# Разбор задач типового расчета

## Типовой расчет по алгебре и геометрии (4 семестр).

Задача 1. Все пункты этой задачи разобраны в лекциях.

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

а) $(\mathbb{Z}_n, +)$ – циклическая группа $\Rightarrow$
$\Rightarrow \forall$ её аддитивная подгруппа $H$ – циклическая
и $\forall l \in \mathbb{N} : l \mid n, n = lk$ $\exists!$ подгруппа $H < \mathbb{Z}_n$:
$|H| = l$, а именно $H = \langle k \rangle$.
(см. лекцию 4 прошлого семестра)

б) $\forall$ подгруппа $H < \mathbb{Z}_n$ является идеалом $\mathbb{Z}_n$,
т.к. $\forall \bar{h} \in H \; \forall \bar{t} \in \mathbb{Z}_n \; \bar{t}\bar{h} = \underbrace{\bar{h} + \bar{h} + \ldots + \bar{h}}_{t \text{ раз}} \in H$
(см. лекцию 8)

2) Укажите среди них максимальные идеалы и найдите факторкольца по ним. (см. лекцию 8 и лекцию 9)

3) Найдите нильрадикал $Rad\mathbb{Z}_n$ и факторкольцо $\mathbb{Z}_n / Rad\,\mathbb{Z}_n$. (см. лекцию 9)

4) Найдите в $\mathbb{Z}_n$ пару идемпотентов и соответствующее им разложение $\mathbb{Z}_n$ во внутреннюю прямую сумму подколец. (см. лекцию 10)

5) Выпишите явные формулы прямого и обратного изоморфизма $\mathbb{Z}_n$ и внешней прямой суммы соотвествующих колец. (см. лекцию 10)

Задачу 1 все должен полностью решить, оформив решение на одном отдельном листе так:

ТР по алгебре и геометрии.
Задача 1.
Вариант 35. Яковлев Кирилл. КМБО-06-18
$\mathbb{Z}_n = \mathbb{Z}_{1000}$

Далее идет решение всех пунктов в правильном порядке. Пункты нумеруются. Каждый пункт начинается с формулировки задания.

Задача 2.

Разберем две задачи, аналогичные задаче 2 Т.Р.

2.1. $R = \left\{ \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha+\beta \end{pmatrix} : \alpha, \beta \in \mathbb{F}_7 \right\} \subset \mathrm{gl}(2, \mathbb{F}_7)$

1) Докажите, что множество $R$ является коммутативным подкольцом кольца матриц $\mathfrak{gl}(2, \mathbb{F}_p)$.

Легко проверяется, что $R$ - подкольцо $\mathrm{gl}(2, \mathbb{F}_7)$,
$R$ коммутативно.

$R$ ассоциативно, поскольку $\mathrm{gl}(2, \mathbb{F}_7)$ ассоциативное кольцо.
$R$-кольцо с единицей $E$.
Т.о., $R$ - КАК1.

2) Сколько в нем элементов?

$|R| = 7^2 = 49$

3) Является ли кольцо $R$ полем?

$R$ является полем $\Leftrightarrow R^* = R \setminus \{0\}$.
$A \in R^* \Leftrightarrow \det A \neq 0$.
$\Rightarrow$ ясно
$\Leftarrow$ $\det A \neq 0 \Rightarrow \exists A^{-1} \in \mathrm{gl}(2, \mathbb{F}_7)$. Проверим, что $A^{-1} \in R$.

$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \alpha+\beta & -\beta \\ \beta & \alpha \end{pmatrix} \in R$, т.к. имеет нужный вид.

Рассм. $A = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha+\beta \end{pmatrix} \in R \setminus \{\bar{0}\} \Leftrightarrow \alpha^2 + \beta^2 \neq 0$

$\det A = 0 \Leftrightarrow \alpha^2 + \alpha\beta + \beta^2 = 0 \Leftrightarrow \left[ \begin{cases} \beta = 0 \\ \alpha = 0 \end{cases} \Leftrightarrow A = \bar{0} \right.$ ✗

$\left. \begin{cases} \beta \neq 0 \\ \frac{\alpha^2}{\beta^2} + \frac{\alpha}{\beta} + 1 = 0 \quad (*) \end{cases} \right.$

Обозначим $t = \frac{\alpha}{\beta}$. $(*) \Rightarrow p(t) = t^2 + t + 1 = 0$.
Перебрав все элементы $\mathbb{F}_7$ в $p(t)$, корни $p(t)$ $\left[ \begin{matrix} t=2 \\ t=-3 \end{matrix} \right.$ $\Leftrightarrow$ $\left[ \begin{matrix} \alpha = 2\beta \\ \alpha = -3\beta \end{matrix} \right.$

При тех значениях $\alpha, \beta$ матрица $A \in R \setminus \{0\}$ не имеет $A^{-1} \in R$.
$\Rightarrow$ $R$ не является полем.

Множество необратимых элементов $R \setminus R^* = R_1 \cup R_2$

$\alpha = 2\beta \quad R_1 = \left\{ \begin{pmatrix} 2\beta & \beta \\ -\beta & 3\beta \end{pmatrix} = \beta \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}, \beta \in \mathbb{F}_7 \right\}$

$\alpha = -3\beta \quad R_2 = \left\{ \begin{pmatrix} -3\beta & \beta \\ -\beta & -2\beta \end{pmatrix} = \beta \begin{pmatrix} -3 & 1 \\ -1 & -2 \end{pmatrix}, \beta \in \mathbb{F}_7 \right\}$

$|R \setminus R^*| = 13$

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

Пусть $R \simeq \mathbb{Z}_n \Rightarrow |R| = |\mathbb{Z}_n| \Rightarrow n = 49$

Пусть $f : R \to \mathbb{Z}_{49}$ изоморфизм $\Rightarrow$

$\Rightarrow (R, +) \simeq (\mathbb{Z}_{49}, +)$ – циклическая группа

$\operatorname{ord}_+ \bar{1} = 49$, но $f(E) = \bar{1}$, а $\operatorname{ord}_+ E = 7$ ⚡ $\Rightarrow$

$\Rightarrow R \not\simeq \mathbb{Z}_n$ ни при каком $n$.

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

$(R^*, \cdot)$ – абелева группа $|R^*| = 49 - 13 = 36 = 2^2 \cdot 3^2$

$\Rightarrow R^*$ изоморфна прямой сумме примарных циклических групп $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ или $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$ или $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ или $\mathbb{Z}_4 \times \mathbb{Z}_9$. Нужно выяснить, какой именно.

A6) Найдите все идеалы $R$.

Легко показать, что $R_1, R_2 \lhd A$.

$|(R_i, +)| = 7$, $R_i$ – циклическая группа $\Rightarrow$

$\Rightarrow \forall A \in R_i \setminus \{\bar{0}\}$ порождает $R_i$, $i = 1, 2$

Докажем, что в $A$ нет других собственных идеалов кроме $R_1, R_2$.

Пусть $I$ – собственный идеал $I \lhd R$, $I \neq \{\bar{0}\}, R \Rightarrow$

Все элементы $I$ необратимы. Пусть $A \in I$, $A \neq 0 \Rightarrow$

$\Rightarrow A \in R_1$ или $A \in R_2$.

Если $A \in R_1 \Rightarrow (A) = R_1 \Rightarrow R_1 \subset I \subset R$, но

$|R_1| = 7$, $|R| = 49$, $|R| \vdots |I|$, $|I| \neq |R| \Rightarrow |I| = 7 = |R_1| \Rightarrow I = R_1$

Аналогично, если $A \in R_2 \Rightarrow I = R_2$.

A7) Найдите нильрадикал $R$.

$\operatorname{Rad} R \subset R \setminus R^* = R_1 \cup R_2$

Легко видеть, что среди элементов $R_1 \cup R_2$ нет нетривиальных нильпотентов. $\Rightarrow \operatorname{Rad} R = \{\bar{0}\}$.

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

$e_1 = \begin{pmatrix} -1 & 3 \\ 3 & 2 \end{pmatrix} \in R_1$ – нетривиальный идемпотент $\quad e_2 = 1 - e_1 = \begin{pmatrix} 2 & -3 \\ 3 & -1 \end{pmatrix} \in R_2$ – другой идемпотент

$\Rightarrow R = (e_1) + (1 - e_1) = \left(\begin{pmatrix} -1 & 3 \\ -3 & 2 \end{pmatrix}\right) \oplus \left(\begin{pmatrix} 2 & -3 \\ 3 & -1 \end{pmatrix}\right) = R_1 \oplus R_2 \simeq \mathbb{Z}_7 \oplus \mathbb{Z}_7$

22. $R=\left\{\begin{pmatrix}\alpha & \beta\\ \beta & \alpha+\beta\end{pmatrix}: \alpha,\beta\in\mathbb{F}_5\right\}\subset Gl(2,\mathbb{F}_5)$

1) $R$ – КАК 1
2) $|R|=5^2=25$
3) $R$ является полем $\Leftrightarrow R^*=R\setminus\{0\}$
$A\in R^*\Leftrightarrow \det A\neq 0$.

} Аналогично 2.1

Рассм. $A=\begin{pmatrix}\alpha & \beta\\ \beta & \alpha+\beta\end{pmatrix}\in R\setminus\{\bar 0\}\Leftrightarrow \alpha^2+\beta^2\neq 0$

$$\det A=0\Leftrightarrow \alpha^2+\alpha\beta-\beta^2=0\Leftrightarrow\left[\begin{array}{l}\begin{cases}\beta=0\\ \alpha=0\end{cases}\Leftrightarrow A=\bar 0\ \text{✗}\\ \begin{cases}\beta\neq 0\\ \frac{\alpha^2}{\beta^2}+\frac{\alpha}{\beta}-1=0\ (*)\end{cases}\end{array}\right.$$

Обозначим $t=\frac{\alpha}{\beta}$ $(*)\Rightarrow p(t)=t^2+t-1=0$
Найдем все корни $p(t)$ в $\mathbb{F}_5$. $\exists!$ корень $t=2\Rightarrow$
$\Rightarrow$ При $\alpha=2\beta$ $A\in R\setminus\{0\}$ не имеет обратной в $R$ $\Rightarrow$
$\Rightarrow$ множество необратимых элементов $R\setminus R^*=R_1$

$\alpha=2\beta$ $R_1=\left\{\begin{pmatrix}2\beta & \beta\\ -\beta & 3\beta\end{pmatrix}=\beta\begin{pmatrix}2 & 1\\ -1 & -2\end{pmatrix}: \beta\in\mathbb{F}_5\right\}$;

A4), A5) Аналогично 2.1.

A6) Легко показать, что $R_1\lhd R$ и других собственных идеалов в $R$ нет.

A7) $\operatorname{Rad}R=R_1$
$\operatorname{Rad}R\subset R\setminus R^*=R_1$ и $R_1\subset \operatorname{Rad}R$ (все элементы $R_1$ нильпотентны)

A8) $R$ нельзя представить в виде прямой суммы подколец, т.к. в $R$ нет нетривиальных идемпотентов (если бы они были, то они должны были бы лежать в $R_1=R\setminus R^*$, но там только нильпотенты), а можно просто сослаться на то, что в $R$ нет 2-х собственных идеалов.

## Разбор пунктов 1), 2), 3), B4), B5) задачи 2 Т.Р.

Разберем вариант задачи 2, в котором кольцо $R$ оказывается полем.

2.3 $R = \left\{ \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_5 \right\} \subset \mathfrak{gl}(2, \mathbb{F}_5)$

1) Докажите, что множество $R$ является коммутативным подкольцом кольца матриц $\mathfrak{gl}(2, \mathbb{F}_p)$.

Легко проверяется, что $R$ – подкольцо $\mathfrak{gl}(2, \mathbb{F}_5)$,
$R$ – коммутативно.

2) Сколько в нем элементов?

$|R| = 5^2 = 25$

3) Является ли кольцо $R$ полем?

$R$ – ассоциативное кольцо, т.к. $\mathfrak{gl}(2, \mathbb{F}_5)$ ассоц.,
$R$ – кольцо с единицей $\bar{E} \Rightarrow R$ – КАК1.

$|R| > 1$

$R$ – является полем $\Leftrightarrow R \setminus \{\bar{0}\} = R^*$.

$A = R^* \Leftrightarrow \det A \neq 0$

$(\Rightarrow)$ ясно.

$(\Leftarrow)$ $\det A \neq 0 \; \exists A^{-1} \in \mathfrak{gl}(2, \mathbb{F}_5)$. Проверим, что $A^{-1} \in R$.

$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \alpha & -\beta \\ -2\beta & \alpha \end{pmatrix} \in R$, т.к. имеет нужный вид.

Рассм. $A = \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} \in R \setminus \{\bar{0}\} \Leftrightarrow \alpha^2 + \beta^2 \neq 0$

$\det A = \alpha^2 - 2\beta^2 = 0 \Leftrightarrow \left[ \begin{array}{l} \left[ \begin{array}{l} \beta = 0 \\ \alpha = 0 \end{array} \right. \Leftrightarrow A = \bar{0} \; \not\in \\ \left[ \begin{array}{l} \beta \neq 0 \\ \frac{\alpha^2}{\beta^2} - 2 = 0. \quad (*) \end{array} \right. \end{array} \right.$

Обозначим $\frac{\alpha}{\beta} = t$. $(*) \Rightarrow t^2 = 2$ – не имеет корней в $\mathbb{F}_5$.

$\Rightarrow \det A \neq 0 \quad \forall A \in R \setminus \{\bar{0}\} \Rightarrow R \setminus \{\bar{0}\} = R^* \Rightarrow$

$\Rightarrow R$ явл. полем.

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

B4) Найдите характеристику $R$ и его простое подполе $F$.

$\operatorname{ord}_+ E = 5 \Rightarrow \operatorname{char} R = 5$

Простое подполе $F$ поля $R$.

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

$F \simeq \mathbb{F}_5$

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

Найдем базис $R = \left\{\begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix}, \alpha, \beta \in \mathbb{F}_5\right\}$ - линейного пространства над $F = \{\alpha E, \alpha \in \mathbb{F}_5\} \simeq \mathbb{F}_5$.

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

1) $E, B$ - линейно независимая система в линейном пространстве $R$ над $F$, т.к. $B \neq \alpha E = (\alpha E)E \quad \forall \alpha \in \mathbb{F}_5$, т.к. $\forall \alpha E \in F$

2) $E, B$ - полная система в линейном пространстве $R$ над $F$, т.к.

$\forall A \in R \quad A = \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} = \alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = \alpha E + \beta B = (\alpha E)E + (\beta E)B$

0, 1, 2) $\Rightarrow \langle E, B \rangle$ - базис $R$ над $F$.

(На самом деле, конечно, $F$ можно отождествить с $\mathbb{F}_5$, тогда все будет записываться более компактно.)

# Разбор пунктов В6), В7), В8) задачи 2 ТР

Продолжаем разбирать вариант

$R = \left\{ \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_5 \right\} \subset Gl(2, \mathbb{F}_5)$, который разбирали в прошлый раз -

Мы доказали, что $R$ - поле,

$\langle E, B \rangle$ - базис $R$ над простым подполем $F \simeq \mathbb{F}_5$, $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$,

$\dim_F R = \dim_{\mathbb{F}_5} R = 2$.

В6) Укажите какой-нибудь примитивный элемент расширения поля $R$ над $F$, найдите его порядок в мультипликативной группе поля $R$.

$R = \{ \alpha E + \beta B : \alpha, \beta \in \mathbb{F}_5 \} \Rightarrow R = F[B] = \mathbb{F}_5[B] \Rightarrow$

$\Rightarrow B$ - примитивный элемент расширения $R \supset F \simeq \mathbb{F}_5$.

$R^* = R \setminus \{0\}$ - мультипликативная группа поля $R$, $|R^*| = 24$.

Найдем $\operatorname{ord} B$ в $R^*$.

$B^2 = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2E$ (*) $\Rightarrow B^4 = 4E = -E \Rightarrow B^8 = E \Rightarrow \operatorname{ord} B = 8$,

т. к. $B^3 = 2B \neq E$, $B^6 = 4B^2 = 4 \cdot 2E = 3E \neq E$

В7) Найдите минимальный многочлен указанного примитивного элемента.

(*) $\Leftrightarrow B^2 = 2E \Rightarrow B$ - корень $h(x) = x^2 - 2 \in \mathbb{F}_5[x] \setminus \{0\}$

1) $h(B) = 0$.

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

(можно вместо 2) доказать 2) $h(x)$ - неприводимый над $\mathbb{F}_5$ мн-н).

3) старший коэффициент $h(x)$ равен 1.

1), 2), 3) $\Rightarrow m_B(x) = h(x) = x^2 - 2$ - минимальный мн-н $B$ над $\mathbb{F}_5$.

В8) Укажите изоморфное полю $R$ факторкольцо кольца многочленов $\mathbb{F}_p[x]$ по некоторому идеалу.

$$R = F[B] = \mathbb{F}_5[B] \simeq \mathbb{F}_5[x] / (m_B(x)) = \mathbb{F}_5[x] / (x^2 - 2)$$

# Разбор задач семинара 10.
## и пунктов 1)–5) задачи 3 типового расчета.

(2) Решим задачу в общем виде. Докажем, что $\mathbb{R}[x]/(x^2+ux+v) \simeq \mathbb{C}$, если $\mathcal{D} = u^2-4v<0$.

Рассмотрим $f: \mathbb{R}[x] \to \mathbb{C}$

$\forall p(x) \in \mathbb{R}[x]$ $f(p(x)) = p(z)$, где $z$ – корень $x^2+ux+v$,

$z = -\frac{u}{2} + i\frac{\sqrt{|\mathcal{D}|}}{2}$,

$\bar{z} = -\frac{u}{2} - i\frac{\sqrt{|\mathcal{D}|}}{2}$ – тоже корень $x^2+ux+v$

$(x-z)(x-\bar{z}) = x^2+ux+v$

$\forall p(x) \in \mathbb{R}[x]$ $p(x) = (x^2+ux+v)q(x)+r(x) = (x^2+ux+v)q(x)+c+dx$,

т.к. $\left[\begin{array}{l} r(x)=0 \\ \deg r(x)<2 \end{array}\right.$

$f(p(x)) = p(z) = c+dz = c+d\left(-\frac{u}{2}+i\frac{\sqrt{|\mathcal{D}|}}{2}\right) = \left(c-\frac{u}{2}d\right)+i\frac{\sqrt{|\mathcal{D}|}}{2}d \in \mathbb{C}$

1) $f$ – гомоморфизм подстановки;

2) Очевидно, $\operatorname{Im} f \subset \mathbb{C}$

$\forall a+ib \in \mathbb{C}$ $\exists\, p(x) = c+dx \in \mathbb{R}[x]$ : $\begin{cases} 1\cdot c + \left(-\frac{u}{2}\right)d = a \\ \frac{\sqrt{|\mathcal{D}|}}{2}d = b \end{cases}$ (*)

$\exists!$ решение $(c,d)^T$ СЛАУ (*), поскольку $\Delta = \begin{vmatrix} 1 & -\frac{u}{2} \\ 0 & \frac{\sqrt{|\mathcal{D}|}}{2} \end{vmatrix} = \frac{\sqrt{|\mathcal{D}|}}{2} \neq 0 \Rightarrow$

$\Rightarrow f(p(x)) = f(c+dx) = c+dz = a+bi \Rightarrow \mathbb{C} \subset \operatorname{Im} f$

т.о., $\operatorname{Im} f = \mathbb{C}$

3) $\operatorname{Ker} f = \{p(x) : p(z) = 0\} = \{p(x) : p(x) = (x^2+ux+v)q(x)\} =$

$= (x^2+ux+v)$.

1), 2), 3) по теореме о гомоморфизме

$$\mathbb{R}[x]/(x^2+ux+v) \simeq \mathbb{C}.$$

⚠ (3) В формулировке ошибка. Должно быть, конечно,

$\mathbb{Z}[x]/(n) \simeq \mathbb{Z}_n[x]$.

Легко доказать для $\varphi: \mathbb{Z}[x] \to \mathbb{Z}_n[x]$

$\forall p(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m \in \mathbb{Z}[x]$ $\varphi(p(x)) = [a_0]_n x^m + [a_1]_n x^{m-1} + \ldots + [a_m]_n$,

что 1) $\varphi$ – гомоморфизм,

2) $\operatorname{Im}\varphi = \mathbb{Z}_n[x]$,

3) $\operatorname{Ker}\varphi = (n) = n\mathbb{Z}[x]$

1), 2), 3) $\Rightarrow$ по теореме о гомоморфизме $\mathbb{Z}[x]/(n) \simeq \mathbb{Z}_n[x]$.

④ Доказать, что $\mathbb{Z}[x]/(x^2-2) \simeq \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$

Решается тоже по теореме о гомоморфизме.

Рассм. $\varphi: \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{2}]$

$\forall p(x) \in \mathbb{Z}[x]$ $\varphi(p(x)) = p(\sqrt{2})$

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

$\varphi(p(x)) = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

Можно считать, что деление с остатком происходит в $\mathbb{Q}[x]$, но поскольку старший коэф. $x^2-2$ единица, $q(x), r(x) \in \mathbb{Z}[x]$. ($\mathbb{Q}[x]$ – ЕК)

1) $\varphi$ – гомоморфизм подстановки

2) Очевидно, $\operatorname{Im}\varphi \subset \mathbb{Z}[\sqrt{2}]$.

$\forall a + b\sqrt{2}$ $\exists\, p(x) = a + bx \in \mathbb{Z}[x]$: $\varphi(p(x)) = a + b\sqrt{2} \Rightarrow \mathbb{Z}[\sqrt{2}] \subset \operatorname{Im}\varphi$

$\operatorname{Im}\varphi = \mathbb{Z}[\sqrt{2}]$

3) $\operatorname{Ker}\varphi = (x^2-2)$

Из 1), 2), 3) по теореме о гомоморфизме $\Rightarrow \mathbb{Z}[x]/(x^2-2) \simeq \mathbb{Z}[\sqrt{2}]$.

⑤ Совершенно аналогично доказывается, что

$$\mathbb{Q}[x]/(x^2-2) \simeq \mathbb{Q}[\sqrt{2}].$$

⑥ Доказать, что $\mathbb{Z}[x]/(x^2-2) \not\simeq \mathbb{Z}[x]/(x^2-3)$

Вспомним, как доказывается, что $\sqrt{3} \notin \mathbb{Q}$.

Пусть $\sqrt{3} = \frac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$, $(m, n) = 1$.

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

$\begin{cases} m = 3k \\ n = 3\ell \end{cases}$, но $(m, n) = 1$ ↯ $\Rightarrow \sqrt{3} \notin \mathbb{Q}$ (т.е. многочлен $x^2-3$ не имеет рациональных корней)

$\mathbb{Z}[x]/(x^2-2) \simeq \mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[x]/(x^2-3) \simeq \mathbb{Z}[\sqrt{3}]$.

Докажем, что $\mathbb{Z}[\sqrt{2}] \neq \mathbb{Z}[\sqrt{3}]$ от противного.

Пусть $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{3}]$ изоморфизм

$\varphi(\sqrt{2}) = a + b\sqrt{3}$, $a, b \in \mathbb{Z}$

$\varphi(2) = \varphi(\sqrt{2}\sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = (a+b\sqrt{3})^2$

с другой стороны $\varphi(2) = \varphi(1+1) = \varphi(1)+\varphi(1) = 1+1 = 2$ $\Big\} \Rightarrow$

$\Rightarrow 2 = (a+b\sqrt{3})^2$.

Докажем, что это невозможно, т.е. что $\sqrt{2} \notin \mathbb{Z}[\sqrt{3}]$.

Пусть $2 = a^2 + 2ab\sqrt{3} + 3b^2$

$2ab\sqrt{3} = 2 - a^2 - b^2$

Если $ab = 0 \Leftrightarrow \begin{bmatrix} a=0 & 2-3b^2=0 \quad 2=3b^2 \Rightarrow 2 \vdots 3 \ \text{✗} \\ b=0 & 2-a^2=0 \quad 2=a^2 \Rightarrow a \vdots 2 \Rightarrow 2 \vdots 4 \ \text{✗} \end{bmatrix}$

Если $ab \neq 0 \Rightarrow \sqrt{3} = \dfrac{2-a^2-b^2}{2ab} \in \mathbb{Q}$ ✗

$\Rightarrow \mathbb{Z}[\sqrt{2}] \neq \mathbb{Z}[\sqrt{3}] \Rightarrow \mathbb{Z}[x]/(x^2-2) \neq \mathbb{Z}[x]/(x^2-3)$

Аналогично можно доказать, что

$\mathbb{Q}[x]/(x^2-2) \neq \mathbb{Q}[x]/(x^2-3)$.

## Т.Р. Задача 3. Разберем пункты 1)–5).

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 $f(x)$.

В случае $s=2$ $\begin{cases} A - \text{ЧК} \Rightarrow 1 \in A \Rightarrow \mathbb{Z} \subset A \\ \alpha \in A \end{cases} \Rightarrow a + b\alpha \in A \quad \forall a, b \in \mathbb{Z} \Rightarrow$

$\Rightarrow \mathbb{Z}[\alpha] = \{ a + b\alpha \vdots a, b \in \mathbb{Z} \} \subset A$

В случае $s=3$ $\begin{cases} A - \text{УК} \Rightarrow 1 \in A \Rightarrow \mathbb{Z} \subset A \\ \alpha \in A \Rightarrow \alpha^2 \in A \end{cases} \Rightarrow a+b\alpha+c\alpha^2 \in A \ \forall a,b,c \in \mathbb{Z} \Rightarrow$

$\Rightarrow \mathbb{Z}[\alpha] = \{ a+b\alpha+c\alpha^2 : a,b,c \in \mathbb{Z} \} \subset A$

Легко проверяется, что $\mathbb{Z}[\alpha]$ – подкольцо $\mathbb{R} \Rightarrow \mathbb{Z}[\alpha]$ – УК.

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

2) Докажите, что $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(f(x))$. – см. ④ выше.

(В случае $s=3$ $r(x) = a+bx+cx^2$)

3) Найдите общий вид элементов $\mathbb{Q}[\alpha]$, где $\alpha$ – корень $f(x)$. Докажите, что $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/(f(x))$. – аналогично ④.

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

Для этого нужно показать, что $f(x)$ – многочлен, неприводимый над $\mathbb{Q}$.

(Многочлен второй или третьей степени неприводим над полем $\Leftrightarrow$ он не имеет корней в этом поле)

$f(x)$ не имеет корней в $\mathbb{Q}$. (Доказывается аналогично началу ⑥.)

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

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

↑ пояснить ↑ пояснить

В ④ доказывается, что $\mathbb{Q}[\alpha]$ – поле, но $K = \operatorname{Quot} A$ – наименьшее поле, содержащее $A$, $\Rightarrow K = \mathbb{Q}[\alpha]$.

# Разбор пунктов 6), 7), 8), 9), 10) задачи 3 ТР

$K = \mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/(f(x))$, где $f(x) = x^5 - d$ – неприводимый над $\mathbb{Q}$ многочлен.

6) Найдите простое подполе поля $K$.

$\mathrm{char}\, K = 0 \Rightarrow$ Простое подполе поля $K$ – $\mathbb{Q}$. $\mathbb{Q} \subset K$

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

$\mathbb{Q} \subset K$, $K = \mathbb{Q}[x]/(f(x))$, где $f(x) = x^5 - d$ – неприводимый над $\mathbb{Q}$ мн-к

$\Rightarrow \dim_{\mathbb{Q}} K = \deg f(x) = 5$

8) Найдите все подполя поля $K$.

$K$ не имеет других собственных подполей, кроме простого подполя $\mathbb{Q}$, т.к. $\dim_{\mathbb{Q}} K = 5$ – простое число. $\Rightarrow$
$\Rightarrow \mathbb{Q}$ – единственное собственное подполе $K$.

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

$K = \mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/(f(x))$, где $f(x) = x^5 - d$ – неприводимый над $\mathbb{Q}$ мн-к

$\Rightarrow m_\alpha(x) = f(x) = x^5 - d$, $\deg_\alpha(x) = 5$

$m_\alpha(\alpha) = f(\alpha) = \alpha^5 - d = 0$, $\alpha = \gamma - 1 \Rightarrow f(\gamma - 1) = (\gamma - 1)^5 - d = 0$

Разложим $f(\gamma - 1)$ по степеням $\gamma$, например, $5 = 3$

$\gamma^3 - 3\gamma^2 + 3\gamma - 1 - d = 0$ $\gamma$ – корень $h(x) = x^3 - 3x^2 + 3x - (d+1)$, $\deg h(x) = 3 = 5$

1) $h(\gamma) = 0$
2) если ли бы степень аннулирующего $\gamma$ многочлена могла бы быть меньше 5, то и степень аннулирующего $\alpha$ мн-на была бы меньше 5 $\not\Rightarrow \deg h(x) = \min\{\deg g(x) : g(x) \in \mathbb{Q}[x] \setminus \{0\} : g(\gamma) = 0\} = 5$
3) старший коэффициент $h(x)$ равен 1

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

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

Рассмотрим для определенности $5 = 3$.
$\langle 1, \alpha, \alpha^2 \rangle$ – базис $K$ над $\mathbb{Q}$, т.к. 0) $1, \alpha, \alpha^2 \in K$,
1) $1, \alpha, \alpha^2$ – полная система в $K = \mathbb{Q}[\alpha]$,
2) $\dim_{\mathbb{Q}} K = 5 = 3$

$\forall u \in K^*$ $u = a + b\alpha + c\alpha^2$, $a, b, c \in \mathbb{Q}$, $a^2 + b^2 + c^2 \neq 0$ $\exists u^{-1} = x + y\alpha + z\alpha^2 \in K$: $uu^{-1} = 1$,
т.е. $(a + b\alpha + c\alpha^2)(x + y\alpha + z\alpha^2) = 1$. Перемножив в $K = \mathbb{Q}[\alpha]$ выражения в левой части, приравняем коэффициенты при базисных векторах $1, \alpha, \alpha^2$ в левой и правой частях равенства. Получим СЛАУ. Решив её, например, методом Крамера, получим нужную формулу $u^{-1}$, подставив вместо $x, y, z$ их выражения через $a, b, c$.

# Разбор задачи 4 ТР.

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 $g(x) = x^s - [d]_p \in \mathbb{F}_p[x]$.

Пусть, например,

$$A = \mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Z},\ \alpha^3 - d = 0\} \Rightarrow$$

$$\Rightarrow R = A/(p) = \{[a]_p + [b]_p[\alpha]_p + [c]_p[\alpha]_p^2 : [a]_p, [b]_p, [c]_p \in \mathbb{Z}_p = \mathbb{F}_p,\ [\alpha]_p^3 - [d]_p = [0]_p\}$$

Обозначим $k = [a]_p$, $l = [b]_p$, $m = [c]_p$, $\beta = [\alpha]_p$

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

$\beta$ – корень $g(x) = x^3 - [d]_p \in \mathbb{F}_p[x]$

Например, если $d = 14$, $p = 13$, $g(x) = x^3 - 1 \in \mathbb{F}_p[x]$.

2) Найдите $|R|$.

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

} решаются стандартно (см. №2 ТР)

4) Выясните, является ли $R$ полем.

$R = \mathbb{F}_p[x]/(g(x))$ является полем $\Leftrightarrow$ $g(x)$ – неприводимый многочлен над $\mathbb{F}_p$.

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

$R$ не явл. полем $\Leftrightarrow$ $g(x)$ – приводимый многочлен.

Рассмотрим 2 принципиально разных варианта.

Пусть $p = 13$.

1) $\alpha$ – корень $f(x) = x^3 - 13 \Rightarrow \beta$ – корень $g(x) = x^3 \Rightarrow R = \mathbb{F}_{13}[\beta] \simeq \mathbb{F}_{13}[x]/(x^3)$

2) $\alpha$ – корень $f(x) = x^3 - 14 \Rightarrow \beta$ – корень $g(x) = x^3 - 1 = (x-1)(x^2+x+1)$,

$x$, $x^2+x+1$ неприводимы над $\mathbb{F}_{13}$ и $((x-1), (x^2+x+1)) = 1$.

$$R = \mathbb{F}_{13}[\beta] \simeq \mathbb{F}_3[x]/((x-1)(x^2+x+1))$$

A5) Найдите нильрадикал $Rad\,R$.

1) $R = \mathbb{F}_{13}[\beta] \simeq \mathbb{F}_{13}[x]/(x^3)$

$[h(x)] \in \mathbb{F}_{13}[x]/(x^3)$ – нильпотент $\Leftrightarrow$

$\Leftrightarrow \exists n \in \mathbb{N} : [h(x)]^n = [\bar{0}]$, т.е. $h^n(x) = x^3 q_1(x) \Leftrightarrow h(x) = x\, q_2(x) \Leftrightarrow$

в силу факториальности $\mathbb{F}_{13}[x]$ и неприводимости $x$.

$\Leftrightarrow [h(x)] = [x]$.

Следовательно, $Rad\ \mathbb{F}_{13}[x]/(x^3) = ([x])$, т.е.

$Rad R = (\beta) = \{0 + l\beta + m\beta^2\}$ ←

(Можно было сразу найти радикал в таком виде. Я специально разбираю более общий случай, т.к. такие конструкции используются в тестах.)

2) $R = \mathbb{F}_{13}[\beta] \simeq \mathbb{F}_{13}[x]/((x-1)(x^2+x+1))$

$[h(x)] \in \mathbb{F}_{13}[x]/((x-1)(x^2+x+1))$ – нильпотент $\Leftrightarrow \exists n \in \mathbb{N} : [h(x)]^n = [\bar{0}]$, т.е.

$h^n(x) = (x-1)(x^2+x+1)q_1(x) \Rightarrow h(x) = (x-1)(x^2+x+1)q_2(x) \Rightarrow [h(x)] = [\bar{0}]$,

поскольку $(x-1), (x^2+x+1)$ – неприводимые взаимно простые многочлены, а $\mathbb{F}_{13}[x]$ – факториальное кольцо.

Следовательно, $Rad\,R = \{\bar{0}\}$.

A6) Представьте $R$ в виде внутренней прямой суммы его подколец и изоморфной внешней прямой суммы колец или докажите, что это невозможно. *Сформулируйте критерий разложения кольца в прямую сумму подколец.*

1) $R \simeq \mathbb{F}_{13}[x]/(x^3)$.

Пусть $[h(x)]$ – идемпотент $\Rightarrow [h(x)]^2 = [h(x)] \Leftrightarrow [h(x)]([h(x)] - [1]) = [0] \Rightarrow$

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

$\Rightarrow \begin{bmatrix} h(x) = x^3 q_1(x) & \Leftrightarrow [h(x)] = [\bar{0}] \\ h(x) - 1 = x^3 q_2(x) & \Leftrightarrow [h(x)] = [1] \end{bmatrix} \Rightarrow$ в $R$ нет нетривиальных идемпотентов $\Rightarrow R$ невозможно разложить в прямую сумму колец.

2) $R \simeq \mathbb{F}_{13}[x]/((x-1)(x^2+x+1)) \simeq \mathbb{F}_{13}[x]/(x-1) \oplus \mathbb{F}_{13}[x]/(x^2+x+1) \simeq$

$\simeq \mathbb{F}_{13} \oplus \mathbb{F}_{13^2}$ – внешняя прямая сумма колец (в данном случае полей, поскольку $(x-1)$ и $(x^2+x-1)$-неприводимые многочлены).

(Отсюда тоже ясно, что $R$ не имеет нетривиальных нильпотентов, т. к. $(a,b)^4 = (a^4, b^4)$, а в полях нет нильпотентов, кроме 0.)

Разложим теперь $R$ во внутреннюю прямую сумму колец. Для этого нужно найти пару нетривиальных идемпотентов.

$((x-1), (x^2+x+1)) = 1 \Rightarrow \exists u(x), v(x) \in \mathbb{F}_{13}[x]: (x-1)u(x) + (x^2+x+1)v(x) = 1.$

$$C = \begin{pmatrix} x-1 & x^2+x+1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{-xc^1+c^2} \begin{pmatrix} x-1 & 2x+1 \\ 1 & -x \\ 0 & 1 \end{pmatrix} \xrightarrow{2c^1+c^2} \begin{pmatrix} x-1 & 3 \\ 1 & -x-2 \\ 0 & 1 \end{pmatrix} \xrightarrow{-4c^2}$$

$$\longrightarrow \begin{pmatrix} x-1 & 1 \\ 1 & 4x+8 \\ 0 & -4 \end{pmatrix} \qquad u_0(x) = 4x+8 = 4x-5 \qquad v_0(x) = -4$$

Сделайте проверку.

$e_1 = (\beta^2+\beta+1)v_0(\beta) = -4-4\beta-4\beta^2$

$e_2 = (\beta-1)u_0(\beta) = (\beta-1)(4\beta-5) = 5+4\beta+4\beta^2 = 1-e_1$ ← (это тоже проверка)

$R = \mathbb{F}_{13}[\beta] = (e_1) \oplus (e_2) = (-4-4\beta-4\beta^2) \oplus (5+4\beta+4\beta^2)$

---

A7) Найдите порядок группы $R^*$ обратимых элементов кольца.

1) $R \simeq \mathbb{F}_3[x]/(x^3)$ – конечное кольцо $\Leftrightarrow$ $[h(x)]$-обратимый элемент $\Leftrightarrow$ $[h(x)]$ не является делителем 0,

$[h(x)]$ – нильп. $\Rightarrow$ делитель нуля.

Пусть $[h(x)] \notin \overline{Rad\ \mathbb{F}_3[x]/(x^3)}$, тогда если $[h(x)][g(x)] = [\bar{0}] \Rightarrow$

$\Rightarrow \begin{cases} h(x)g(x) = x^3 q_1(x) \\ h(x) \neq x\, q_2(x) \end{cases} \Rightarrow g(x) = x^3 q_3(x) \Rightarrow [g(x)] = [\bar{0}] \Rightarrow [h(x)]$ не явл. делителем нуля $\Rightarrow [h(x)]$-обратимый элемент. $\Rightarrow$

$\Rightarrow R^* = R \setminus Rad R$, $|R| = 13^3$, $|Rad\, R| = 13^2 \Rightarrow |R^*| = 13^3 - 13^2$.

2) $R \simeq \frac{\mathbb{F}_{13}[x]}{((x-1)(x^2+x+1))} \simeq \mathbb{F}_{13} \oplus \mathbb{F}_{13^2}$

$(a,b) \in (\mathbb{F}_{13} \oplus \mathbb{F}_{13^2})^* \Leftrightarrow \begin{cases} a \in \mathbb{F}_{13}^* \\ b \in \mathbb{F}_{13^2}^* \end{cases} \Rightarrow$

$|R^*| = |\mathbb{F}_{13}^*||\mathbb{F}_{13^2}^*| = (13-1)\cdot(13^2-1)$

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

B5) Найдите в поле $R$ его простое подполе и степень расширения $R$ над простым подполем. Найдите минимальный многочлен элемента $\beta$.

Решается стандартно.

B6) Какой известной группе изоморфна мультипликативная группа поля $R^*$ ? Найдите порядок элемента $\beta$ в $R^*$.

В следующей лекции будет доказано, что мультипликативная группа поля циклическая.

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

Пример разложения неприводимого многочлена над $\mathbb{F}_p$ на линейные множители рассмотрен в лекции 14. Поле разложения многочлена – это наименьшее по включению поле, над которым многочлен раскладывается на линейные множители. (Будет в следующей лекции).

# Разбор задачи №5 ТР.

(Здесь я рассматриваю поле $\mathbb{F}_5$, а не $\mathbb{F}_3$, как в ТР).

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

$g(x) = x^3-x^2-x-2$

1) Разложите $f(x)$ на неприводимые множители над $\mathbb{F}_3$.

Найдите поле разложения $K$ многочлена $f(x)$.

Подбираем корни $f(x)$ в $\mathbb{F}_5$ и раскладываем

$f(x) = (x-1)(x+1)(x^2+2x-2) = (x-1)(x+1)f_1(x)$.

$f_1(x) = x^2+2x-2$ не имеет корней в $\mathbb{F}_5 \Rightarrow f_1(x)$ - неприводимый многочлен над $\mathbb{F}_5$.

Присоединим к $\mathbb{F}_5$ корень $f_1(x)$ $\alpha$.

Рассмотрим $\mathbb{F}_5[\alpha] \simeq \mathbb{F}_5[x]/(x^2+2x-2) = \mathbb{F}_5[x]/(f_1(x))$,

$\mathbb{F}_5[\alpha] = \{a+b\alpha : \alpha^2+2\alpha-2=0,\ a,b \in \mathbb{F}_5\}$

$\mathbb{F}_5[\alpha]$ содержит оба корня $f_2(x)$ (второй корень $f_2(x)$ равен $\alpha^5 = -2-\alpha$).

Над $\mathbb{F}_5[\alpha]$ $f(x)$ раскладывается на линейные множители $f(x) = (x-1)(x+1)(x-\alpha)(x+2+\alpha)$ и $\mathbb{F}_5[\alpha]$ - наименьшее поле, которое содержит $\alpha \Rightarrow$

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

2) Найдите $dim_{\mathbb{F}_5} K$ и $|K|$.

$dim_{\mathbb{F}_5} K = dim_{\mathbb{F}_5} \mathbb{F}_5[\alpha] = \deg f_2(x) = 2$, $|K| = 5^2$

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

Сначала разложим $g(x)$ на неприводимые множители над $\mathbb{F}_5$ аналогично $f(x)$ в 1). $g(x) = (x-2)(x^2+x+1) = (x-2)g_1(x)$

$g_1(x) = x^2+x+1$ неприводим над $\mathbb{F}_5$. Найдем его корни в $K = \mathbb{F}_5[\alpha]$ подставляя в $g_1(x) = 0$ $x = a+b\alpha$, $\alpha^2 = 2-2\alpha$.

Приравнивая коэффициенты при базисных векторах $1, \alpha$, получаем систему для нахождения $a$ и $b$.

(При этом для решения квадратного уравнения можно использовать обычную формулу, но помнить о том, что мы проводим вычисления в поле $\mathbb{F}_5$).

Находим корни $g_2(x)$ $\gamma_1 = 1-\alpha$, $\gamma_2 = -2+\alpha$.

Т.о., корни $g(x)$ в $K$: $\gamma_1 = 1-\alpha$, $\gamma_2 = -2+\alpha$, $\gamma_3 = 2$, $g(x) = (x-2)(x-1+\alpha)(x+2-\alpha)$

4), 5) сделайте самостоятельно.