 1, 0, 0, \ldots)$

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 2 & 2 & 3 & 3 & 4 & 4 & 0 \\ 4 & 3 & 4 & 3 & 1 & 2 & 1 \\ 3 & 4 & 2 & 1 & 4 & 2 & 2 \\ 1 & 4 & 1 & 4 & 1 & 4 & 1 \\ 2 & 0 & 3 & 0 & 4 & 0 & 0 \\ 4 & 4 & 4 & 4 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{10} \\ a_{11} \\ a_{20} \\ a_{21} \\ a_{30} \\ a_{31} \\ a_{32} \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 3 \\ 4 \\ 2 \\ 0 \\ 4 \end{pmatrix} \Rightarrow$$

$$\left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 2 & 2 & 3 & 3 & 4 & 4 & 0 & 4 \\ 4 & 3 & 4 & 3 & 1 & 2 & 1 & 3 \\ 3 & 4 & 2 & 1 & 4 & 2 & 2 & 4 \\ 1 & 4 & 1 & 4 & 1 & 4 & 1 & 2 \\ 2 & 0 & 3 & 0 & 4 & 0 & 0 & 0 \\ 4 & 4 & 4 & 4 & 1 & 1 & 0 & 4 \end{array}\right) \sim \left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 2 & 4 & 0 & 4 \\ 0 & 3 & 0 & 3 & 2 & 2 & 1 & 3 \\ 0 & 4 & 4 & 1 & 1 & 2 & 2 & 4 \\ 0 & 4 & 0 & 4 & 0 & 4 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 & 2 & 1 & 0 & 4 \end{array}\right) \sim \left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 2 & 4 & 0 & 4 \\ 0 & 0 & 1 & 1 & 4 & 1 & 1 & 2 \\ 0 & 0 & 4 & 2 & 1 & 3 & 1 & 2 \\ 0 & 0 & 4 & 3 & 1 & 1 & 1 & 4 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 4 & 2 \end{array}\right)$$

$$\left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 2 & 4 & 0 & 4 \\ 0 & 0 & 1 & 1 & 4 & 1 & 1 & 2 \\ 0 & 0 & 0 & 3 & 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 4 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 4 & 3 & 4 & 4 & 3 \\ 0 & 0 & 0 & 0 & 2 & 2 & 4 & 2 \end{array}\right) \sim \left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 2 & 4 & 0 & 4 \\ 0 & 0 & 1 & 1 & 4 & 1 & 1 & 2 \\ 0 & 0 & 0 & 3 & 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 & 4 & 2 \end{array}\right) \sim \left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 2 & 4 & 0 & 4 \\ 0 & 0 & 1 & 1 & 4 & 1 & 1 & 2 \\ 0 & 0 & 0 & 3 & 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 4 & 2 & 3 \end{array}\right)$$

$$\left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 2 & 4 & 0 & 4 \\ 0 & 0 & 1 & 1 & 4 & 1 & 1 & 2 \\ 0 & 0 & 0 & 3 & 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 4 & 2 & 3 \end{array}\right) \sim \begin{cases} a_{10} + a_{20} + a_{30} = 0 \\ 2a_{11} + a_{20} + 3a_{21} + 2a_{30} + 4a_{31} = 4 \\ a_{20} + a_{21} + 4a_{30} + a_{31} + a_{32} = 2 \\ 3a_{21} + 4a_{31} + 2a_{32} = 4 \\ a_{32} = 4 \\ 3a_{30} + 2a_{31} + 3a_{32} = 1 \\ 4a_{31} + 2a_{32} = 3 \end{cases} \sim \begin{cases} a_{10} = 3 \\ a_{11} = 4 \\ a_{20} = 4 \\ a_{21} = 2 \\ a_{32} = 4 \\ a_{30} = 3 \\ a_{31} = 0 \end{cases}$$

$u(i) = 3 \cdot 2^i + 4 \cdot 2^i \binom{i}{1} + 4 \cdot 3^i + 2 \cdot 3^i \binom{i}{1} + 3 \cdot 4^i + 4 \cdot 4^i \binom{i}{2} =$
$= 2^i(3 + 4i) + 3^i(4 + 2i) + 4^i(3 + 2i(i - 1)).$
i = 1742; j = 989;
u(i) = 3; u(i+1) = 0; u(i+2) = 3; u(i+3) = 0; u(i+4) = 0; u(i+5) = 2;
u(i+6) = 0; u(i+7) = 2.
u(j) = 2; u(j+1) = 1; u(j+2) = 0; u(j+3) = 1; u(j+4) = 0; u(j+5) = 1;
u(j+6) = 4; u(j+7) = 1.

3.3. Задача №3

Вариант №30

Задание:
(Найти период многочлена f(x) над кольцом)
R - кольца, f(x) - многочлен над R, deg f(x)=n

1) Постройте импульсную последовательность с характеристическим многочленом f(x) до первого «повтора».

2) Выпишите длину подхода и периода импульсной последовательности

3) Найдите период многочлена f(x) и дефект подхода

4) Является ли f(x) многочленом максимального периода?

5) Является ли f(x) реверсивным многочленом?

6) Выпишете последовательности u, с характеристическим многочленом f(x) до первого «повтора»

7) Выпишите длину подхода и периода последовательности u

Дано:
$R = \mathbb{Z}_9$
$f[x] := 3 + 8x + x^2$
$u[\overline{1, 2}] = (1, 6)$
Решение:

1) $f(x) = x^2 - f_1 x - f_0 = x^2 + 8x + 3 \quad \Rightarrow \quad f_1 = 1, f_0 = 6$
   $u_i = f_1 u(i-1) + f_0 u(i-2) = u(i-1) + 6u(i-2)$
   $e^f[\overline{1,2}] = (0,1)$
   $e^f = (0,1,1,7,4,1,7,\ldots)$

2) $\lambda(e^f) = 2, \quad T(e^f) = 3$

3) e^f является периодичной, и т.к. f(x) унитарный, то f(x) является периодическим. Причём $\lambda(f) = \lambda(e^f) = 2, T(f) = T(e^f) = 3$

4) $\mathbb{Z}_9 \sim \mathbb{Z}_{3^2}$
   $(3^2-1)\cdot 3 = 24 \neq T(f) \quad \Rightarrow \quad f(x)$ не максимального периода.

5) Т.к. $\lambda(f) \neq 0$, то f(x) - не является реверсивным многочленом.

6) $u(i) = (1,6,3,3,3,3,\ldots)$

7) $\lambda(u) = 2, \quad T(u) = 1$

3.4. Задача №4

Вариант №17

Задание:

(Найти циклы Lp(f))

P – поле, f(x) – характеристический многочлен.

1) На какие циклы разбивается множество Lp(f)

2) Чему равно $N_f^{(t)}$, $C_f^{(t)}$ для всех t?

3) Выпишет цикловой тип многочлена $C_f(y)$

Дано:

$P = \mathbb{Z}_5$

$f[x] := 3 + 4x + x^2 + x^3$

Решение:

Если $P = \mathbb{Z}_5$ и $f[x] := 3+4x+x^2+x^3 \Rightarrow L_p(f)$ состоит из последовательностей вида:

$u_i = 4u(i-1) + u(i-2) + 2u(i-3)$

$u_1 = (0)$ с циклом длины 1.

$u_2 = (0, 0, 1, 4, 2, 4, 1, 2, 2, 2, 4, 2, 1, 4, 1, 0, 4, 3, 1, 0, 2, 0, 2, 2, 0, 1, 3, 3, 2, 2, 1, 0, 0, 2, 3, 4, 3, 2, 4, 4, 4, 3, 4, 2, 3, 2, 0, 3, 1, 2, 0, 4, 0, 4, 4, 0, 2, 1, 1, 4, 4, 2, 0, 0, 4, 1, 3, 1, 4, 3, 3, 3, 1, 3, 4, 1, 4, 0, 1, 2, 4, 0, 3, 0, 3, 3, 0, 4, 2, 2, 3, 3, 4, 0, 0, 3, 2, 1, 2, 3, 1, 1, 1, 2, 1, 3, 2, 3, 0, 2, 4, 3, 0, 1, 0, 1, 1, 0, 3, 4, 4, 1, 1, 3, 0, 0, 1, \ldots)$ с циклом длинны 124.

$C_f^{(1)} = 1, \quad C_f^{(124)} = 1$

$N_f^{(1)} = 1 \cdot C_f^{(1)} = 1, \quad N_f^{(124)} = 124 \cdot C_f^{(124)} = 124$

Цикловой тип $C_f(y) = C_f^{(1)} y^1 + C_f^{(124)} y^{124} = y^{124} + y^1$

3.5. Задача №5

Вариант №16

Задание:

u ЛРП над полем. Доказать, что $\forall H(x) \in P[x] \Rightarrow m_{H(x)u}(x) = \dfrac{m_u(x)}{(m_u(x), H(x))}$.

Решение:

По теореме №11 §3 главы 25.

Теорема. *Пусть u — ЛРП над полем P с характеристическим многочленом F(x) и генератором Φ(x). Тогда*

1) $M_u(x) = \dfrac{F(x)}{(F(x), (x))}$;

2) если v = H(x)u для некоторого $H(x) \in P[x]$, *то* $M_v(x) = \dfrac{M_u(x)}{(H(x), M_u(x))}$

Рассматривая п.2, заметим, что согласно теореме №6 §2 главы №25

Теорема. *Пусть* $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in R[x], m > 0$. *Тогда для любой ЛРП* $u \in L_R(F)$ *существует единственный многочлен* $\Phi(x) \in R[x]$ *такой, что* $u = \Phi(x) \cdot e^F, deg\,\Phi(x) < m$, *и этот многочлен имеет вид:*

$(x) = u(0)x^{m-1} + \sum\limits_{k=1}^{m-1} (u(k) - f_m u(k-1) - \ldots - f_{m-k} u(0)) x^{m-1-k}$

$\forall A(x) \in P[x]$ справедливы следующие соотношения:

$$A(x)H(x)u = (0) \Leftrightarrow Mu(x)|A(x)H(x) \Leftrightarrow \frac{m_u(x)}{(m_u(x), H(x))} \;\Big|\; A(x).$$