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: «Кольца. Поля. Конечные поля. ЛРП.»

Студент группы ККСО-03-19	Николенко В.О.	_____ *(подпись)*
Руководитель курсовой работы	Кожухов П. В.	_____ *(подпись)*
Консультант	Ассистент Тыщенко Н.С.	_____ *(подпись)*

Работа представлена к защите	«__» _________ 2021 г.
Допущен к защите	«__» _________ 2021 г.
Оценка	«_____»

Москва – 2021

СОДЕРЖАНИЕ

1. Общая теория колец 3
   1.1. Задача №1 3
   1.2. Задача №2 5
   1.3. Задача №3 8
   1.4. Задача №4 9
   1.5. Задача №5 10
2. Общая теория полей/Конечные поля 11
   2.1. Задача №1 вариант 19 11
   2.2. Задача №2 вариант 18 12
   2.3. Задача №3 вариант 11 12
   2.4. Задача №4 вариант 25 16
   2.5. Задача №5 вариант 27 19
3. ЛРП 21
   3.1. Задача №1 вариант 13 21
   3.2. Задача №2 вариант 14 23
   3.3. Задача №3 вариант 24 28
   3.4. Задача №4 вариант 30 29

1. ОБЩАЯ ТЕОРИЯ КОЛЕЦ

1.1. Задача №1

Дано:
1) Найдите компоненты элементов $a_1 = 371, b_1 = 122, c_1 = 158$ кольца $\mathbb{R} = \mathbb{Z}_{438}$
2) Постройте изоморфизм колец φ кольца $\mathbb{Z}_{741}$
3) Найдите $\varphi(a_2), \varphi(b_2), \varphi(c_2), a_2 = 642, b_2 = 510, c_2 = 519$
4) Найдите $\varphi(2, 11, 17)$

Решение:
1) Т.к. $428 = 2{\cdot}3{\cdot}73$, кольцо можно разложить в прямую сумму идеалов, и их порядки равны делителям порядка исходного кольца:
$\mathbb{Z}_{438} = \mathbb{I}_1 \dot{+} \mathbb{I}_2 \dot{+} \mathbb{I}_3$
$\mathbb{I}_s = \{r \in \mathbb{Z}_{438} \big| p_s^{k_s} \cdot r = 0\}$
$\mathbb{I}_1 = \{0, 219\}$
$\mathbb{I}_2 = \{0, 146, 292\}$
$\mathbb{I}_3 = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192, 198, 204, 210, 216, 222, 228, 234, 240, 246, 252, 258, 264, 270, 276, 282, 288, 294, 300, 306, 312, 318, 324, 330, 336, 342, 348, 354, 360, 366, 372, 378, 384, 390, 396, 402, 408, 414, 420, 426, 432\}$
Тогда мы можем выразить $\forall$ элемент разложимого кольца:
$r = i_1 + i_2 + \cdots + i_k$, где $i_s \in \mathbb{I}_s, s \in \overline{1, k}$.
Найдём компоненты элемента r:
$i_s = r \cdot e_s$,где $i_s, e_s \in \mathbb{I}_s, s \in \overline{1, k}$.
Найдём элементы e_s.
$\sqsupset$ у нас есть два ненулевых элемента e_s, r_s идеала $\mathbb{I}_s$. Тогда выполняется:
$e_s \cdot e_s = e_s$
e_1 идеала $\mathbb{I}_1$:
$219 \cdot 219 \big(mod 438\big) = 219 = e_1$
e_2 идеала $\mathbb{I}_2$:
$292 \cdot 292 \big(mod 438\big) = 292 = e_2$
e_3 идеала $\mathbb{I}_3$:
$366 \cdot 366 \big(mod 438\big) = 366 = e_3$

Найдём компоненты элемента a_1:
$i_1 = 219 \cdot 371 \big(mod 438\big) = 219;$
$i_2 = 292 \cdot 371 \big(mod 438\big) = 146;$
$i_3 = 266 \cdot 371 \big(mod 438\big) = 6;$
Тогда разложение элемента a_1 имеет вид:
$371 = 219 + 146 + 6$

Найдём компоненты элемента b_1:
$i_1 = 219 \cdot 122 \big(mod 438\big) = 0;$
$i_2 = 292 \cdot 122 \big(mod 438\big) = 146;$
$i_3 = 266 \cdot 122 \big(mod 438\big) = 414;$
Тогда разложение элемента b_1 имеет вид:
$122 = 0 + 146 + 414$

Найдём компоненты элемента c_1:
$i_1 = 219 \cdot 158 \big(mod 438\big) = 0;$
$i_2 = 292 \cdot 158 \big(mod 438\big) = 146;$
$i_3 = 266 \cdot 158 \big(mod 438\big) = 12;$
Тогда разложение элемента c_1 имеет вид:
$158 = 0 + 146 + 12$

$2\big)$ Изоморфизм колец φ кольца $\mathbb{Z}_{741}$:
$\varphi : \mathbb{Z}_{741} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{13} \oplus \mathbb{Z}_{19}$

$3\big)$ Образ изоморфизма φ - элемент, содержащий компоненты остатков от деления на порядки подколец, тогда:
$642 \big(mod 3\big) = 0;\ 642 \big(mod 13\big) = 5;\ 642 \big(mod 19\big) = 15;$
$\Rightarrow \varphi\big(642\big) = \big([0]_3, [5]_{13}, [15]_{19}\big)$
$510 \big(mod 3\big) = 0;\ 510 \big(mod 13\big) = 3;\ 510 \big(mod 19\big) = 16;$
$\Rightarrow \varphi\big(510\big) = \big([0]_3, [3]_{13}, [16]_{19}\big)$
$519 \big(mod 3\big) = 0;\ 519 \big(mod 13\big) = 12;\ 519 \big(mod 19\big) = 6;$
$\Rightarrow \varphi\big(519\big) = \big([0]_3, [12]_{13}, [6]_{19}\big)$

4) A система сравнений - прообраз изоморфизма φ:

$$\begin{cases} x \equiv 2(mod 3) \\ x \equiv 11(mod 13) \\ x \equiv 17(mod 19) \end{cases}$$

$x = 3t_1 + 2, t_1 \in \mathbb{Z}$
$3t_1 + 2 \equiv 11(mod 13) \Leftrightarrow 3t_1 \equiv 9(mod 13)$
$t_1 = 13t_2 + 3, t_2 \in \mathbb{Z}$. Тогда подставим его в 3-е сравнение:
$39t_2 + 11 = 17(mod 19) \Leftrightarrow 39t_2 \equiv 6(mod 9)$
$t_2 = 19t_3 + 6, t_3 \in \mathbb{Z}$. И подставим значение t_2 в решение 1-ого сравнения:
$x = 39 \cdot (19t_3 + 6) + 11 = 741t_3 + 245, t_3 \in \mathbb{Z}$
$x \equiv 245(mod 741) \Rightarrow \varphi^{-1}(1, 11, 17) = [245]_{741}$

1.2. Задача №2

Дано:

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 нуляи обратимые элементы (с обратными элементами). Где $P = GF(3) = \{0, e, \alpha\}, f_1(x) = x^2 + x + \alpha, f_2(x) = x^2 + \alpha$

Решение:

Рассмотрим первое факторкольцо $P[x]/f_1(x)$. Т.к. многочлен $f_1(x) = x^2 + x + \alpha$ неприводим над $GF(3)$, то указаннное факторкольцо - поле из 9 элменетов вида $ax + b$.

Тогда построим таблицу Кэли по умножению, в силу того, что множество ограниченое(см. Таблица 1).

Судя по таблице Кэли делителей нуля нет и обратный $\exists$ для $\forall \backslash \{0\}$, где обратный для e это e, для α это α, для ex это $ex + e$, для αx это $\alpha x + \alpha$, для $ex + e$ это ex, для $ex + \alpha$ это $\alpha x + e$, для $\alpha x + e$ это $ex + \alpha$, для $\alpha x + \alpha$ это αx.

Далее рассмотрим второе факторкольцо $P[x]/f_2(x)$. Т.к. многочлен $f_2(x) = x^2 + \alpha$ приводим над множеством $GF(3)$, то это не поле. Построим для него таблицу Кэли по сложению(см. Таблица 3).

Делители нуля:

$ex + e; ex + \alpha; \alpha x + e; \alpha x + \alpha$

Обратные $\exists$ для $\forall \backslash \{0, ex + e; ex + \alpha; \alpha x + e; \alpha x + \alpha\}$, где обратный для e это e, для α это α, для ex это ex, для αx это αx.

Таблица 1. Таблица Кэли по умножению для R_1

$\cdot$	0	e	α	ex	αx	$ex+e$	$ex+\alpha$	$\alpha x+e$	$\alpha x+\alpha$
0	0	0	0	0	0	0	0	0	0
e	0	e	α	ex	αx	$ex+e$	$ex+\alpha$	$\alpha x+e$	$\alpha x+\alpha$
α	0	α	e	αx	ex	$\alpha x+\alpha$	$\alpha x+e$	$ex+\alpha$	$ex+e$
ex	0	ex	αx	$\alpha x+e$	$ex+\alpha$	e	$ex+e$	$\alpha x+\alpha$	α
αx	0	αx	ex	$ex+\alpha$	$\alpha x+e$	α	$\alpha x+\alpha$	$ex+e$	e
$ex+e$	0	$ex+e$	$\alpha x+\alpha$	e	α	$ex+\alpha$	αx	ex	$\alpha x+e$
$ex+\alpha$	0	$ex+\alpha$	$\alpha x+e$	$ex+e$	$\alpha x+\alpha$	αx	α	e	ex
$\alpha x+e$	0	$\alpha x+e$	$ex\alpha$	$\alpha x+\alpha$	$ex+e$	ex	e	α	αx
$\alpha x+\alpha$	0	$\alpha x+\alpha$	$ex+e$	α	e	$\alpha x+e$	ex	αx	$ex+\alpha$

Таблица 3. Таблица Кэли по умножению для R_2

$\cdot$	0	e	α	ex	αx	$ex+e$	$ex+\alpha$	$\alpha x+e$	$\alpha x+\alpha$
0	0	0	0	0	0	0	0	0	0
e	0	e	α	ex	αx	$ex+e$	$ex+\alpha$	$\alpha x+e$	$\alpha x+\alpha$
α	0	α	e	αx	ex	$\alpha x+\alpha$	$\alpha x+e$	$ex+\alpha$	$ex+e$
ex	0	ex	αx	e	α	$ex+e$	$\alpha x+e$	$ex+\alpha$	$\alpha x+\alpha$
αx	0	αx	ex	α	e	$\alpha x+\alpha$	$ex+\alpha$	$\alpha x+e$	$ex+e$
$ex+e$	0	$ex+e$	$\alpha x+\alpha$	$ex+e$	$\alpha x+\alpha$	$\alpha x+\alpha$	0	0	$ex+e$
$ex+\alpha$	0	$ex+\alpha$	$\alpha x+e$	$\alpha x+e$	$ex+\alpha$	0	$ex+\alpha$	$\alpha x+e$	0
$\alpha x+e$	0	$\alpha x+e$	$ex+\alpha$	$ex+\alpha$	$\alpha x+e$	0	$\alpha x+e$	$ex+\alpha$	0
$\alpha x+\alpha$	0	$\alpha x+\alpha$	$ex+e$	$\alpha x+\alpha$	$ex+e$	$ex+e$	0	0	$\alpha x+\alpha$

1.3. Задача №3

Дано:

Являются ли $\mathbb{R}_1, \mathbb{R}_2$ полями или кольцами? Если да, то в $\mathbb{R}_1, \mathbb{R}_2$ найти (не менее 3, если возможно) собственные идеалы и (не менее 3, если возможно) собственные подкольца, не являющиеся идеалами. Являются ли данные подкольца кольцами главных идеалов?

Множества: $\mathbb{R}_1 = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}, \mathbb{R}_2 = 8\mathbb{Z} + 12\mathbb{Z}$.

Решение:

На множестве $\mathbb{R}_1$ посмотрим замкнутость по сложению и по умножению:

$(a + b \cdot \sqrt{5}) + (c + d \cdot \sqrt{5}) = (a + c) + (b + d) \cdot \sqrt{5} \Rightarrow$ выполняется.

$(a + b \cdot \sqrt{5}) \cdot (c + d \cdot \sqrt{5}) = (ac + 5bd) + (ad + bc) \cdot \sqrt{5} \Rightarrow$ выполняется.

Рассмотрим свойства кольца $\mathbb{Z}$:

1$\big)$$(\mathbb{Z}; +)$ — абелева группа,

2$\big)$$(\mathbb{Z}; \cdot)$ — полугруппа,

3$\big)$ операция умножения дистрибутивна относительно сложения.

При этом группа $(\mathbb{Z}; +)$ называется аддитивнойгруппойкольца $\mathbb{Z}$, а ее нейтральный элемент 0 — нулем кольца $\mathbb{R}$. Кольцо $(\mathbb{R}; +)$ называется коммутативным.

У кольца есть нейтральный по сложению - 0, и есть нейтральный по умножению - 1.

Плюс ко всему выше упомянотому покажем, что существуют обратные элементы по сложению:

$(a + b \cdot \sqrt{5}) + (c + d \cdot \sqrt{5}) = 0, c = -a, d = -b \Rightarrow \exists$

А также по умножению:

$(a + b \cdot \sqrt{5}) \cdot (c + d \cdot \sqrt{5}) = 1, c = \frac{a}{a^2 - 5 \cdot b^2}, d = \frac{-b \cdot \sqrt{5}}{a^2 - 5 \cdot b^2}$

Получаем, что у нас не должно выполняться равенство между a^2 и $5 \cdot b^2 \Rightarrow$ обратный по умножению $\exists$ не для всех элементов кольца. Тогда по умножению это полугруппа, а по сложению это абелева группа.

Покажем, что кольцо дистрибутивно:

$(a + b \cdot \sqrt{5}) \cdot \big((c + d \cdot \sqrt{5}) + (e + f \cdot \sqrt{5})\big) = (a + b \cdot \sqrt{5}) \cdot (c + d \cdot \sqrt{5}) + (a + b \cdot \sqrt{5}) \cdot (e + f \cdot \sqrt{5}) \Leftrightarrow$

$\Leftrightarrow \big(a \cdot (b + e) + 5b \cdot (d + f)\big) + \big(b \cdot (c + e) + a \cdot (d + f)\big) \cdot \sqrt{5} = \big(a \cdot (b + e) + 5b \cdot (d + f)\big) + \big(b \cdot (c + e) + a \cdot (d + f)\big) \cdot \sqrt{5} \Rightarrow \square$

Выше была доказана дистрибутивность умножения отн-о сложения. Следовательно перед нами коммутативное кольцо с e в силу своей абелевости и единицы.

Далее рассмотрим мн-во $\mathbb{R}_2$:

$8\mathbb{Z} + 12\mathbb{Z} = 8z_1 + 12z_2$

Так как мы вправе сделать следующую замену: $2z_1 + 3z_2 = \mathbb{Z}$, то получим: $8\mathbb{Z} + 12\mathbb{Z} = 8z_1 + 12z_2 = 4(2z_1 + 3z_2) = 4\mathbb{Z}$. Мы знаем что $4\mathbb{Z}$ является коммутативным кольцом относительно двух бинарных операций: сложения и умножения. Все подкольца кольца $4\mathbb{Z}$ являются его идеалами, но $\exists$ бесконечное множество собственных идеалов $(8\mathbb{Z}, 12\mathbb{Z}, 16\mathbb{Z}, 20\mathbb{Z} \dots)$.

Во мн-ве $\mathbb{R}_1 \exists$ одно единственное подкольцо $\mathbb{Z}$, которое не является его идеалом $\Rightarrow$ мн-во $\mathbb{R}_1$ не кольцо собственных идеалов.

Как гласит определение, "Идеал I кольца R называют главным, если существует такой элемент $s \in \mathbb{R}$, что $\mathbb{I} = (s)_{\mathbb{R}}$ (говорят, что элемент s порождает идеал I). Коммутативное кольцо $\mathbb{R}$ с единицей называют кольцом главных идеалов, если все его идеалы главные". Таким образом во мн-ве $\mathbb{R}_2$ все его идеалы являются главными в силу выполнения равенства: $\big((s)\big)_{\mathbb{R}} = s\mathbb{R}$, а как следствие из этого $\mathbb{R}_2$ - кольцо главных идеалов.

1.4. Задача №4

Дано:

$\varphi : R \to L$ - эпиморфизм, доказать, что из $B < L \Rightarrow \varphi(\varphi^{-1}(B)) = B$

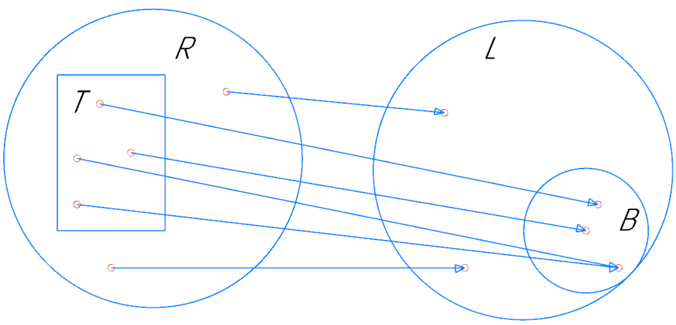
Решение:

По теореме 40: Пусть $\varphi : (R, \cdot) \to (L, \cdot)$ — гомоморфизм групп и если к тому же φ — эпиморфизм (что нам дано по условию), то при $B < L$ (и это нам тоже дано в условии) $\Rightarrow \varphi(\varphi^{-1}(B)) = B$;

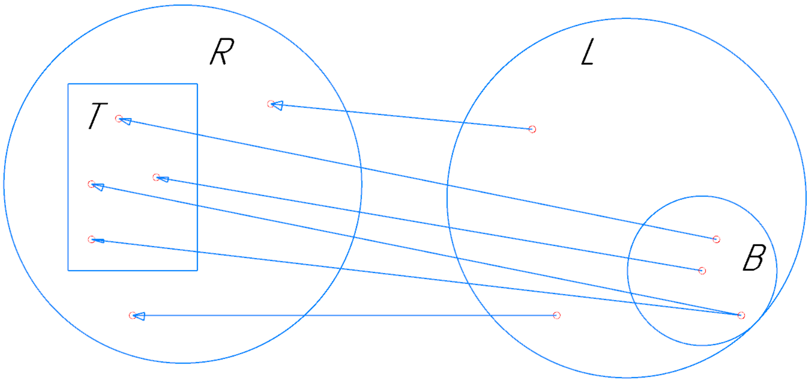
Дополнительное пояснение:

Исходя из определения эпиморфизма можно сказать, что отображение $\varphi : R \to L$ сюръективно. И тогда для этого отображения выполняются следующие свойства: $\varphi(R) = L$; $\varphi(L)^{-1} = R$.

Это будет выглядеть следующим образом:



То есть, из определения сюръекции вытекает то, что для каждого эл-та из L есть хотя бы один эл-т из R. И, так как мы можем выделить некую область B в L, куда будут отображаться эл-ты из какой-то области (Пусть она будет T) в R, мы можем утверждать, что $\varphi(T) = B$, то есть все наши элементы отображённые в B отображаются обратно в область T. Это обратное отображение будет выглядеть следующим образом:



Тогда справедливо утверждение $\varphi(\varphi^{-1}(B)) = B\square$

1.5. Задача №5

Дано:
Пусть $m \in \mathbb{N}, d|m, 1 \leq d \leq m$. Докажите, что $(\mathbb{Z}/m)/([d]_m\mathbb{Z}_m) \equiv \mathbb{Z}/d$.

Решение:
Докажем гомоморфизм:

Гомоморфизм φ кольца $(R, +, \cdot)$ в кольцо $(L, +, \cdot)$ — это такое отображение $\varphi : R \to L$, при котором для любой операции $* \in \{+, \}$ выполнено условие $\forall a, b \in R : \varphi(a*b) = \varphi(a)*\varphi(b)$. $\Leftrightarrow \varphi(ab) = [ab]_d = [a]_d[b]_d = \varphi(a)\varphi(b)$

Построим эпиморфизм:

$\varphi : \mathbb{Z}/m \to \mathbb{Z}/d$, $[a]_m \to [a]_m$.

$Im\varphi = \mathbb{Z}/d$;

В силу того, что $[d]_m\mathbb{Z}_m = \{0, d, \ldots, d(m-1)\}$, то $[d]_m\mathbb{Z}_m = ker\varphi$(все по модулю m обратятся в $[0]_m$).

$\Rightarrow \big(\mathbb{Z}/m\big)/[d]_m\mathbb{Z}_m \cong \mathbb{Z}/d$ (по т. об эпиморфизме колец)$\square$.

2. ОБЩАЯ ТЕОРИЯ ПОЛЕЙ/КОНЕЧНЫЕ ПОЛЯ

2.1. Задача №1 вариант 19

Дано:
$a = e + 3$, $P = \mathbb{C}$
$b = 2y + 4$, $T = \mathbb{Z}_5[y]/_{y^3+4y^2+3}$
Найти минимальный многочлен , $m_{a,P}[x]$
Найти минимальный многочлен , $m_{b,H}[x]$, где H - простое подполе поля

Решение:
Заметим, что неразложимым многочленом над $\mathbb{C}$ является лишь двучлен, тогда $m_{a,P}[x] = (z - e - 3)$

Найдём минимальный многочлен $m_{b,H}[x]$, где H - простое подполе поля:

Простое поле может быть изоморфно $\mathbb{Q}$ или $\mathbb{Z}/p$. В силу конечности нашего поля T его простое подполе может быть изоморфно лишь $\mathbb{Z}/p$. Тогда $H = \mathbb{Z}/5 \cong \mathbb{Z}_5$.

В силу того, что эл-т $b = 2y + 4$ примитивен в поле $\mathbb{Z}_5[y]/_{y^3+4y^2+3}$ построим минимальный многочлен с помощью метода неопределённых коэффициентов относительно него:

$A \cdot \alpha^3 + B \cdot \alpha^2 + C \cdot \alpha + D = A(2y + 4)^3 + B(2y + 4)^2 + C(2y + 4) + D = 3Ay^3 + (3A + 4B)y^2 + (A + B + 2C)y + (4A + B + 4C + D)$

В силу того, что всякий минимальный многочлен унитарен $A = 1 \Rightarrow$

$3y^3 + (3 + 4B)y^2 + (1 + B + 2C)y + (4 + B + 4C + D) = 3(y^3 + 4y^2 + 3) = 3y^3 + 2y^2 + 4$

Тогда составим систему уравнений:

$$\begin{cases} 3 + 4B = 2 \Rightarrow B = 1 \\ 1 + B + 2C = 0 \Rightarrow C = 4 \\ 4 + B + 4C + D = 4 \Rightarrow D = 3 \end{cases} \Rightarrow m_{2y+4,H} = y^3 + y^2 + 4y + 3$$

Проверим его на неприводимость:
Повторений $\frac{3}{2} = 1$ штука. Тогда $k = 1$, а в $u(x)$ пололжим x.
И каждая ступень алгоритма будет в себя включать:
1)$u(x) = u(x)^{p^k}(mod\ f(x))$
2)$\big(f(x), u(x) - x\big)$

Так как у нас всего 1 ступень алгоритма, то проверим НОД $y^5\big(mod\ y^3+y^2+4y+3\big)+4y$ и y^3+y^2+4y+3. Упростим $y^5\big(mod\ y^3+y^2+4y+3\big) = 4y^2+4$

Тогда $\big(4y^2 + 4y + 4, y^3 + y^2 + 4y + 3\big) = 1$

$$
\begin{array}{r|l}
\underline{-\begin{array}{l} y^3+y^2+4y+3 \\ y^3+y^2+y \end{array}} & \frac{4y^2+4y+4}{4y} \\
3y+3 &
\end{array}
$$

$$
\begin{array}{r|l}
\underline{-\begin{array}{l} 4y^2+4y+4 \\ 4y^2+4y \end{array}} & \frac{3y+3}{3y} \\
4 &
\end{array}
$$

$\Rightarrow$ наш $f(y) = y^3 + y^2 + 4y + 3$ неприводим, однако $f(\alpha)$ приводим и α является его корнем $\Rightarrow m_{2y+4,H} = y^3 + y^2 + 4y + 3$.

2.2. Задача №2 вариант 18

Дано:
$f(x) = \frac{1}{2}x^3 - 4$, $P = \mathbb{Q}$.
Найти минимальное поле разложения T многочлена $f(x) \in P[x]$
Разложить $f(x)$ над полем T
Найти $[T : P]$

Решение:
В $\mathbb{Q}$ многочлен можно представить как:

$f(x) = \frac{1}{2}x^3 - 4 = (x-2)(\frac{1}{2}x^2 + x + 2)$, где $\frac{1}{2}x^2 + x + 2$ приводим лишь над полем $\mathbb{C}$ и даёт корни $-1 \pm i\sqrt{3} \Rightarrow$ минимальное поле разложения $\mathbb{C}$.

Тогда разложение многочлена над $\mathbb{C}$ имеет слеующий вид:
$f(x) = \frac{1}{2}x^3 - 4 = (x-2) \cdot (x + 1 - i\sqrt{3}) \cdot (x + 1 + i\sqrt{3})$

Мы знаем, что расширение $[\mathbb{C} : \mathbb{R}] = 2$. Расширение равно 2, так как нам достаточно двух векторов (которые являются базисом): 1, i, для того, чтоб из $\mathbb{R}$ перейти в $\mathbb{C}$. Однако у нас нет фиксированного базиса для $[\mathbb{R} : \mathbb{Q}] \Rightarrow$ это расширение равно ∞. Иначе говоря, $[\mathbb{R} : \mathbb{Q}]$ - трансцендентное расширение, в силу существования $e, \Pi, \sqrt{2}, \ldots$ Следовательно, опираясь на т. о башне полей, мы можем утверждать, что $[\mathbb{C} : \mathbb{Q}] = \infty$ в силу того, что $[\mathbb{R} : \mathbb{Q}] = \infty$.

2.3. Задача №3 вариант 11

Дано:
Приводимы или неприводимы многочлены $f_1(x)$ и $f_2(x)$ в $\mathbb{Z}_5[x]$.

Если оба многочлена неприводимы, то построить в явном виде изоморфизм полей $\mathbb{Z}_5[x]\big/_{f_1(x)} \to \mathbb{Z}_5[x]\big/_{f_2(x)}$, где $f_1(x) = x^4 + 3x^3 + 3x + 1$ и $f_2(x) = x^4 + x^3 + 3x^2 + 4x + 2$.

Решение:

Покажем, что многочлены $f_1(x)$ и $f_2(x)$ неприводимы в $\mathbb{Z}_5[x]$. Для этого воспользуемся алгоритмом проверки на нериводимость:

Повторений $\frac{4}{2} = 2$ штуки. Тогда $k \in \overline{1, 2}$, а в $u(x)$ положим x.

И каждая ступень алгоритма будет в себя включать:

1)$u(x) = u(x)^{p^k}(mod\ f(x))$

2)$\big(f(x), u(x) - x\big)$

Проверим первый многочлен: $u(x) = x^5 \Rightarrow u(x) = x^5(mod(x^4 + 3x^3 + 3x + 1)) = 4x^3 + 2x^2 + 3x + 3$.

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

Далее, НОД от $x^4 + 3x^3 + 3x + 1$ и $4x^3 + 2x^2 + 3x + 3 - x$ равен 1.

Следующий шаг: $\big(4x^3 + 2x^2 + 3x + 3\big)^5(mod(x^4 + 3x^3 + 3x + 1)) = 4x^{15} + 2x^{10} + 3x^5 + 1(mod(x^4 + 3x^3 + 3x + 1)) = 4x^3 + 2x^2$, а НОД от $4x^3 + 2x^2 - x$ и $x^4 + 3x^3 + 3x + 1$ равен одному $\Rightarrow$ он неприводим.

Проверяем второй многочлен: $u(x) = x^5 \Rightarrow u(x) = x^5(mod(x^4 + x^3 + 3x^2 + 4x + 2)) = 3x^3 + 4x^2 + 2x + 2$.

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

НОД от $3x^3 + 4x^2 + 2x + 2$ и $x^4 + x^3 + 3x^2 + 4x + 2$ равен 1.

Следующий шаг: $\big(3x^3 + 4x^2 + 2x + 2\big)^5(mod(x^4 + x^3 + 3x^2 + 4x + 2)) = 3x^{15} + 4x^{10} + 2x^5 + 2(mod(x^4 + x^3 + 3x^2 + 4x + 2)) = 4x^3 + 2x + 3$, а НОД от $4x^3 + 2x + 3 - x$ и $x^4 + x^3 + 3x^2 + 4x + 2$ равен одному $\Rightarrow$ и второй многочлен неприводим.

Тогда построим $\varphi : \mathbb{Z}_5[x]\Big/_{f_1(x)} \to \mathbb{Z}_5[x]\Big/_{f_2(x)}$:

Сначала убедимся, что факторполя равномощны. Их мощность равна $5^4 = 625$, где 5 - модуль, а 4 - максимальная степень многочлена. Тогда факторизуем число $625 - 1 = 624 = 2^4 \cdot 3^1 \cdot 13^1$. Найдём все делтители числа 624: $1, 2, 3, 4, 6, 8, 12, 13, 16, 24, 26, 39, 48, 52, 78, 104, 208, 312, 624$. Рассмотрим все его делители кроме единицы и его самого.

Введём обозначения $P_1 = \mathbb{Z}_5/f_1[x], P_2 = \mathbb{Z}_5/f_2[x]$ а затем проверим, является ли примитивным $x \in P_1$:

$x^2(mod\ f_1(x)) = x^2 \neq 1$
$x^3(mod\ f_1(x)) = x^3 \neq 1$
$x^4(mod\ f_1(x)) = 2x^3 + 2x + 4 \neq 1$
$x^6(mod\ f_1(x)) = 3x^2 + x + 1 \neq 1$
$x^8(mod\ f_1(x)) = 2x^3 + x^2 + x + 2 \neq 1$
$x^{12}(mod\ f_1(x)) = 4x^3 + 2x^2 + 2 \neq 1$
$x^{13}(mod\ f_1(x)) = 1 \Rightarrow$ дальше можно уже не проверять, эл-т $x \in P_1[x]$ не примитивен.

Попробуем проверить примитивен ли $x \in P_2[x]$:
$x^2(mod\ f_2(x)) = x^2 \neq 1$
$x^3(mod\ f_2(x)) = x^3 \neq 1$
$x^4(mod\ f_2(x)) = 4x^3 + 4x^2 + 2x + 2 \neq 1$
$x^6(mod\ f_2(x)) = x^3 + 3x^2 + 4 \neq 1$
$x^8(mod\ f_2(x)) = 4x^2 + 1 \neq 1$
$x^{12}(mod\ f_2(x)) = 3x^3 + 4x^2 + x + 4 \neq 1$
$x^{13}(mod\ f_2(x)) = x^3 + 2x^2 + 2x + 4 \neq 1$
$x^{16}(mod\ f_2(x)) = 4x^3 + x + 4 \neq 1$
$x^{24}(mod\ f_2(x)) = x^3 + 3x + 1 \neq 1$
$x^{26}(mod\ f_2(x)) = x^3 + 2x + 2 \neq 1$
$x^{39}(mod\ f_2(x)) = 3x^2 + 2x + 3 \neq 1$
$x^{48}(mod\ f_2(x)) = 2x^3 + 4x^2 + 2x + 3 \neq 1$
$x^{52}(mod\ f_2(x)) = x^3 + 2x \neq 1$
$x^{78}(mod\ f_2(x)) = 4x^3 + 3x + 1 \neq 1$
$x^{104}(mod\ f_2(x)) = 2x^3 + 4x + 1 \neq 1$
$x^{208}(mod\ f_2(x)) = 2x^3 + 4x \neq 1$
$x^{312}(mod\ f_2(x)) = 4 \neq 1$

$\Rightarrow x$ - наш примитивный элемент из $P_2[x]$, а значит следующим шагом мы можем найти минимальный многочлен. Для этого используем метод неопределённых коэффициентов:

$A \cdot x^4 + B \cdot x^3 + C \cdot x^2 + D \cdot x + F$, где $A = 1$ в силу того что примитивный м-ен всегда унитарный. Следовательно будет:

$x^4 + B \cdot x^3 + C \cdot x^2 + D \cdot x + F = x^4 + x^3 + 3x^2 + 4x + 2 \Rightarrow$

$$\begin{cases} B = 1 \\ C = 3 \\ D = 4 \\ F = 2 \end{cases} \Rightarrow m_{x,P_2} = f_2(x) = x^4 + x^3 + 3x^2 + 4x + 2$$

Он является минимальным для обоих примитивных элементов разных полей, тогда мы можем найти примитивный элемент над $P_1[x]$. Попробуем проверить примитивен ли $3x^3 + x^2 + x + 4 \in P_1$:

$(3x^3 + x^2 + x + 4)^2 (mod\ f_1(x)) = 4x^3 + 3x^2 + 4x + 1 \neq 1$
$(3x^3 + x^2 + x + 4)^3 (mod\ f_1(x)) = 1x^3 + 4x^2 + x + 1 \neq 1$
$(3x^3 + x^2 + x + 4)^4 (mod\ f_1(x)) = 3x^2 + 3x + 3 \neq 1$
$(3x^3 + x^2 + x + 4)^6 (mod\ f_1(x)) = 3x^3 + 3x^2 + 3x + 3 \neq 1$
$(3x^3 + x^2 + x + 4)^8 (mod\ f_1(x)) = x^3 + 2x^2 + x \neq 1$
$(3x^3 + x^2 + x + 4)^{12} (mod\ f_1(x)) = 2x^3 \neq 1$
$(3x^3 + x^2 + x + 4)^{13} (mod\ f_1(x)) = 2x^2 + x \neq 1$
$(3x^3 + x^2 + x + 4)^{16} (mod\ f_1(x)) = 2x^3 + 2x^2 + 2 \neq 1$
$(3x^3 + x^2 + x + 4)^{24} (mod\ f_1(x)) = 2x^2 + 4x + 4 \neq 1$
$(3x^3 + x^2 + x + 4)^{26} (mod\ f_1(x)) = 2x^3 + x^2 + 3x + 1 \neq 1$
$(3x^3 + x^2 + x + 4)^{39} (mod\ f_1(x)) = x^3 + 3x^2 + x + 3 \neq 1$
$(3x^3 + x^2 + x + 4)^{48} (mod\ f_1(x)) = 4x^3 + 2x^2 + 2 \neq 1$
$(3x^3 + x^2 + x + 4)^{52} (mod\ f_1(x)) = 2x^3 + x^2 + 3x + 4 \neq 1$
$(3x^3 + x^2 + x + 4)^{78} (mod\ f_1(x)) = 3x^3 + 4x^2 + 2x + 2 \neq 1$
$(3x^3 + x^2 + x + 4)^{104} (mod\ f_1(x)) = 4x^3 + 2x^2 + x + 4 \neq 1$
$(3x^3 + x^2 + x + 4)^{208} (mod\ f_1(x)) = 4x^3 + 2x^2 + x + 3 \neq 1$
$(3x^3 + x^2 + x + 4)^{312} (mod\ f_1(x)) = 4 \neq 1$

Проверим, является ли наш примитивный элемент из P_1 корнем $f_2(x) = m_{x,P_2}$:

$(3x^3 + x^2 + x + 4)^4 + (3x^3 + x^2 + x + 4)^3 + 3(3x^3 + x^2 + x + 4)^2 + 4(3x^3 + x^2 + x + 4) + 2\big(mod\ f_1(x)\big) = 0 \Rightarrow$ наш примитивный элемент из P_1 - корень для многочлена из P_2, который в свою очередь является минимальным для обоих полей.

Покажем, что у нас $\exists$ отображение $0 \to 0$. В силу того, что $0 \nexists$ в мультипликативной группе поля, рассмотрим любую константу. Видим, что на 156 шаге мы получаем отображение $2 \to 2 \Rightarrow$ так же будет и для нуля.

Минимальный многочлен и два примитивных элемента, которые являются его корнями, из обоих полей есть $\Rightarrow$ введём изоморфизм:

$\varphi : P_1 \to P_2 : \varphi(p = (3x^3 + x^2 + x + 4)^n) = x^n, n \in \overline{1, 624}$

В силу равномощности множеств ($|P_1| = |P_2|$) отображение является сюрьективным, а так же инъективным, потому что оно проходит через примитивыне элементы и каждый раз при возведении в степень а затем взятии модуля будут получаться разные значения. Значит перед нами биективное отображение. Далее проверим на гомоморфность:

$\varphi(a \cdot b) = \varphi((3x^3 + x^2 + x + 4)^{n_1} \cdot (3x^3 + x^2 + x + 4)^{n_2}) = \varphi((3x^3 + x^2 + x + 4)^{n_1 + n_2}) = (x)^{n_1 + n_2} = x^{n_1} \cdot x^{n_2} = \varphi(a) \cdot \varphi(b)$

2.4. Задача №4 вариант 25

Дано:

Постройте неприводимый многочлен над $\mathbb{Z}_5$ степени 23. (с конструктивным алгоритмом построения).

Решение:

Возьмём многочлен $f(z) = z^{23} + z^{19} + z^3 + z^2 + z + 4$ и проверим его на простоту по следующему алгоритму:

Повторений $\frac{23}{2} = 11$ штук. Тогда $k \in \overline{1, 11}$, а в $u(z)$ пололжим z.

И каждая ступень алгоритма будет в себя включать:

$1\big) u(z) = u(z)^{p^k} (mod\ f(z))$

$2\big) \big(f(z), u(z) - z\big)$

$1\big)$ $\underline{u(z)^{11^1} = z^5}$

$\underline{u(z)^{11^1} - z = z^5 + 4}$

НОД: $\big(z^{23} + z^{19} + z^3 + z^2 + z + 4, z^5 + 4z\big) = 1$

Распишем подробно алгоритм Евклида для многочленов:

$z^{23} + z^{19} + z^3 + z^2 + z + 4 = (z^5 + 4z)(z^{18} + 2z^{14} + 2z^{10} + 2z^6 + 2z^2) + (3z^3 + z^2 + z + 4)$

$(z^5 + 4z) = (3z^3 + z^2 + z + 4)(2z^2 + z + 4) + (2x^2 + x + 4)$

$(3z^3 + z^2 + z + 4) = (2z^2 + z + 4)(4z + 1) + (3z)$

$(2z^2 + z + 4) = 3z \cdot (4z + 2) + 4 \Rightarrow$ НОД равен 1.

$2\big)$ Остаток от деления z^{25} на $z^{23} + z^{19} + z^3 + z^2 + z + 4$ даёт $4z^{21} + 4z^5 + 4z^4 + 4z^3 + z^2$

$\underline{u(z)^{11^2} = 4z^{21} + 4z^5 + 4z^4 + 4z^3 + z^2}$

$\underline{u(z)^{11^2} - z = 4z^{21} + 4z^5 + 4z^4 + 4z^3 + z^2 + 4z}$

НОД: $\big(z^{23} + z^{19} + z^3 + z^2 + z + 4, 4z^{21} + 4z^5 + 4z^4 + 4z^3 + z^2 + 4z\big) = 1$

Распишем подробно алгоритм Евклида для многочленов:

$z^{23} + z^{19} + z^3 + z^2 + z + 4 = (4z^{21} + 4z^5 + 4z^4 + 4z^3 + z^2 + 4z)(4z^2) + (z^{19} + 4z^7 + 4z^6 + 4z^5 + z^4 + z^2 + z + 4)$

$(4z^{21} + 4z^5 + 4z^4 + 4z^3 + z^2 + 4z) = (z^{19} + 4z^7 + 4z^6 + 4z^5 + z^4 + z^2 + z + 4)(4z^2) + (4z^9 + 4z^8 + 4z^7 + z^6 + 4z^5 + 4z)$

$(z^{19} + 4z^7 + 4z^6 + 4z^5 + z^4 + z^2 + z + 4) = (4z^9 + 4z^8 + 4z^7 + z^6 + 4z^5 + 4z)(4z^{10} + 3z^9 + 4z^7 + 2z^6 + 2z^5 + 2z^4 + 2z^3 + 2z + 3) + (4z^7 + 4z^5 + 3z^4 + 3z^2 + 4z + 4)$

$(4z^9 + 4z^8 + 4z^7 + z^6 + 4z^5 + 4z) = (4z^7 + 4z^5 + 3z^4 + 3z^2 + 4z + 4)(z^2 + z) + (4z^6 + z^5 + 2z^4 + 3z^3 + 2z^2)$

$(4z^7 + 4z^5 + 3z^4 + 3z^2 + 4z + 4) = (4z^6 + z^5 + 2z^4 + 3z^3 + 2z^2)(z + 1) +$

$(z^5+3z^4+z^2+4z+4)$

$(4z^6+z^5+2z^4+3z^3+2z^2) = (z^5+3z^4+z^2+4z+4)(4z+4)+(4z^3+2z^2+3z+4)$

$(z^5+3z^4+z^2+4z+4) = (4z^3+2z^2+3z+4)(4z^2+2)+(z^2+3z+1)$

$(4z^3+2z^2+3z+4) = (z^2+3z+1)(4z)+(4z+4)$

$(z^2+3z+1) = (4z+4)(4z+3)+4 \Rightarrow$ НОД равен одному.

3) Остаток от деления z^{125} на $z^{23}+z^{19}+z^3+z^2+z+4$ даёт $3z^{19}+2z^{18}+z^{17}+3z^{16}+4z^{15}+4z^{14}+4z^{13}+4z^{12}+4z^{10}+z^9+2z^8+3z^7+z^6+z^5+z^4+z^3+4z^2$

$u(z)^{11^3} = 3z^{19}+2z^{18}+z^{17}+3z^{16}+4z^{15}+4z^{14}+4z^{13}+4z^{12}+4z^{10}+z^9+2z^8+3z^7+z^6+z^5+z^4+z^3+4z^2$

$u(z)^{11^3}-z = 3z^{19}+2z^{18}+z^{17}+3z^{16}+4z^{15}+4z^{14}+4z^{13}+4z^{12}+4z^{10}+z^9+2z^8+3z^7+z^6+z^5+z^4+z^3+4z^2+4z$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, 3z^{19}+2z^{18}+z^{17}+3z^{16}+4z^{15}+4z^{14}+4z^{13}+4z^{12}+4z^{10}+z^9+2z^8+3z^7+z^6+z^5+z^4+z^3+4z^2+4z\big) = 1$

4) $\big(3z^{19}+2z^{18}+z^{17}+3z^{16}+4z^{15}+4z^{14}+4z^{13}+4z^{12}+4z^{10}+z^9+2z^8+3z^7+z^6+z^5+z^4+z^3+4z^2\big)^5(mod\ f(z)) = z^{22}+z^{21}+4z^{20}+z^{18}+4z^{17}+z^{16}+2z^{15}+3z^{14}+4z^{13}+2z^{12}+3z^{11}+2z^{10}+3z^8+3z^5+z^4+3z^2+3z$

$u(z)^{11^4} = z^{22}+z^{21}+4z^{20}+z^{18}+4z^{17}+z^{16}+2z^{15}+3z^{14}+4z^{13}+2z^{12}+3z^{11}+2z^{10}+3z^8+3z^5+z^4+3z^2+3z$

$u(z)^{11^4}-z = z^{22}+z^{21}+4z^{20}+z^{18}+4z^{17}+z^{16}+2z^{15}+3z^{14}+4z^{13}+2z^{12}+3z^{11}+2z^{10}+3z^8+3z^5+z^4+3z^2+2z$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, z^{22}+z^{21}+4z^{20}+z^{18}+4z^{17}+z^{16}+2z^{15}+3z^{14}+4z^{13}+2z^{12}+3z^{11}+2z^{10}+3z^8+3z^5+z^4+3z^2+2z\big) = 1$

5) $\big(z^{22}+z^{21}+4z^{20}+z^{18}+4z^{17}+z^{16}+2z^{15}+3z^{14}+4z^{13}+2z^{12}+3z^{11}+2z^{10}+3z^8+3z^5+z^4+3z^2+3z\big)^5\big(mod\ f(z)\big) = z^{110}+z^{105}+z^{100}+z^{90}+z^{85}+z^{80}+z^{75}+z^{65}+z^{60}+z^{55}+z^{50}+z^{40}+z^{25}+z^{20}+z^{10}+z^5\big(mod\ f(z)\big) = 2z^{22}+z^{21}+4z^{20}+2z^{18}+3z^{17}+3z^{16}+z^{15}+z^{14}+z^{13}+3z^{12}+z^9+3z^8+4z^7+3z^6+z^3+3z^2+3z+3$

$u(z)^{11^5} = 2z^{22}+z^{21}+4z^{20}+2z^{18}+3z^{17}+3z^{16}+z^{15}+z^{14}+z^{13}+3z^{12}+z^9+3z^8+4z^7+3z^6+z^3+3z^2+3z+3$

$u(z)^{11^5}-z = 2z^{22}+z^{21}+4z^{20}+2z^{18}+3z^{17}+3z^{16}+z^{15}+z^{14}+z^{13}+3z^{12}+z^9+3z^8+4z^7+3z^6+z^3+3z^2+2z+3$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, 2z^{22}+z^{21}+4z^{20}+2z^{18}+3z^{17}+3z^{16}+z^{15}+z^{14}+z^{13}+3z^{12}+z^9+3z^8+4z^7+3z^6+z^3+3z^2+2z+3\big) = 1$

6) $\big(2z^{22}+z^{21}+4z^{20}+2z^{18}+3z^{17}+3z^{16}+z^{15}+z^{14}+z^{13}+3z^{12}+z^9+3z^8+4z^7+3z^6+z^3+3z^2+3z+3\big)^5(mod\ f(z)) = z^{110}+z^{105}+z^{100}+z^{90}+z^{85}+z^{80}+z^{75}+z^{70}+z^{65}+z^{60}+z^{45}+z^{40}+z^{35}+z^{30}+z^{15}+z^{10}+z^5+3(mod$

$f(z)) = z^{21}+2z^{20}+4z^{19}+2z^{18}+3z^{16}+3z^{15}+2z^{11}+z^{10}+4z^7+z^6+3z^5+z^4+2z+2$

$u(z)^{11^6} = z^{21}+2z^{20}+4z^{19}+2z^{18}+3z^{16}+3z^{15}+2z^{11}+z^{10}+4z^7+z^6$
$+3z^5+z^4+2z+2$

$u(z)^{11^6} - z = z^{21}+2z^{20}+4z^{19}+2z^{18}+3z^{16}+3z^{15}+2z^{11}+z^{10}+4z^7$
$+z^6+3z^5+z^4+z+2$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, z^{21}+2z^{20}+4z^{19}+2z^{18}+3z^{16}+3z^{15}+2z^{11}+z^{10}+4z^7+z^6+3z^5+z^4+z+2\big) = 1$

7) $\big(z^{21}+2z^{20}+4z^{19}+2z^{18}+3z^{16}+3z^{15}+2z^{11}+z^{10}+4z^7+z^6+3z^5+z^4+2z+2\big)^5 (mod\ f(z)) = z^{105}+2z^{100}+4z^{95}+2z^{90}+3z^{80}+3z^{75}+2z^{55}+z^{50}+4z^{35}+z^{30}+3z^{25}+z^{20}+2z^5+2 (mod\ f(z)) = 3z^{22}+3z^{21}+z^{20}+4z^{19}+z^{18}+3z^{17}+3z^{16}+3z^{15}+2z^{14}+2z^{13}+2z^{12}+3z^{10}+2z^9+2z^8+2z^7+2z^6+4z^5+2z^4+3z^3+4z^2+3z+3$

$u(z)^{11^7} = 3z^{22}+3z^{21}+z^{20}+4z^{19}+z^{18}+3z^{17}+3z^{16}+3z^{15}+2z^{14}+2z^{13}$
$+2z^{12}+3z^{10}+2z^9+2z^8+2z^7+2z^6+4z^5+2z^4+3z^3+4z^2+3z+3$

$u(z)^{11^7} - z = 3z^{22}+3z^{21}+z^{20}+4z^{19}+z^{18}+3z^{17}+3z^{16}+3z^{15}+2z^{14}+2z^{13}$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, 3z^{22}+3z^{21}+z^{20}+4z^{19}+z^{18}+3z^{17}+3z^{16}+3z^{15}+2z^{14}+2z^{13}+2z^{12}+3z^{10}+2z^9+2z^8+2z^7+2z^6+4z^5+2z^4+3z^3+4z^2+2z+3\big) = 1$

8) $\big(3z^{22}+3z^{21}+z^{20}+4z^{19}+z^{18}+3z^{17}+3z^{16}+3z^{15}+2z^{14}+2z^{13}+2z^{12}+3z^{10}+2z^9+2z^8+2z^7+2z^6+4z^5+2z^4+3z^3+4z^2+3z+3\big)^5 (mod\ f(z)) = (mod\ f(z)) = 3z^{110}+3z^{105}+z^{100}+4z^{95}+z^{90}+3z^{85}+3z^{80}+3z^{75}+2z^{65}+2z^{60}+3z^{50}+2z^{45}+2z^{40}+2z^{35}+2z^{30}+4z^{25}+2z^{20}+3z^{15}+4z^{10}+3z^5+3 (mod\ f(z)) = 4z^{22}+3z^{21}+2z^{20}+z^{19}+z^{18}+2z^{15}+2z^{13}+2z^{12}+3z^{10}+3z^9+2z^8+2z^7+4z^6+z^5+z^3+z^2+4z+3$

$u(z)^{11^8} = 4z^{22}+3z^{21}+2z^{20}+z^{19}+z^{18}+2z^{15}+2z^{13}+2z^{12}+3z^{10}+3z^9$
$+2z^8+2z^7+4z^6+z^5+z^3+z^2+4z+3$

$u(z)^{11^8} - z = 4z^{22}+3z^{21}+2z^{20}+z^{19}+z^{18}+2z^{15}+2z^{13}+2z^{12}+3z^{10}$
$+3z^9+2z^8+2z^7+4z^6+z^5+z^3+z^2+3z+3$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, 4z^{22}+3z^{21}+2z^{20}+z^{19}+z^{18}+2z^{15}+2z^{13}+2z^{12}+3z^{10}+3z^9+2z^8+2z^7+4z^6+z^5+z^3+z^2+3z+3\big) = 1$

9) $\big(4z^{22}+3z^{21}+2z^{20}+z^{19}+z^{18}+2z^{15}+2z^{13}+2z^{12}+3z^{10}+3z^9+2z^8+2z^7+4z^6+z^5+z^3+z^2+4z+3\big)^5 (mod\ f(z)) = 4z^{110}+3z^{105}+2z^{100}+z^{95}+z^{90}+2z^{75}+2z^{65}+2z^{60}+3z^{50}+3z^{45}+2z^{40}+2z^{35}+4z^{30}+z^{25}+z^{15}+z^{10}+4z^5+3 (mod\ f(z)) = 4z^{22}+3z^{21}+z^{20}+3z^{19}+3z^{18}+3z^{17}+4z^{14}+3z^{12}+4z^{11}+z^{10}+2z^9+3z^8+4z^7+2z^6+2z^5+4z^4+3z^2+4z+2$

$u(z)^{11^9} = 4z^{22}+3z^{21}+z^{20}+3z^{19}+3z^{18}+3z^{17}+4z^{14}+3z^{12}+4z^{11}+z^{10}$

$+2z^9+3z^8+4z^7+2z^6+2z^5+4z^4+3z^2+4z+2$

$u(z)^{11^9}-z=4z^{22}+3z^{21}+z^{20}+3z^{19}+3z^{18}+3z^{17}+4z^{14}+3z^{12}+4z^{11}$
$+z^{10}+2z^9+3z^8+4z^7+2z^6+2z^5+4z^4+3z^2+3z+2$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, 4z^{22}+3z^{21}+z^{20}+3z^{19}+3z^{18}+3z^{17}+4z^{14}+3z^{12}+4z^{11}+z^{10}+2z^9+3z^8+4z^7+2z^6+2z^5+4z^4+3z^2+3z+2\big)=1$

10) $\big(4z^{22}+3z^{21}+z^{20}+3z^{19}+3z^{18}+3z^{17}+4z^{14}+3z^{12}+4z^{11}+z^{10}+2z^9+3z^8+4z^7+2z^6+2z^5+4z^4+3z^2+3z+2\big)^5(mod\ f(z))=4z^{110}+3z^{105}+z^{100}+3z^{95}+3z^{90}+3z^{85}+4z^{70}+3z^{60}+4z^{55}+z^{50}+2z^{45}+3z^{40}+4z^{35}+2z^{30}+2z^{25}+4z^{20}+3z^{10}+4z^5+2(mod\ f(z))=4z^{22}+z^{21}+2z^{20}+3z^{19}+4z^{17}+2z^{16}+3z^{15}+2z^{14}+4z^{13}+2z^{12}+2z^{11}+3z^{10}+4z^8+3z^7+z^6+3z^5+z^4+3z^3+z^2$

$u(z)^{11^{10}}=4z^{22}+z^{21}+2z^{20}+3z^{19}+4z^{17}+2z^{16}+3z^{15}+2z^{14}+4z^{13}$
$+2z^{12}+2z^{11}+3z^{10}+4z^8+3z^7+z^6+3z^5+z^4+3z^3+z^2$

$u(z)^{11^{10}}-z=4z^{22}+z^{21}+2z^{20}+3z^{19}+4z^{17}+2z^{16}+3z^{15}+2z^{14}+4z^{13}$
$+2z^{12}+2z^{11}+3z^{10}+4z^8+3z^7+z^6+3z^5+z^4+3z^3+z^2+4z$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, 4z^{22}+z^{21}+2z^{20}+3z^{19}+4z^{17}+2z^{16}+3z^{15}+2z^{14}+4z^{13}+2z^{12}+2z^{11}+3z^{10}+4z^8+3z^7+z^6+3z^5+z^4+3z^3+z^2+4z\big)=1$

11) $\big(4z^{22}+z^{21}+2z^{20}+3z^{19}+4z^{17}+2z^{16}+3z^{15}+2z^{14}+4z^{13}+2z^{12}+2z^{11}+3z^{10}+4z^8+3z^7+z^6+3z^5+z^4+3z^3+z^2\big)(mod\ f(z))=4z^{110}+z^{105}+2z^{100}+3z^{95}+4z^{85}+2z^{80}+z^{75}+2z^{70}+4z^{65}+2z^{60}+2z^{55}+3z^{50}+4z^{40}+3z^{35}+z^{30}+3z^{25}+z^{20}+3z^{15}+z^{10}(mod\ f(z))=2z^{22}+2z^{21}+3z^{20}+2z^{19}+2z^{18}+4z^{17}+4z^{16}+3z^{15}+z^{14}+4z^{11}+z^{10}+z^9+3z^8+2z^7+3z^6+3z^5+3z^4+4z^3+4z^2+z+4$

$u(z)^{11^{11}}=2z^{22}+2z^{21}+3z^{20}+2z^{19}+2z^{18}+4z^{17}+4z^{16}+3z^{15}+z^{14}$
$+4z^{11}+z^{10}+z^9+3z^8+2z^7+3z^6+3z^5+3z^4+4z^3+4z^2+z+4$

$u(z)^{11^{11}}-z=2z^{22}+2z^{21}+3z^{20}+2z^{19}+2z^{18}+4z^{17}+4z^{16}+3z^{15}+z^{14}$
$+4z^{11}+z^{10}+z^9+3z^8+2z^7+3z^6+3z^5+3z^4+4z^3+4z^2+4$

НОД: $\big(z^{23}+z^{19}+z^3+z^2+z+4, 2z^{22}+2z^{21}+3z^{20}+2z^{19}+2z^{18}+4z^{17}+4z^{16}+3z^{15}+z^{14}+4z^{11}+z^{10}+z^9+3z^8+2z^7+3z^6+3z^5+3z^4+4z^3+4z^2+4\big)=1$

Так как все НОДы дали 1 то из всех этих вычислений делаем вывод, что наш многочлен неприводим над $\mathbb{Z}_5\square$.

2.5. Задача №5 вариант 27

Дано:

Пусть P' — минимальное поле разложения многочлена $f(x)$ над полем P. Докажите, что если $deg f(x)=m$, то $[P':P]\leq m!$.

Решение:

По следствию т. о строении простых алгебраических расширений, $\big[P_{a_1} : P\big] = deg\ m_{a_1,P'}(x) \leq m, \big[P_{a_2} : P\big] = deg\ m_{a_2,P'}(x) \leq (m-1)\dots$

В силу того, что многчлен $f(x)$ имеет m корней над полем разложения, то мн-во расширений, которыми мы будем дополнять P до P' можно записать как:

$\epsilon = \Big\{\big[P(a_i)_i, P_{i-1}\big| i \in \overline{1,m}, f(a_i) = 0, P_0 = P\big]\Big\}$

Тогда по т. о башне полей имеем:

$\big[P' : P\big] = \big[P' : P_{m-1}\big] \cdot \big[P_{m-1} : P_{m-2}\big] \cdot \dots \cdot \big[P_1 : P\big] \leq 1 \cdot 2 \cdot 3 \cdot \dots \cdot (m-1) \cdot m \leq m!$

3. ЛРП

3.1. Задача №1 вариант 13

Дано:

Определить над каким полем последовательность
$u = 2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, |2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, |2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, |2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, |2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, |2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, |2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1 \dots$

Является ли последовательность u ЛРП? Если да, то каков её характеристический многочлен минимальной степени, общий член $u(i)$, а также $Ann(u)$. Если последовательность - ЛРП, то является ли она периодической? Если да, то вычислите период и длину подхода ЛРП.

Решение:

Цикл: 2, 0, 2, 1, 2, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, 2, 0, 2, 1

u является периодической ЛРП в силу того, что задана над полем. Наш многочлен реверсивен, так как свободный коэффициент многочлена в любом случае обратим $\Rightarrow$ деффект данного многочлена равен 0, а значит подход любой последовательности с данным характеристическим многочленом равен нулю $\Rightarrow \lambda = 0$ и $\forall i \geq \lambda : u(i+52) = u(i)$, где период равен 52, а длина подхода 0.

Т.к. нет цифр превыщающих 2, то ЛРП задана над $\mathbb{Z}_3$

Увидим, что последовательность $2, 0, 2, 2$ встречается внутри изначального периода, а значит ЛРП порядков $1, 2, 3$ нам не подойдут, так как зациклятся на моменте $(\dots, 2, 1, \underline{2, 0, 2}, \dots)$.

Далее предположим, что наша ЛРП порядка 4. Тогда решим систему уравнений:

$$\begin{cases} f_3+2f_2+2f_0=2 \\ 2f_3+f_2+2f_1=1 \\ f_3+2f_2+f_1+2f_0=0 \\ f_2+2f_1+f_0=2 \end{cases} \Rightarrow \left(\begin{array}{cccc|c} 2&0&2&1&2 \\ 0&2&1&2&1 \\ 2&1&2&1&0 \\ 1&2&1&0&2 \end{array}\right) \sim \left(\begin{array}{cccc|c} 2&0&2&1&2 \\ 0&2&1&2&1 \\ 0&1&0&0&1 \\ 0&1&0&2&2 \end{array}\right) \sim \quad (1)$$

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

$\Rightarrow f_3=2, f_2=1, f_1=1, f_0=2$

$\Rightarrow$ характеристический многочлен будет иметь вид $F(x)=x^4-2x^3-x^2-x-2=x^4+x^3+2x^2+2x+1=(x^2+2x+2)^2$. Проверим, даёт ли нам наш характеристический многочлен нужную последовательность при помощи программы на СИ и получим следующую последовательность:

$\underline{2,0,2,1}, 2,1,0,2,0,1,1,1,1,0,1,2,1,2,0,1,0,2,2,2,\underline{2,0,2,1}$

Видим, что последовательность полученная при помощи характеристического многочлена не соответствует нашему изначальному периоду.

Построим предположение, что порядок ЛРП 5, тогда:

$$\begin{cases} 2f_4+f_3+2f_2+2f_0=1 \\ f_4+2f_3+f_2+2f_1=0 \\ f_3+2f_2+f_1+2f_0=2 \\ 2f_4+f_2+2f_1+f_0=1 \\ f_4+2f_3+f_1+2f_0=0 \end{cases} \Rightarrow \left(\begin{array}{ccccc|c} 2&0&2&1&2&1 \\ 0&2&1&2&1&0 \\ 2&1&2&1&0&2 \\ 1&2&1&0&2&1 \\ 2&1&0&2&1&0 \end{array}\right) \sim \quad (3)$$

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

$$\sim \left(\begin{array}{ccccc|c} 2 & 2 & 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 2 & 2 & 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 \end{array}\right) \Rightarrow \qquad (5)$$

$\Rightarrow f_4 = 0, f_3 = 0, f_2 = 1, f_1 = 1, f_0 = 1 \Rightarrow$ характеристический многочлен $F(x) = x^5 - x^2 - x - 1 = x^5 + 2x^2 + 2x + 2 = (x^2 + 2)(x^3 + 2x + 2)$

Проверим, какую последовательность нам даёт наш характеристичекий многочлен:

$\underline{2, 0, 2, 1, 2}, 1, 0, 2, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 2, 0, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 0, 1, 1, 2, 2, 2, 1, 2, 0, 2, 2, 0, 1, 1, 1, 0, 2, 0, \underline{2, 0, 2, 1, 2}$

Увидим, что последовательность эквивалентна нашему периоду, тогда докажем, что многочлен является минимальным в $\mathbb{Z}_3$.

Найдём генератор ЛРП:

$u(0)x^4 + \big(u(1) - 0 \cdot u(0)\big)x^3 + \big(u(2) - 0 \cdot u(1) - 0 \cdot u(0)\big)x^2 + \big(u(3) - 0 \cdot u(2) - 0 \cdot u(1) - u(0)\big)x + \big(u(4) - 0 \cdot u(3) - 0 \cdot u(2) - u(1) - u(0)\big) = 2x^4 + 2x^2 + 2x$, где $u(0) = 2, u(1) = 0, u(2) = 2, u(3) = 1, u(4) = 2$.

Найдём НОД $x^5 + 2x^2 + 2x + 2 = (x^2 + 2)(x^3 + 2x + 2)$ и $2x^4 + 2x^2 + 2x$. Для этого разложим $2x^4 + 2x^2 + 2x = 2x(x + 2)(x^2 + x + 2)$, тогда увидим, что НОД этих двух многочленов равен 1.

$\Rightarrow$ наш характеристический многочлен минимальный.

Тогда определим $Ann(u)$:

$u(i) = u(i-3) + u(i-4) + u(i-5), i \geq 5 \Rightarrow Ann(u) = \mathbb{Z}_3[x](x^5 + 2x^2 + 2x + 2)$

3.2. Задача №2 вариант 14

Дано:

Найти определенный член последовательности.

$f(x) = x^6 + 2x^5 + x^4 + 3x^3 + 5x^2 + 5x + 5$ – характеристический многочлен ЛРП $u, deg f(x) = 6, P = \mathbb{Z}_7, u[\overline{1, 6}] = \big(3, 2, 6, 3, 0, 2\big)$. Найдите:

1$\big)u(i), u(i + 1), u(i + 2), \ldots, u(i + n)$,где $i = 754$;

2$\big)u(j), u(j + 1), u(j + 2), \ldots, u(j + n)$,где $j = 1979$.

Решение:

Для простоты вычислений разложим наш $f(x)$ на линейные множители:

Заметим, что корнем многочлена является $x = 2 \Rightarrow$ найдём кратность этого корня:

$f'(x) = 6x^5 + 3x^4 + 4x^3 + 2x^2 + 3x + 5$

Заметим, что $f'(2) = 6\cdot 2^5+3\cdot 2^4+4\cdot 2^3+2\cdot 2^2+3\cdot 2+5 = 6 \Rightarrow x = 2\big(I\big)$. Тогда поделим $f(x)$ на $(x+5)$ получим $f(x) = x^5+4x^4+2x^3+5x+1$. Заметим, что корнем многочлена так же является $x = 3$. Проверим его кратность:

$f'(x) = 5x^4 + 2x^3 + 6x^2 + 5, f'(3) = 0;$
$f''(x) = 6x^3 + 6x^2 + 5x, f''(3) = 0$
$f^{(III)}(x) = 4x^2 + 5x + 5, f^{(III)}(3) = 0$
$f^{(IV)}(x) = x + 5, f^{(IV)}(3) = 1 \neq 0 \Rightarrow x = 3\big(IV\big)$

Тогда увидим что $f(x)$ раскладывается в следующее произведение:
$f(x) = x^6 + 2x^5 + x^4 + 3x^3 + 5x^2 + 5x + 5 = (x + 5)\cdot(x + 4)^4\cdot(x + 2)$

$k_1 = 0, k_2 = 3, k_3 = 0; \alpha_1 = 2, \alpha_2 = 3, \alpha_3 = 5$

$u = a_{10}\alpha_1^{<0>} + a_{20}\alpha_2^{<0>} + a_{21}\alpha_2^{<1>} + a_{22}\alpha_2^{<2>} + a_{23}\alpha_2^{<3>} + a_{30}\alpha_3^{<0>}$

$$u(i) = a_{10}\cdot 2^i + a_{20}\cdot 3^i + a_{21}\cdot \binom{i}{1} 3^i + a_{22}\cdot \binom{i}{2} 3^i + a_{23}\cdot \binom{i}{3} 3^i + a_{30}\cdot 5^i \tag{6}$$

$$u(i) = a_{10}\cdot 2^i + \left(a_{20} + a_{21}\cdot i + a_{22}\cdot \binom{i}{2} + a_{23}\cdot \binom{i}{3}\right) 3^i + a_{30}\cdot 5^i \tag{7}$$

$$\alpha_1^{<0>} = \left(2^0\cdot 1, 2^0\cdot \binom{1}{0} 2^1, 2^0\cdot \binom{2}{0} 2^2, 2^0\cdot \binom{3}{0} 2^3, 2^0\cdot \binom{4}{0} 2^4, \dots\right) = \tag{8}$$

$= (1, 2, 4, 1, 2, 4, \dots)$

$$\alpha_2^{<0>} = \left(3^0\cdot 1, 3^0\cdot \binom{1}{0} 3^1, 3^0\cdot \binom{2}{0} 3^2, 3^0\cdot \binom{3}{0} 3^3, 3^0\cdot \binom{4}{0} 3^4, \dots\right) = \tag{9}$$

$= (1, 3, 2, 6, 4, 5, \dots)$

$$\alpha_2^{<1>} = \left(3^1\cdot 0, 3^1\cdot 1, 3^1\cdot \binom{2}{1} 3^1, 3^1\cdot \binom{3}{1} 3^2, 3^1\cdot \binom{4}{1} 3^3, \dots\right) = \tag{10}$$

$= (0, 3, 4, 4, 2, 4, \dots)$

$$\alpha_2^{<2>} = \left(3^2\cdot 0, 3^2\cdot 0, 3^2\cdot 1, 3^2\cdot \binom{3}{2} 3^1, 3^2\cdot \binom{4}{2} 3^2, \dots\right) = \tag{11}$$

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

$$\alpha_2^{<3>} = \left(3^3 \cdot 0, 3^3 \cdot 0, 3^3 \cdot 0, 3^3 \cdot 1, 3^3 \cdot \binom{4}{3} 3^1, \dots\right) = \tag{12}$$

$$= (0, 0, 0, 6, 2, 1, \dots)$$

$$\alpha_3^{<0>} = \left(5^0 \cdot 1, 5^0 \cdot \binom{1}{0} 5^1, 5^0 \cdot \binom{2}{0} 5^2, 5^0 \cdot \binom{3}{0} 5^3, 5^0 \cdot \binom{4}{0} 5^4, \dots\right) = \tag{13}$$

$$= (1, 5, 4, 6, 2, 3, \dots)$$

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 2 & 3 & 3 & 0 & 0 & 5 \\ 4 & 2 & 4 & 2 & 0 & 4 \\ 1 & 6 & 4 & 4 & 6 & 6 \\ 2 & 4 & 2 & 3 & 2 & 2 \\ 4 & 5 & 4 & 1 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} a_{10} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{30} \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ 6 \\ 3 \\ 0 \\ 2 \end{pmatrix} \Rightarrow \tag{14}$$

$a_{10} = 0, a_{20} = 3, a_{21} = 0, a_{22} = 0, a_{23} = 1, a_{30} = 0$
Для $i \in \overline{1, \infty}$:

$$u(i) = 3 \cdot 3^{i-1} + \binom{i-1}{3} 3^{i-1} \tag{15}$$

$$u(754) = 3 \cdot 3^{753} + \binom{753}{3} 3^{753} = 3^{125 \cdot 6 + 4} + \binom{4}{3} 3^{125 \cdot 6 + 3} = 4 + 3 = 0 \tag{16}$$

$$u(755) = 3 \cdot 3^{754} + \binom{754}{3} 3^{754} = 3^{125 \cdot 6 + 5} + \binom{5}{3} 3^{125 \cdot 6 + 4} = 5 + 5 = 3 \tag{17}$$

$$u(756) = 3 \cdot 3^{755} + \binom{755}{3} 3^{755} = 3 \tag{18}$$

$$u(757) = 3 \cdot 3^{756} + \binom{756}{3} 3^{756} = 3 \tag{19}$$

$$u(758) = 3 \cdot 3^{757} + \binom{757}{3} 3^{757} = 2 \tag{20}$$

$$u(759) = 3 \cdot 3^{758} + \binom{758}{3} 3^{758} = 6 \tag{21}$$

$$u(760) = 3 \cdot 3^{759} + \binom{759}{3} 3^{759} = 3 \tag{22}$$

$$u(1979) = 3 \cdot 3^{1978} + \binom{1978}{3} 3^{1978} = 3 \cdot 3^{329 \cdot 6+4} + \binom{4}{3} 3^{329 \cdot 6+4} = 5 + 2 = 0 \tag{23}$$

$$u(1980) = 3 \cdot 3^{1979} + \binom{1979}{3} 3^{1979} = 3 \cdot 3^{329 \cdot 6+5} + \binom{5}{3} 3^{329 \cdot 6+5} = 1 + 1 = 2 \tag{24}$$

$$u(1981) = 3 \cdot 3^{1980} + \binom{1980}{3} 3^{1980} = 2 \tag{25}$$

$$u(1982) = 3 \cdot 3^{1981} + \binom{1981}{3} 3^{1981} = 2 \tag{26}$$

$$u(1983) = 3 \cdot 3^{1982} + \binom{1982}{3} 3^{1982} = 6 \tag{27}$$

$$u(1984) = 3 \cdot 3^{1983} + \binom{1983}{3} 3^{1983} = 4 \tag{28}$$

$$u(1985) = 3 \cdot 3^{1984} + \binom{1984}{3} 3^{1984} = 2 \tag{29}$$

Для $i \in \overline{0, \infty}$:

$$u(i) = 3 \cdot 3^i + \binom{i}{3} 3^i \tag{30}$$

$$u(754) = 3 \cdot 3^{754} + \binom{754}{3} 3^{754} = 3^{125 \cdot 6 + 5} + \binom{5}{3} 3^{125 \cdot 6 + 4} = 5 + 5 = 3 \tag{31}$$

$$u(755) = 3 \cdot 3^{755} + \binom{755}{3} 3^{755} = 3^{125 \cdot 6 + 6} + \binom{6}{3} 3^{125 \cdot 6 + 5} = 1 + 2 = 3 \tag{32}$$

$$u(756) = 3 \cdot 3^{756} + \binom{756}{3} 3^{756} = 3 \tag{33}$$

$$u(757) = 3 \cdot 3^{757} + \binom{757}{3} 3^{757} = 2 \tag{34}$$

$$u(758) = 3 \cdot 3^{758} + \binom{758}{3} 3^{758} = 6 \tag{35}$$

$$u(759) = 3 \cdot 3^{759} + \binom{759}{3} 3^{759} = 3 \tag{36}$$

$$u(760) = 3 \cdot 3^{760} + \binom{760}{3} 3^{760} = 0 \tag{37}$$

$$u(1979) = 3 \cdot 3^{1979} + \binom{1979}{3} 3^{1979} = 3 \cdot 3^{329 \cdot 6 + 5} + \binom{5}{3} 3^{329 \cdot 6 + 5} = 1 + 1 = 2 \tag{38}$$

$$u(1980) = 3 \cdot 3^{1980} + \binom{1980}{3} 3^{1980} = 3 \cdot 3^{330 \cdot 6} + \binom{6}{3} 3^{330 \cdot 6} = 3 + 6 = 2 \tag{39}$$

$$u(1981) = 3 \cdot 3^{1981} + \binom{1981}{3} 3^{1981} = 2 \tag{40}$$

$$u(1982) = 3 \cdot 3^{1982} + \binom{1982}{3} 3^{1982} = 6 \tag{41}$$

$$u(1983) = 3 \cdot 3^{1983} + \binom{1983}{3} 3^{1983} = 4 \tag{42}$$

$$u(1984) = 3 \cdot 3^{1984} + \binom{1984}{3} 3^{1984} = 2 \tag{43}$$

$$u(1985) = 3 \cdot 3^{1985} + \binom{1985}{3} 3^{1985} = 0 \tag{44}$$

3.3. Задача №3 вариант 24

<u>Дано:</u>

$R = \mathbb{Z}_8$ - кольцо, $f(x) = x^2 + 5x + 2$ - многочлен над R, $degf(x) = 2$

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 $u[\overline{1,2}] = (3,1)$.

<u>Решение:</u>

$f(x) = x^2 - f_1 x - f_0 = x^2 + 5x + 2 \Rightarrow f_1 = 3, f_0 = 6$

$u(i+2) = f_1 \cdot u(i+1) + f_0 \cdot u(i) = 3 \cdot u(i+1) + 6 \cdot u(i)$

$e^f[\overline{0,1}] = (0,1) \Rightarrow e^f = (0,1,3,\underline{7},\underline{7},\dots) \Rightarrow$ подход равен 3, а период 1.

$\Lambda(e^f) = 3, T(e^f) = 1$. Тогда e^f периодическая так же как и $f(x)$ в силу своей унитарности.

$\Lambda(e^f) = \Lambda(f) = 3, T(e^f) = T(f) = 1.$

Т.к. $\Lambda(f) = 3 \neq 0$ и т.к. свободный член не обратим в поле $\mathbb{Z}_8$, то наш многочлен не реверсивный.

Так как многочлен не реверсивный, то он не является максимальным.

$u[\overline{1,2}] = (3, 1, \underline{5}, \underline{5}, \dots)$

$\Lambda(u) = 2, T(u) = 1$

3.4. Задача №4 вариант 30

Дано:

Задача 4 (Найти циклы Lp(f)) $P = \mathbb{Z}_{13}$ - поле, $f(x) = x^2 + 11$ – характеристический многочлен.

1) На какие циклы разбивается множество $Lp(f)$

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

3) Выпишите цикловой тип многочлена $C_f(y)$.

Решение:

$f(x) = x^2 - f_1 x - f_0 = x^2 + 11 \Rightarrow f_1 = 0, f_0 = 2$

Всего у нас может быть $13^2 = 169$ последовательностей, а не включая нулевую $168 = 24 \cdot 7$, т.е. 7 уникальных.

$u(i + 2) = 2u(i)$ Тогда рассмотрим некоторые циклы:

(0) - цикл длины 1.

$(\underline{0, 1}, 0, 2, 0, 4, 0, 8, 0, 3, 0, 6, 0, 12, 0, 11, 0, 9, 0, 5, 0, 10, 0, 7, \underline{0, 1}, \dots)$

Выше мы видим, что из $(0, 1)$ можно выйти в любую последовательность вида $(0, n)$ или $(n, 0), n \in \overline{1, 12} \Rightarrow$ она является уникальной и длина её периода 24.

Далее рассмотрим последовательность вида $(1, 1)$:

$(\underline{1, 1}, 2, 2, 4, 4, 8, 8, 3, 3, 6, 6, 12, 12, 11, 11, 9, 9, 5, 5, 10, 10, 7, 7, \underline{1, 1}, \dots)$ ещё одна уникальная. Однако у нас вычёркиваются все последовательности вида $(n, n), n \in \underline{1, 12}$ и так далее...

Найдём оставшиеся уникальные последовательности, у которых длина цикла так же будет равна 24, в силу того, что многочлен неприводим над полем:

$(\underline{1, 3}, 2, 6, 4, 12, 8, 11, 3, 9, 6, 5, 12, 10, 11, 7, 9, 1, 5, 2, 10, 4, 7, 8, \underline{1, 3}, \dots)$

$(\underline{1, 4}, 2, 8, 4, 3, 8, 6, 3, 12, 6, 11, 12, 9, 11, 5, 9, 10, 5, 7, 10, 1, 7, 2, \underline{1, 4}, \dots)$

$(\underline{1, 6}, 2, 12, 4, 11, 8, 9, 3, 5, 6, 10, 12, 7, 11, 1, 9, 2, 5, 4, 10, 8, 7, 3, \underline{1, 6}, \dots)$

$(\underline{1, 8}, 2, 3, 4, 6, 8, 12, 3, 11, 6, 9, 12, 5, 11, 10, 9, 7, 5, 1, 10, 2, 7, 4, \underline{1, 8}, \dots)$

$(\underline{1, 11}, 1, 11, 2, 9, 4, 5, 8, 10, 3, 7, 6, 1, 12, 2, 11, 4, 9, 8, 5, 3, 10, 6, 7, 12, \underline{1, 11}, \dots)$

$C_f^1 = 1, C_f^{24} = 7$, для $t \neq 1$ и 24 $C_f^t = 0$

$N_f^1 = 1 \cdot C_f^1 = 1, N_f^{24} = 7 \cdot C_f^{24} = 168$

Многочлен $f(x) = x^2 + 11$ реверсивен, так как его свободный член обратим в $\mathbb{Z}_{13}$, а так же неприводим над нашим полем (т.к. у него нет корней). Тогда цикловой тип многочлена будет выглядеть следующим образом:

$C_f(y) = y + 7y^{24}$