**Типовой расчет по алгебре и геометрии**

**Тришин Никита КМБО-02-19**

**Вариант 23**

**Задача 1**

1) Перечислите все собственные идеалы кольца $\mathbb{Z}_n$.

2) Укажите среди них максимальные идеалы и найдите факторкольца

по ним.

3) Найдите нильрадикал $Rad\mathbb{Z}_n$ и факторкольцо $\mathbb{Z}_n/Rad\mathbb{Z}_n$.

4) Найдите в $\mathbb{Z}_n$ пару идемпотентов и соответствующее им разложение $\mathbb{Z}_n$ во внутреннюю прямую сумму подколец.

5) Выпишите явные формулы прямого и обратного изоморфизма $\mathbb{Z}_n$ и

внешней прямой суммы соотвествующих колец.

$$n = 175 = 5^2 * 7$$

1)

Идеалы $\mathbb{Z}_{175}$ это $I_m$, где $m = \{0, 1, 5, 7, 25, 35\}$

$I_0 = \{0\}$ – нулевой идеал

$I_1 = \mathbb{Z}_{175}$

$I_5 = \{0,5, 10, 15,20, \dots, 170\}$(все числа кратные 5 и меньше 175)$I_5 = 5\mathbb{Z}_{175}$

$I_7 = \{0,7,14,21, \dots, 168\}$ $I_7 = 7\mathbb{Z}_{175}$

$I_{25} = \{0,25,50,75,100,125,150\}$ $I_{25} = 25\mathbb{Z}_{175}$

$I_{35} = \{0,35,70,105,140\}$ $I_{35} = 35\mathbb{Z}_{175}$

Ответ:$I_5, I_7, I_{25}, I_{35}$

2)$I_5$ и $I_7$ – максимальные идеалы

$\mathbb{Z}_{175}\ /\ I_5 = \mathbb{Z}_{175}/\ 5\mathbb{Z}_{175} = \mathbb{Z}_5$

$\mathbb{Z}_{175}\ /\ I_7 = \mathbb{Z}_{175}/\ 7\mathbb{Z}_{175} = \mathbb{Z}_7$

3) Нильпотент в $\mathbb{Z}_{175}$ имеет вид $z = 5^a * 7^b * c;\ \ a, b, c \in \mathbb{N}$

То есть $35, 70, 105, 140$

$Rad\ \mathbb{Z}_{175} = \{0;\ 35;\ 70;\ 105;\ 140\}\ \cong \mathbb{Z}_5$

$\mathbb{Z}_{175}\ /Rad\ \mathbb{Z}_{175} = \mathbb{Z}_{175}\ /\mathbb{Z}_5 = \mathbb{Z}_{35}$

4)$25x + 7y = 1$

$$\frac{25}{7} = 3 + \frac{4}{7} = 3 + \frac{1}{\frac{7}{4}} = 3 + \frac{1}{1 + \frac{3}{4}} = 3 + \frac{1}{1 + \frac{1}{\frac{4}{3}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}} =$$

$$= \frac{7}{2}$$

$25 * 2 + 7 * (-7) = 1$

Идемпотенты:

$e_1 = 25 * 2 = 50$

$e_2 = 7 * (-7) = -49 = 175 - 49 = 126$

$50^2 = 2500 = 50(mod\ 175)$

$126^2 = 15876 = 126(mod\ 175)$

$\mathbb{Z}_{175} = (50) \oplus (126) = (2 * 25_{175}) \oplus (7 * (-7)_{175})$

5)Прямой изоморфизм

$\mathbb{Z}_{175} = \mathbb{Z}_{25} \times \mathbb{Z}_7$

$a \in \mathbb{Z}_{175}$

$a \to (u = a(mod\ 25), v = a(mod\ 7))$

Обратный изоморфизм

$a \in \mathbb{Z}_{175}$

$a = e_1 u + e_2 v\ mod(175);\ \ u \in \mathbb{Z}_{25}, v \in \mathbb{Z}_7$

$a = 126u + 50v\ mod(175);\ \ u \in \mathbb{Z}_{25}, v \in \mathbb{Z}_7$

Проверка:

Например, $12 \in \mathbb{Z}_{175}$

$12 \to (12, 5)$

$12 * 126 + 50 * 5 = 1512 + 250 = 1762 = 12 (mod\ 175)$

Все верно!

$\mathbb{Z}_{175} = \mathbb{Z}_{25} \oplus \mathbb{Z}_7$

$\forall [a]_{175} \in \mathbb{Z}_{175}\ \ f([a]_{175}) = ([a]_{25} [a]_7)$

$\forall ([r_1]_{25}, [r_2]_7) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_7$

$f^{-1}\big(([r_1]_{25}, [r_2]_7)\big) = [126u + 50v]_{175}$

**Задача 2**

1) Докажите, что множество R матриц вида $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

является коммутативным подкольцом кольца матриц $\mathbf{gl}(2, \mathbb{F}_p)$.

2) Сколько в нем элементов?

3) Является ли кольцо R полем?

Если R не является полем, выполните пункты задания A.

Если R является полем, выполните пункты задания B.

A4) Изоморфно ли кольцо R кольцу $\mathbb{Z}_n$ при некотором n?

A5) Опишите группу $R^*$ обратимых элементов кольца R.

A6) Найдите все идеалы R.

A7) Найдите нильрадикал R.

A8) Представьте R в виде внутренней прямой суммы его подколец и изоморфной внешней прямой суммы колец или докажите, что это невозможно.

B4) Найдите характеристику R и его простое подполе F.

B5) Найдите базис и степень расширения поля R над полем F.

B6) Укажите какой-нибудь примитивный элемент расширения поля R над F, найдите его порядок в мультипликативной группе поля R.

B7) Найдите минимальный многочлен указанного примитивного элемента.

B8) Укажите изоморфное полю R факторкольцо кольца многочленов $\mathbb{F}_p[x]$ по некоторому идеалу.

$$p = 5, \begin{cases} \beta + 2\gamma = 0 \\ 3(\delta - \alpha) = \beta \end{cases}$$

1) $\begin{cases} \beta + 2\gamma = 0 \\ 3(\delta - \alpha) = \beta \end{cases}$

$$3(\delta - \alpha) = -2\gamma$$

$$\gamma = \frac{3}{2}\alpha - \frac{3}{2}\delta$$

$$\beta = 3\delta - 3\alpha$$

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & 3\delta - 3\alpha \\ \frac{3}{2}\alpha - \frac{3}{2}\delta & \delta \end{pmatrix}$$

Докажем, что $A_1A_2 = A_2A_1$

$$\begin{pmatrix} \alpha_1 & 3\delta_1 - 3\alpha_1 \\ \frac{3}{2}\alpha_1 - \frac{3}{2}\delta_1 & \delta_1 \end{pmatrix}\begin{pmatrix} \alpha_2 & 3\delta_2 - 3\alpha_2 \\ \frac{3}{2}\alpha_2 - \frac{3}{2}\delta_2 & \delta_2 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1\alpha_2 + \frac{9}{2}(\delta_1 - \alpha_1)(\alpha_2 - \delta_2) & 3\alpha_1(\delta_2 - \alpha_2) + 3\delta_2(\delta_1 - \alpha_1) \\ \frac{3}{2}\alpha_2(\alpha_1 - \delta_1) + \frac{3}{2}\delta_1(\alpha_2 - \delta_2) & \frac{9}{2}(\alpha_1 - \delta_1)(\delta_2 - \alpha_2) + \delta_1\delta_2 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1\alpha_2 + \frac{9}{2}(\delta_1\alpha_2 - \delta_1\delta_2 - \alpha_1\alpha_2 + \alpha_1\delta_2) & 3(\alpha_1\delta_2 - \alpha_1\alpha_2 + \delta_2\delta_1 - \alpha_1\delta_2) \\ \frac{3}{2}(\alpha_2\alpha_1 - \alpha_2\delta_1 + \delta_1\alpha_2 - \delta_1\delta_2) & \frac{9}{2}(\alpha_1\delta_2 - \alpha_1\alpha_2 - \delta_1\delta_2 + \delta_1\alpha_2) \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_1\alpha_2 + \frac{9}{2}(\delta_1\alpha_2 - \delta_1\delta_2 - \alpha_1\alpha_2 + \alpha_1\delta_2) & 3(-\alpha_1\alpha_2 + \delta_2\delta_1) \\ \frac{3}{2}(\alpha_2\alpha_1 - \delta_1\delta_2) & \frac{9}{2}(\alpha_1\delta_2 - \alpha_1\alpha_2 - \delta_1\delta_2 + \delta_1\alpha_2) \end{pmatrix}$$

$$\begin{pmatrix} \alpha_2 & 3\delta_2 - 3\alpha_2 \\ \frac{3}{2}\alpha_2 - \frac{3}{2}\delta_2 & \delta_2 \end{pmatrix}\begin{pmatrix} \alpha_1 & 3\delta_1 - 3\alpha_1 \\ \frac{3}{2}\alpha_1 - \frac{3}{2}\delta_1 & \delta_1 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_2\alpha_1 + \frac{9}{2}(\delta_2 - \alpha_2)(\alpha_1 - \delta_1) & 3\alpha_2(\delta_1 - \alpha_1) + 3\delta_1(\delta_2 - \alpha_2) \\ \frac{3}{2}\alpha_1(\alpha_2 - \delta_2) + \frac{3}{2}\delta_2(\alpha_1 - \delta_1) & \frac{9}{2}(\alpha_2 - \delta_2)(\delta_1 - \alpha_1) + \delta_2\delta_1 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_2\alpha_1 + \frac{9}{2}(\delta_2\alpha_1 - \delta_2\delta_1 - \alpha_2\alpha_1 + \alpha_2\delta_1) & 3(\alpha_2\delta_1 - \alpha_2\alpha_1 + \delta_1\delta_2 - \alpha_1\delta_2) \\ \frac{3}{2}(\alpha_1\alpha_2 - \alpha_1\delta_2 + \delta_2\alpha_1 - \delta_2\delta_1) & \frac{9}{2}(\alpha_2\delta_1 - \alpha_2\alpha_1 - \delta_2\delta_1 + \delta_2\alpha_1) + \delta_2\delta_1 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_1\alpha_2 + \frac{9}{2}(\delta_1\alpha_2 - \delta_1\delta_2 - \alpha_1\alpha_2 + \alpha_1\delta_2) & 3(-\alpha_1\alpha_2 + \delta_2\delta_1) \\ \frac{3}{2}(\alpha_2\alpha_1 - \delta_1\delta_2) & \frac{9}{2}(\alpha_1\delta_2 - \alpha_1\alpha_2 - \delta_1\delta_2 + \delta_1\alpha_2) + \delta_2\delta_1 \end{pmatrix}$$

Как мы видим, $\mathrm{A}_1A_2 = A_2A_1 \Rightarrow R -$ коммутативно

$R$ является подкольцом $\mathbf{gl}(2, \mathbb{F}_p)$ только если

1)$\bar{0} \in R$

2)$\forall a_1, a_2 \in A \Rightarrow a_1 + a_2 \in R$

3)$\forall a \in A\ \exists a^{-1} \in R$

4)$\forall a_1, a_2 \in A \Rightarrow a_1 a_2 \in R$

Проверим эти пункты:

$\alpha, \beta, \delta, \gamma \in \mathbb{F}_5$

1)Пусть $\alpha = \beta = \delta = \gamma = 0$, то есть $\begin{pmatrix} \alpha & \beta \\ \delta & \gamma \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = (\text{очевидно})\bar{0} \in R$

2) $\begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \gamma_1 \end{pmatrix} + \begin{pmatrix} \alpha_2 & \beta_2 \\ \delta_2 & \gamma_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 + \alpha_2 & \beta_1 + \beta_2 \\ \delta_1 + \delta_2 & \gamma_1 + \gamma_2 \end{pmatrix} \in R$

3) $\begin{pmatrix} \alpha & \beta \\ \delta & \gamma \end{pmatrix}^{-1} = \frac{1}{\det\begin{pmatrix} \alpha & \beta \\ \delta & \gamma \end{pmatrix}}\begin{pmatrix} -\gamma & \beta \\ \delta & -\alpha \end{pmatrix} \in R$

4) $\begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \gamma_1 \end{pmatrix}\begin{pmatrix} \alpha_2 & \beta_2 \\ \delta_2 & \gamma_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 + \beta_1\delta_2 & \alpha_1\beta_2 + \beta_1\gamma_2 \\ \delta_1\alpha_2 + \gamma_1\delta_2 & \delta_1\beta_2 + \gamma_1\gamma_2 \end{pmatrix} \in R$

Все пункты верны, значит $R$ является коммутативным подкольцом $\mathbf{gl}(2, \mathbb{F}_p)$

2)$|R| = 5^2 = 25$

3)Проверим, является ли $R$ полем

$R$ является полем только если $R^* = R \ \setminus \{0\}$

$\Rightarrow A \in R^* \Leftrightarrow \det A \neq 0$

$\Leftarrow \det A \neq 0 \Rightarrow \exists\ A^{-1} \in \mathfrak{gl}(2, \mathbb{F}_p)$

Проверим, что $A^{-1} \in R$

$\det A = 0 \Rightarrow \alpha\delta - \beta\gamma = 0$

$$\gamma = \frac{3}{2}\alpha - \frac{3}{2}\delta$$

$\beta = 3\delta - 3\alpha$

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & 3\delta - 3\alpha \\ \frac{3}{2}\alpha - \frac{3}{2}\delta & \delta \end{pmatrix}$$

$$\alpha\delta - (3\delta - 3\alpha)\left(\frac{3}{2}\alpha - \frac{3}{2}\delta\right) = 0$$

$$\alpha\delta + \frac{9}{2}(\alpha^2 - 2\alpha\delta + \delta^2) = 0$$

$$\frac{9}{2}\alpha^2 - 8\alpha\delta + \frac{9}{2}\delta^2 = 0$$

$$\frac{9}{2}\alpha^2 - 8\alpha\delta + \frac{9}{2}\delta^2 = 0 \Leftrightarrow \left[\begin{array}{l} \begin{cases} \alpha = 0 \\ \delta = 0 \end{cases} \Leftrightarrow A = \bar{0} \\ \begin{cases} \dfrac{9\alpha^2}{2\delta^2} - 8 + \dfrac{9\alpha}{2\delta} = 0 \\ \delta \neq 0 \end{cases} \end{array}\right.$$

Пусть $t = \frac{\alpha}{\delta}$

$$\frac{9}{2}t^2 + \frac{9}{2}t - 8 = 0$$

$2t^2 + 2t - 3 = 0$

$t = 0\colon\ -3 \neq 0$

$t = 1\colon 2 + 2 - 3 = 1 \neq 0$

$t = 2: 8 + 4 - 3 = 9 = 4 \neq 0$

$t = 3: 3 + 1 - 3 = 1 \neq 0$

$t = 4: 2 + 8 - 3 = 7 = 2 \neq 0$

При любом $t$ уравнение не имеет корней в $\mathbb{F}_5 \Rightarrow \det A \neq 0 \forall A \in R\ \{\bar{0}\} \Rightarrow$

$\Rightarrow R \setminus \{\bar{0}\} = R^* \Rightarrow R -$ поле

В4)$ord_+ E = 5 \Rightarrow char\ R = 5$

Найдем простое подполе

$F = \{\alpha E, \alpha \in \mathbb{F}_5\} = \left\{\begin{pmatrix} \alpha & 2\alpha \\ 4\alpha & 0 \end{pmatrix}, \alpha \in \mathbb{F}_5\right\}$

$F \simeq \mathbb{F}_5$

В5) Найдем базис $R = \left\{\begin{pmatrix} \alpha & 3\delta - 3\alpha \\ \frac{3}{2}\alpha - \frac{3}{2}\delta & \delta \end{pmatrix}, \alpha, \delta \in \mathbb{F}_5\right\} -$ линейного пространства над $F = \{\alpha E, \alpha \in \mathbb{F}_5\}$

$E = \begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in R$

$E, B -$ линейно независимая система в $R$ над $F$ так как $B \neq \alpha E\ \forall \alpha \in \mathbb{F}_5$

$E, B -$ полная система в $R$ над $F$, так как $A = \begin{pmatrix} \alpha & 3\delta - 3\alpha \\ \frac{3}{2}\alpha - \frac{3}{2}\delta & \delta \end{pmatrix} = \alpha E + \delta B$

$< E, B > -$ базис $R$ над полем $F$

$\dim_F R = 2$

В6)$R = \{\alpha E + \delta B; \alpha, \delta \in \mathbb{F}_5\} \Rightarrow R = F[B] \Rightarrow B -$ примитивный элемент расширения $R$ над $F$.

Найдем $ord\ B$ в $R^*$.

$|R^*| = 24$

$B = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix}$

$< B >= \{\begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix},$

$, \begin{pmatrix} 1 & 4 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 4 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 1 & 0 \end{pmatrix},$

$, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$

$ord\ B = 24$

$E = \begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in R$

B7)$B^2 = \begin{pmatrix} 3 & 3 \\ 1 & 4 \end{pmatrix} = 4B + 3E$

$h(x) = x^2 - 4x - 3 \in \mathbb{F}_5[x] \setminus \{\bar{0}\}$

$h(B) = 0$

$\deg h = 2 = \min(\deg f(x): f(x) \in \mathbb{F}_5[x] \setminus \{\bar{0}\}, f(B) = \bar{0})$ т. к. $1 = \deg f(x) : f(B) = \bar{0}$

Старший коэффициент $h(x) = 1$

Из всего этого следует, что $h(x)$ – максимальный многочлен $B$ над $\mathbb{F}_5$

B8)$R = F[B] = \mathbb{F}_5[B] \backsimeq \mathbb{F}_5 \,/\, (m_B(x)) = \mathbb{F}_5 \,/\, (x^2 - 4x - 3)$

**Задача 3**

Пусть A — наименьшее целостное подкольцо поля $\mathbb{R}$, содержащее число

$\alpha = \sqrt[s]{d}(\alpha -$ корень $f(x) = x^s - d)$.

$K = Quot\ A$ — его поле отношений.

1) Найдите общий вид элементов кольца $A$. Покажите, что $A = \mathbb{Z}[\alpha]$,

где $\alpha$ – корень $f(x)$.

2) Докажите, что $\mathbb{Z}[\alpha] \backsimeq \mathbb{Z}[x] \,/\, (f(x))$

3) Найдите общий вид элементов $\mathbb{Q}[\alpha]$, где $\alpha$ – корень $f(x)$. Докажите,

что $\mathbb{Q}[\alpha] \backsimeq \mathbb{Q}[x] \,/\, (f(x))$.

4) Докажите, что $\mathbb{Q}[\alpha] \backsimeq \mathbb{Q}[x] \,/\, (f(x))$ является полем.

5) Докажите, что $K = \mathbb{Q}[\alpha]$.

6) Найдите простое подполе поля $K$.

7) Найдите степень расширения поля $K$ над его простым подполем.

8) Найдите все подполя поля $K$.

9) Найдите минимальный многочлен $\gamma = 1 + \alpha \in K$ над простым подполем поля $K$.

10) Найдите явную формулу для обратного элемента в $K^*$.

$s = 3, d = 11$
$\alpha = \sqrt[3]{11}$

$f(x) = x^3 - 11$

1)$\left\{\begin{array}{c} A + \text{ЦК} \Rightarrow 1 \in A \Rightarrow \mathbb{Z} \subset A \\ \alpha \in A \Rightarrow \alpha^2 \in A \Rightarrow a + b\alpha + c\alpha^2 \in A \end{array}\right. \Rightarrow \forall a, b, c \in A$

Но $\forall a, b, c \in \mathbb{Z} \Rightarrow \mathbb{Z}[\alpha] = \left\{a + b\sqrt[3]{11} + c * 11^{\frac{2}{3}};\ a, b, c \in \mathbb{Z}\right\} \subset A$

Докажем, что $\mathbb{Z}\left[\sqrt[3]{11}\right]$ – подкольцо $\mathbb{R}$

$1) 0 = 0 + 0 * \sqrt[3]{11} + 0 * 11^{\frac{2}{3}} \in \mathbb{Z}[\alpha]$

$2) d_1 = a_1 + b_1\alpha + c_1\alpha^2 \in \mathbb{Z}[\alpha]$

$d_2 = a_2 + b_2\alpha + c_2\alpha^2 \in \mathbb{Z}[\alpha]$

$d_1 + d_2(\alpha_1 + \alpha_2) + (b_1 + b_2)\alpha + (c_1 + c_2)\alpha^2 \in \mathbb{Z}[\alpha]$

$3) d = a_1 + b_2\alpha + c_2\alpha^2 \in \mathbb{Z}[\alpha], -d = (-a_1) + (-b_2)\alpha + (-c_2)\alpha^2 \in \mathbb{Z}[\alpha]$

$4)\ d_1 = a_1 + b_1\alpha + c_1\alpha^2 \in \mathbb{Z}[\alpha]$

$d_2 = a_2 + b_2\alpha + c_2\alpha^2 \in \mathbb{Z}[\alpha]$

$d_1 d_2 = (a_1 + b_1\alpha + c_1\alpha^2)(a_2 + b_2\alpha + c_2\alpha^2) = (a_1a_2 + b_1b_2 + b_2c_1) +$

$+(a_1b_2 + a_2b_1 + c_1c_2)\alpha + (c_1a_2 + b_1b_2 + a_1c_2)\alpha^2 \in \mathbb{Z}[\alpha]$

Из 1–4 следует, что $\mathbb{Z}[\alpha]$ –подкольцо $\mathbb{R} \Rightarrow \mathbb{Z}[\alpha]$ – ЦК

$\mathbb{Z}[\alpha] \subset A$, но по условию $A$ – наименьшее ЦК в $\mathbb{R}$, содержащее $\alpha \Rightarrow \mathbb{Z}[\alpha] = A$

2)Рассмотрим $\varphi: \mathbb{Z}[x] \to \mathbb{Z}[\alpha]$

$\forall p(x) \in \mathbb{Z}[x]\quad \varphi\big(p(x)\big) = p(\alpha)$

$p(x) = (x^3 - 11)q(x) + r(x) = (x^3 - 11)q(x) + a + bx$

$\varphi\big(p(x)\big) = a + b\alpha \in \mathbb{Z}[\alpha]$

1)$\varphi$ — гомоморфизм подстановки

2)Очевидно, что $Im\ \varphi \subset \mathbb{Z}[\alpha]$

3)$Ker\ \varphi = x^3 - 11$

Из 1,2 и 3 следует, что $\mathbb{Z}[\alpha] \backsimeq \mathbb{Z}[x] / (x^3 - 11)$ (Согласно теореме о гомоморфизме)

3)$\mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2,;\ a, b, c \in \mathbb{Q}\}$

Докажем, что $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/ (x^3 - 11)$

Рассмотрим $\varphi: \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$

$\forall p(x) \in \mathbb{Q}[x]\ \varphi(p(x)) = p(\alpha)$

$p(x) = (x^3 - 11)q(x) + r(x) = (x^3 - 11)q(x) + a + bx + cx^2$

$\varphi(p(x)) = a + b\alpha + c\alpha^2 \in \mathbb{Q}[\alpha]$

1)$\varphi$ — гомоморфизм подстановки

2)Очевидно, что $Im\ \varphi \subset \mathbb{Q}[\alpha]$

$\forall a + b\alpha + c\alpha^2 \exists p(x) = a + bx + cx^2 \in \mathbb{Q}[x]$:

$\varphi(p(x)) = a + b\alpha + c\alpha^2 \Rightarrow \mathbb{Q}[\alpha] \subset Im\ \varphi$

$Im\ \varphi = \mathbb{Q}[\alpha]$

3)$Ker\ \varphi = x^3 - 11$

Из 1,2 и 3 следует, что $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/ (x^3 - 11)$ (По теореме о гомоморфизме)

4)$\mathbb{Q}[\alpha] \backsimeq \mathbb{Q}[x] / (f(x))$ является полем если $f(x)$ не приводим над $\mathbb{Q}$.

$(*)\ \deg f(x) = 3 \Rightarrow f(x)$ неприводим над $\mathbb{Q} \Leftrightarrow f(x)$ не имеет корней в этом поле

Докажем утверждение $(*)$ от противного

Пусть $\sqrt[3]{11} = \frac{m}{n}; m, n \in \mathbb{Z}, (m, n) = 1$

$$11 = \frac{m^3}{n^3} \Leftrightarrow 11n^3 = m^3 \Rightarrow m = 11k \Rightarrow 11n^3 = 11^3k^3 \Rightarrow n^3 = 11^2k^3 \Rightarrow$$

$$\Rightarrow n = 11l$$

$\begin{cases} m = 11k \\ n = 11l \end{cases}$, но $(m, n) = 1$. Противоречие! $\Rightarrow$ многочлен не имеет рациональных корней в $\mathbb{Q}$.

5)$A = \mathbb{Z}[\sqrt[3]{11}] \subset \mathbb{Q}[\sqrt[3]{11}]$, так как $\forall\, z \in \mathbb{Z}[\alpha], z = a + b\alpha + c\alpha^2 \;\; a, b, c \in \mathbb{Z} \subset \mathbb{Q}$

$\mathbb{Q}[\sqrt[3]{11}] \in Quot\ \mathbb{Z}[\sqrt[3]{11}]$ так как

Пусть $p \in \mathbb{Q}[\sqrt[3]{11}]$

$$p = n_1 + n_2\alpha + n_3\alpha^2 = \frac{p_1}{q_1} + \frac{p_2}{q_2}\alpha + \frac{p_3}{q_3}\alpha^2$$

$p_i \in \mathbb{Z}, \qquad q_i \in \mathbb{N}$

$$p = \frac{p_1 q_3 q_2 + p_1 q_1 q_3 \alpha + p_3 q_1 q_2 \alpha^2}{q_1 * q_2 * q_3} = \frac{a}{b}; a \in \mathbb{Z}[\alpha], \beta \in \mathbb{Z}[\alpha] \,/\, \{\bar{0}\}$$

$\Rightarrow \mathbb{Q}[\alpha] \subset Quot\ \mathbb{Z}[\alpha] = Quot\ A$

$\mathbb{Q}[\alpha]$ −поле, $Quot\ A - \min$ поле, содержащее $A \Rightarrow K = \mathbb{Q}[\alpha]$

6)$char\ K = 0 \Rightarrow$ Простое подполе поля $K - \mathbb{Q}$

$\mathbb{Q} \subset K$

7)$\mathbb{Q} \subset K, K = \mathbb{Q}[x] \,/\, (f(x))$, но $f(x)$ − неприводимый многочлен над $\mathbb{Q} \Rightarrow$

$\Rightarrow \dim_{\mathbb{Q}} K = \deg f(x) = 3$

8) $\dim_{\mathbb{Q}} K = 3$ − простое число $\Rightarrow \mathbb{Q}$ единственное собственное подполе $K$

9)$K = \mathbb{Q}[\alpha] \simeq \mathbb{Q}[x] \,/\, (f(x))$, но $f(x)$ −неприводимый многочлен над $\mathbb{Q} \Rightarrow$

$\Rightarrow m\alpha(x) = f(x)$

$\deg \alpha(x) = 3$

$m\alpha(\alpha) = f(\alpha) = \sqrt[3]{11^3} - 11 = 0$

$\alpha = \gamma - 1 \Rightarrow f(\gamma - 1) = (\gamma - 1)^3 - 11 = 0$

Разложим $f(\gamma - 1)$ по степеням $\gamma$

$\gamma^3 - 3\gamma^2 + 3\gamma - 1 - 11 = 0$

$\gamma$ — корень

$h(x) = x^3 - 3x^2 + 3x - 12$

$\deg h(x) = 3$

1)$h(\gamma) = 0$

2)Допустим, степень аннулирующего $\gamma$ многочлена меньше 3. Но тогда степень аннулирующего $\alpha$ меньше 3. Противоречие!

$\Rightarrow \deg h(x) = \min\{\deg g(x) : g(x) \in \mathbb{Q}[x]/\{\bar{0}\} : g(x) = 0\} = 3$

3)Старший коэффициент $h(x) = 1$

1),2),3) $\Rightarrow m\gamma(x) = h(x)$

10)Найдем базис $K$ над $\mathbb{Q}$

$\dim_{\mathbb{Q}} K = 3$

$1, \sqrt[3]{11}, \sqrt[3]{11^2}$ —полная и линейно независимая система в $K = \mathbb{Q}[\sqrt[3]{11}]$

$\forall u \in K^*\ U = a + b\sqrt[3]{11} + c\sqrt[3]{11}; a, b, c \in \mathbb{R}$

При $a^2 + b^2 + c^2 \neq 0\ \exists\ u^{-1} = x + y\sqrt[3]{11} + z\sqrt[3]{11^2} \in K : u * u^{-1} = 0$

Т. е. $\left(a + \sqrt[3]{11}b + \sqrt[3]{11^2}c\right)\left(x + y\sqrt[3]{11} + z\sqrt[3]{11^2}\right) = 1$

$ax + bz + cy + \sqrt[3]{11}(ay + bx + 11bz) + \sqrt[3]{11^2}(az + by + cx) = 1$

$$\begin{cases} ax + bz + cy = 1 \\ ay + bx + 11cz = 0 \\ az + by + cx = 0 \end{cases}$$

$$\begin{pmatrix} a & c & b \\ b & a & 11c \\ c & b & a \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$\Delta = a^3 + 11c^2 + b^2 - 13abc$

$$\Delta_1 = \begin{vmatrix} 1 & c & b \\ 0 & a & 11c \\ 0 & b & a \end{vmatrix} = \begin{vmatrix} a & 11c \\ b & a \end{vmatrix} = a^2 - 11bc$$

$$\Delta_2 = \begin{vmatrix} a & 1 & b \\ b & 0 & 11c \\ c & 0 & a \end{vmatrix} = \begin{vmatrix} b & 11c \\ c & a \end{vmatrix} = ab - 11c^2$$

$$\Delta_3 = \begin{vmatrix} a & c & 1 \\ b & a & 0 \\ c & b & 0 \end{vmatrix} = \begin{vmatrix} b & a \\ c & b \end{vmatrix} = b^2 - ac$$

$$x = \frac{a^2 - 11bc}{a^3 + 11c^2 + b^2 - 13abc}$$

$$y = \frac{ab - 11c^2}{a^3 + 11c^2 + b^2 - 13abc}$$

$$z = \frac{b^2 - ac}{a^3 + 11c^2 + b^2 - 13abc}$$

$$u^{-1} = \frac{a^2 - 11bc}{a^3 + 11c^2 + b^2 - 13abc} + \frac{ab - 11c^2}{a^3 + 11c^2 + b^2 - 13abc}\sqrt[3]{11} + \frac{b^2 - ac}{a^3 + 11c^2 + b^2 - 13abc}\sqrt[3]{11^2}$$

## Задача 4

Пусть $R = A/(p)$, где $A$ — кольцо из задачи 3.

1) Найдите общий вид элементов кольца $R$. Покажите, что $R = \mathbb{F}_p[\beta]$,

где $\beta$ – корень $g(x) = x^s - [d]_p \in \mathbb{F}_p[x]$

2) Найдите $|R|$.

3) Докажите, что $R \backsimeq \mathbb{F}_p[x]/(g(x))$.

4) Выясните, является ли $R$ полем.

Если $R$ не является полем, выполните пункты задания А.

Если $R$ является полем, выполните пункты задания В.

А5) Найдите нильрадикал $Rad\ R$.

А6) Представьте $R$ в виде внутренней прямой суммы его подколец и изоморфной внешней прямой суммы колец или докажите, что это невозможно.

А7) Найдите порядок группы $R^*$ обратимых элементов кольца.

В5) Найдите в поле $R$ его простое подполе и степень расширения $R$ над простым подполем. Найдите минимальный многочлен элемента $\beta$.

В6) Какой известной группе изоморфна мультипликативная группа поля $R^*$? Найдите порядок элемента $\beta$ в $R^*$.

B7) Разложите многочлен $g(x)$ на линейные множители над $R$. Докажите, что $R$ является полем разложения многочлена $g(x)$.

$p = 11$

$A = \left\{a + b\sqrt[3]{11} + c * 11^{\frac{2}{3}};\ a, b, c \in \mathbb{Z}; \sqrt[3]{11^3} - 11 = 0\right\}$

1)$R = A\,/(p) = \{[a]_{11} + [b]_{11}\left[\sqrt[3]{11}\right]_{11} + [c]_{11}\left[\sqrt[3]{11^2}\right]: [a]_{11}, [b]_{11}, [c]_{11} \in \mathbb{Z}_{11} = \mathbb{F}_{11}, \left[\sqrt[3]{11^3}\right]_{11} - \left[\sqrt[3]{11}\right]_{11} = [0]_{11}\}$

Обозначим $k = [a]_{11}, l = [b]_{11}, m = [c]_{11}, \beta = \left[\sqrt[3]{11}\right]_{11}$

$R = \{k + l\beta + m\beta^2: k, l, m \in \mathbb{F}_{11}, \beta^3 - [11]_{11} = \bar{0}\} = \mathbb{F}_{11}[\beta],$

$\beta -$ корень $g(x) = x^3 - [11]_5 \in \mathbb{F}_{11}[x]$

2)$|R| = 11^3 = 1331$

3)Рассмотрим $\varphi: \mathbb{F}_{11}[x] \to \mathbb{F}_{11}\left[\sqrt[3]{11}\right] = \mathbb{F}_{11}[\beta]$

Т. е. $\forall p(x) \in \mathbb{F}_{11}[x]\ \varphi\big(p(x)\big) = p(\beta)\ \beta = \sqrt[3]{11}$

$p(x) = x^3q(x) + r(x) = x^3q(x) + k + lx + mx^2; k, l, m \in \mathbb{F}_{11}$

$\varphi\big(p(x)\big) = k + l\beta + m\beta^2 \in \mathbb{F}_{11}[\beta]$

1)$\varphi -$ гомоморфизм, так как

$\forall p_1(x), p_2(x) \in \mathbb{F}_{11}[x]$

$\varphi\big(p_1(x) + p_2(x)\big) = p_1(\beta) + p_2(\beta) = \varphi\big(p_1(x)\big) + \varphi(p_2(x))$

$\varphi\big(p_1(x) * p_2(x)\big) = p_1(\beta) * p_2(\beta) = \varphi\big(p_1(x)\big) * \varphi(p_2(x))$

2)$Im\ \varphi \subset \mathbb{F}_{11}[\beta]$

$\forall k + l\beta + m\beta^2\ \exists\ p(x) = k + lx + mx^2 \in \mathbb{F}_{11}[x]$:

$\varphi\big(p(x)\big) = k + l\beta + m\beta^2 \Rightarrow \mathbb{F}_{11}[\beta] \subset Im\ \varphi$

$\begin{cases} Im\ \varphi \subset \mathbb{F}_{11}[\beta] \\ \mathbb{F}_{11}[\beta] \subset Im\ \varphi \end{cases} \Rightarrow Im\ \varphi = \mathbb{F}_{11}[\beta]$

3)$Ker\ \varphi = x^3$

1),2),3) $\Rightarrow R \backsimeq \mathbb{F}_p[x]/(x^3)$

4)Для того, чтобы узнать, является ли $R$ полем, нам необходимо узнать, является ли $g(x)$ неприводимым многочленом.

$f(x) = x^3 - [11]_{11} \Rightarrow \beta -$ корень $g(x) = x^3 \Rightarrow$

$\Rightarrow R = \mathbb{F}_{11}[\beta] \simeq \mathbb{F}_{11}[x]\ /(x^3)$

$x^3$ является приводимым над $\mathbb{F}_{11}$

А5)$R = \mathbb{F}_{11}[\beta] \simeq \mathbb{F}_{11}[x]\ /(x^3)$

$[h(x)] \in \mathbb{F}_{11}[x]/(x^3) -$ нильпотент $\Leftrightarrow \exists n \in \mathbb{N}: [h(x)]^n = [\bar{0}]$

$h^n(x) = x^3$

$q_1(x) \Leftrightarrow h(x) = xq_2(x) \Leftrightarrow [h(x)] = [x]$

$\Rightarrow Rad\ \mathbb{F}_{11}[x]/(x^3) = ([x])$

$Rad\ \mathbb{F}_{11}[x]/[x^3] = \{0 + l\beta + m\beta^2\}$

А6) Пусть $A_1, A_2 -$ собственные подкольца $A$, то есть

$A = A_1 \bigoplus A_2 \Leftrightarrow \exists$ нетривиальный идемпотент $e \in A$

Пусть $[h(x)] -$ идемпотент$\Rightarrow [h(x)]^2 = [h(x)] \Leftrightarrow [h(x)][h(x) - 1] = [1] \Rightarrow$

$\Rightarrow h(x)(h(x) - 1) = x^3 q(x)$, но

$$(h(x), h(x) - 1) = [1] \Rightarrow \left[\begin{array}{l} h(x) = x^3 q_1(x) \Leftrightarrow [h(x)] = [\bar{0}] \\ h(x) - 1 = q_2(x) \Leftrightarrow [h(x)] = [1] \end{array}\right. \Rightarrow$$

$\Rightarrow$ В $R$ нет неприводимых идемпотентов $\Rightarrow R$ невозможно разложить прямую сумму колец.

А7)$R \simeq \mathbb{F}_{11}[x]\ /\ (x^3) -$ конечное кольцо$\Leftrightarrow [h(x)] -$ обратимый элемент, то есть не является делителем нуля.

$[h(x)] -$ нильпотент $\Rightarrow$ делитель нуля

Пусть $[h(x)] \notin Rad\ \mathbb{F}_{11}[x]/(x^3)$, тогда

Если $[h(x)][g(x)] = [\bar{0}] \Rightarrow$

$\begin{cases} h(x)g(x) = x^3 q_1(x) \\ h(x) \neq x q_2(x) \end{cases} \Rightarrow g(x) = x^3 q_3(x) \Rightarrow$

$\Rightarrow [g(x)] = [\bar{0}] \Rightarrow [h(x)]$ не делитель нуля $\Rightarrow [h(x)]$ − обратимый элемент $\Rightarrow$

$\Rightarrow R^* = R \,/\, Rad\ R, |R| = 11^3$

$|Rad\ R| = 11^2 \Rightarrow |R^*| = 11^3 - 11^2 = 1210$

**Задача 5**

Даны многочлены $f(x), g(x) \in \mathbb{F}_3[x]$

1) Разложите $f(x)$ на неприводимые множители над $\mathbb{F}_3$. Найдите поле разложения $K$ многочлена $f(x)$.

2) Найдите $\dim_{\mathbb{F}_3} K$ и $|K|$.

3) Решите в поле $K$ уравнение $g(x) = 0$.

4) Докажите, что K является полем разложения многочлена $g(x)$.

5) Найдите какой-нибудь неприводимый многочлен $h(x) \in \mathbb{F}_3[x]$, не имеющий корней в $K$.

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

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

1) $x^4 + x^3 + x^2 - 1 = 0$ при $x = 2$

$(x-2)(x^3 + x + 2) = (x-2)f_1(x)$

$f_1(x) = x^3 + x + 2$ −не имеет корней в $\mathbb{F}_3 \Rightarrow$ неприводимый многочлен над $\mathbb{F}_3$.

Присоединим к $\mathbb{F}_3$ корень $f_1(x)$ $\alpha$.

Рассмотрим $\mathbb{F}_3[\alpha] \simeq \mathbb{F}_3[x] \,/\, f_1(x)$

$\deg f_1(x) = 3$

$\alpha = [x]$ − корень $f_1 \Rightarrow \alpha, \alpha^3, \alpha^9$ − корни $f_1(x)$, различные между собой.

$\alpha, \alpha^3, \alpha^9$ − корни $f_1(x)$, различные между собой.

$\alpha, \alpha^3, \alpha^9 \in \mathbb{F}_3[\alpha] \Rightarrow \mathbb{F}_3[\alpha]$ – поле, над которым $f_1(x)$ раскладывается на линейные множители, и $\mathbb{F}_3[\alpha]$ – минимальное из таких полей$\Rightarrow$

$\Rightarrow \mathbb{F}_3[\alpha] \backsimeq \mathbb{F}_3[x] \,/\, f_1(x)$ – поле разложения $f_1(x)$

$\dim_{\mathbb{F}_3} \mathbb{F}_3[\alpha] = \deg f_1(x) = 3$

$f_1(x) = (x-\alpha)(x-\alpha^3)(x-\alpha^9)$

$\alpha^3 = \alpha - 2$

$\alpha^9 = (\alpha-2)^3 = \alpha^3 - 8 - 6\alpha^2 + 12\alpha = \alpha^3 - 2 = \alpha - 2 - 2 = \alpha - 1$

$f_1(x) = (x-\alpha)(x-\alpha+2)(x-\alpha+1)$

$f(x) = (x-2)(x-\alpha)(x-\alpha+2)(x-\alpha+1)$

$K = \mathbb{F}_5[\alpha]$ – поле разложения $f(x)$

2)$\dim_{\mathbb{F}_3} K = \dim_{\mathbb{F}_3} \mathbb{F}_3[\alpha] = \deg f_1(x) = 3 \;\; |K| = 3^3 = 27$

3)
$g(x) = x^4 + x^3 + x^2 - x + 1 = 0$

Разложим $g(x)$ на неприводимые многочлены

$(x-1)(x-2)(x^2+x-1) = (x-1)(x-2)g_1(x)$

$g_1(x)$ – неприводимый над $\mathbb{F}_5$. Найдем его корни в $K$

$x = a + b\alpha$

$\alpha^2 = 1 - \alpha$

$x^2 + x - 1 = 0$

$a^2 + 2ab\alpha + b^2\alpha^2 + a + b\alpha - 1 = 0$

$a^2 + 2ab\alpha + b^2(1-\alpha) + a + b\alpha - 1 = 0$

$\alpha(2ab - b^2 + b) + a^2 + b^2 + a - 1 = 0$

$$\begin{cases} 2ab - b^2 + b = 0 \\ a^2 + b^2 + a - 1 = 0 \end{cases}$$

$2a - b + 1 = 0$

$b = 2a + 1$

$a^2 + 4a^2 + 4a + 1 + a - 1 = 0$

$2a^2 + 2a = 0$

$a(2a + 2) = 0$

$a = 0 \Rightarrow b = 1$

$a = 2 \Rightarrow b = 2$

$x_1 = \alpha$

$x_2 = 2 + 2\alpha$

$g(x) = (x - 1)(x - 2)(x - 2 - 2\alpha)(x - \alpha)$

4)Как можно видеть из номера выше, все корни $g(x)$ лежат в $K$. При этом заметим, что поле разложения $g(x)$ не может иметь размерность меньше, чем размерность $K$ так как в противном случае $\alpha$ выражался бы линейно через элементы $\mathbb{F}_3 \Rightarrow K$ является полем разложения $g(x)$.

5)Пусть $h(x) = x^3 + 2x^2 + x + 1$

1)неприводимый многочлен над $\mathbb{F}_3$ так как

$h(0) = 1, h(1) = 2, h(2) = 1$

2)$\deg h(x) = 3$

$1), 2) \Rightarrow$ поле разложения $h(x)$ имеет степень расширения 3 над $\mathbb{F}_3$, что больше, чем у $K \Rightarrow K$ не поле разложения $h(x)$.