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

(2) Решим задачу в общем виде. Докажем, что

$$\mathbb{R}[x]/(x^2+ux+v) \simeq \mathbb{C}, \text{ если } D = u^2-4v<0.$$

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,

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

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

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

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

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

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

1) f – гомоморфизм подстановки;

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

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

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

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

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

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

что 1) φ – гомоморфизм,

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

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

1), 2), 3) $\Longrightarrow$ 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) φ – 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 $\Longrightarrow \mathbb{Z}[x]/(x^2-2) \simeq \mathbb{Z}[\sqrt{2}]$.

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

$3 = \frac{m^2}{n^2} \Longleftrightarrow 3n^2 = m^2 \Rightarrow m = 3k \Rightarrow 3n^2 = 3^2k^2 \Rightarrow n^2 = 3k^2 \Rightarrow n = 3l$

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

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

Докажем, что $\mathbb{Z}[\sqrt{2}] \not\simeq \mathbb{Z}[\sqrt{3}]$ от противного.

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

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

$$\left.\begin{array}{l}\varphi(2) = \varphi(\sqrt{2}\sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = (a+b\sqrt{3})^2 \\ \text{С другой стороны } \varphi(2) = \varphi(1+1) = \varphi(1)+\varphi(1) = 1+1 = 2\end{array}\right\} \Rightarrow$$

$\Rightarrow 2 = (a+b\sqrt{3})^2$, т.е. что $\sqrt{2} \in \mathbb{Z}[\sqrt{3}]$.

Докажем, что это невозможно,

Пусть $2 = a^2 + 2ab\sqrt{3} + 3b^2$

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

если $ab = 0 \Leftrightarrow \left[\begin{array}{l} a=0 \quad 2-3b^2=0 \quad 2=3b^2 \Rightarrow 2 \vdots 3 \text{ ?!} \\ b=0 \quad 2-a^2=0 \quad 2=a^2 \Rightarrow a \vdots 2 \Rightarrow 2 \vdots 4 \text{ ?!}\end{array}\right.$

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

$$\Rightarrow \mathbb{Z}[\sqrt{2}] \not\simeq \mathbb{Z}[\sqrt{3}] \Rightarrow \mathbb{Z}[x]/(x^2-2) \not\simeq \mathbb{Z}[x]/(x^2-3)$$

Аналогично можно доказать, что

$$\mathbb{Q}[x]/(x^2-2) \not\simeq \mathbb{Q}[x]/(x^2-3).$$

Т.Р. Задача 3. Разберем пункты 1)–5).

Пусть A — наименьшее целостное подкольцо поля $\mathbb{R}$, содержащее число $\alpha = \sqrt[s]{d}$ (α – 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 α – корень $f(x)$.

В случае $s=2$ $\left\{\begin{array}{l} A - ЦК \Rightarrow 1 \in A \Rightarrow \mathbb{Z} \subset A \\ \alpha \in A \end{array}\right. \Rightarrow a + b\alpha \in A \quad \forall a, b \in \mathbb{Z} \Rightarrow$

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

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

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

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

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

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 α – 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 $K = \mathbb{Q}[\alpha]$.

$A = \mathbb{Z}[\alpha] \underset{\uparrow}{\subseteq} \mathbb{Q}[\alpha] \underset{\uparrow}{\subseteq} \mathrm{Quot}\,\mathbb{Z}[\alpha] = \mathrm{Quot}\,A = K$

пояснить пояснить

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