Лекция 29 октября (вторая половина)

Теорема Если K - факториально, то $K[x]$ тоже факториально.

Док-во состоит из нескольких шагов

$K \subset Q_K$ ← поле частных целостного кольца K

$\underbrace{Q_K[x]}$ — факториальное кольцо

у любой дроби из $Q_K[x]$ имеется редуцированное представление в виде

$$\frac{a}{b}\cdot f_{red}(x)$$

где $a, b \in K$, НОД$(a,b)=1$

$f_{red}(x) \in K[x]$

содержание $cont(f)=1$.

$f \in K[x]$ $\quad cont(f) :=$ НОД(коэф-тов f)

содержание f

$$h(x) = a_0 + a_1x + a_2x^2 + \dots \in Q_K[x]$$

$$= \frac{p_0}{q_0} + \frac{p_1}{q_1}x + \frac{p_2}{q_2}x^2 + \dots$$

приводим к общему знаменателю и выносим за скобку этот общий знаменатель

$$\frac{1}{q}(A_0 + A_1x + \dots + A_nx^n)$$

$$A_i \in K$$

$$Q_K \ni \frac{\text{НОД}(A_i)}{q} \, f_{red}(x)$$

$$f_{red} \in K[x], \ \mathrm{cont}(f) = 1$$

$$\frac{\text{НОД}(A_i)}{q} = \frac{a}{б} \quad \boxed{\text{НОД}(a,b) = 1}$$

В факториальном кольце НОД есть и определён однозначно с точностью до умножения на обратимые элементы

$$a = p_1 \dots p_m$$

$$b = q_1 \dots q_s$$

?

НОД = общая часть этих разложений

из факториальности любой общий делитель d делит НОД, т.к. любой? неприводимый множитель из разложения d должен входить и в a и в b, а значит в НОД.

Факт: редуцированная запись единственна с точностью до умножения на обратимые константы a, b и fred из K.

$$\boxed{\frac{a}{b} f_{red} = \frac{c}{d} h_{red}}$$

$НОД(a,b)=1$ $\quad$ $НОД(c,d)=1$

$\operatorname{cont} f_{red} = \operatorname{cont} h_{red} = 1$

⇙

$a = s_1 c$

$b = s_2 d$

$f_{red} = s_3 h_{red}$

$s_1, s_2, s_3 \in K$ обратимы.

$$ad \underbrace{f_{red}}_{cont} = bc \underbrace{h_{red}}_{cont}$$

$$ad = bc$$

$$НОД(a,b)=1 \Rightarrow c = sa$$

$$ad = sab$$

$d = sb$

$\frac{c}{d} = \frac{sa}{sb}$ нод$(c,d)=1 \Rightarrow$ s обратим

↓

с точностью до обратимых констант

$f_{red} = h_{red}$

шаг 2 Лемма Гаусса:

неприводимый в $K[x]$ многочлен f содержания $\mathrm{cont}(f)=1$ остаётся неприводимым и в $Q_K[x]$.

Док-во: $f \in K[x]$

пусть в $Q_K[x)$ $f = gh$

$$f = \frac{a}{b} g_{red} \frac{c}{d} h_{red} =$$

$$\boxed{\underline{f} = \frac{p}{q} g_{red} h_{red}}$$

$\frac{p}{q}$ = несократимое представление для $\frac{ac}{bd} \in Q$.

$p, q \in K$ и НОД$(p,q) = 1$.

$$\boxed{\operatorname{cont}(g_{red} \cdot h_{red}) = 1} \quad ⊛$$

если это так, то $1 \cdot f$ и $\underline{\frac{p}{q}\, g_{red}\, h_{red}}$

это 2 редуцированных представления одного и того же многочлена $\Rightarrow$

$$\frac{p}{q} = 1 \qquad f = \underset{K[x]}{g_{red}}\;\underset{K[x]}{h_{red}}$$

⊛ следует из более общего утверждения:

__Лемма__ $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$

$\forall f, g \in K[x]$

__Док-во__: Достаточно проверить, что $\forall$ неприводимого $q \in K$

q делит все к-ты $fg \Leftrightarrow$ q делит все к-ты f или q делит все к-ты g

$\Leftarrow$ очевидно

$$\Rightarrow \quad K[x] \xrightarrow{\rho} \frac{K}{(q)}[x]$$

редукция коэф-тов по модулю q

$$a_0 + a_1 x + \ldots + a_n x^n \longmapsto [a_0]_q + [a_1]_q x + \ldots + [a_n]_q x^n$$

Упр) это гомоморфизм колец.

Упр. 2) $A \xrightarrow{\varphi} B$ гомоморфизм колец

$$A[x] \to B[x]$$

$$a_0 + a_1 x + \ldots + a_n x^n \longmapsto \varphi(a_0) + \varphi(a_1) x + \ldots + \varphi(a_n) x^n$$

это тоже гомоморфизм.

если q делит все к-ты fg

$$0 = \rho(fg) = \underline{\underline{\rho(f)}} \cdot \underline{\underline{\rho(g)}}$$

$\frac{K}{(q)}$ – это кольцо без делителей нуля

т.к. q неприводим, а значит прост

(раз K факториально)

$\Downarrow$

$\frac{K}{(q)}[x]$ тоже без делителей нуля

$\Downarrow$

$\rho(f)$ или $\rho(g)$ нулевой.

Док. во теоремы о том, что

K факториально $\Rightarrow$ $K[x]$ факториально

$f \in K[x]$

в $Q_K[x]$ f имеет единств. разложение на неприводимые.

$$f = \underbrace{cont(f) \cdot f_{red}} = q_1(x)\, q_2(x) \dots q_m(x)$$

$q_i \in Q_K[x]$ и неприводимы.

$$= \frac{a}{b}\, \underbrace{q_{1red}\, q_{2red} \dots q_{m\,red}}_{}.$$

неприводимы в $Q_K[x]$ и лежат в $\underline{\underline{K}}[x]$

$\boxed{cont(f)} = \frac{a}{b} \in K$

$f_{red} = q_{1red} \dots q_{m\,red}$

внутри K (т.к. K факториально)

$cont(f) = p_1 \dots p_m$ где $p_i \in K$ неприв.

$$f = p_1 \dots p_m\, q_{1\,red}(x) \dots q_{m\,red}(x)$$

(∃-ние разл.)

$$f = \underbrace{c_1 \dots c_m}\left(q_1(x) \dots q_m(x)\right) = \underbrace{d_1 \dots d_n}\left(h_1(x) \dots h_m(x)\right)$$

у q_i и h_i должно быть содержание 1

$$q_1(x) \dots q_m(x) = h_1(x) \dots h_m(x)$$

в $\underline{K}[x]$

в $\boxed{Q}[x]$

Продумать!

Как раскладывать на неприводимые множители в $\mathbb{Q}[x]$ и в $\mathbb{Z}[x]$

неприводимость в $\mathbb{Z}[x] \Longrightarrow$ неприв. в $\mathbb{Q}[x]$ (по лемме Гаусса)

① алгоритм Кронекера

$f \in \mathbb{Z}[x]$ выясняем приводим f или нет и если приводим получаем разложение

$\deg f = 2n$ или $2n+1$

$n = \left[\frac{\deg f}{2}\right]$

$f = \boxed{gh}$ в $\mathbb{Z}[x]$

у g или у h — пусть у h — степень $\underline{\underline{\leq}}\, n$

Зафиксируем произвольно $n+1$ чисел

$z_0, z_1, \dots, z_n \in \mathbb{Z}$

вычислим $f(z_0)$ $f(z_1)$ . . . $f(z_n)$.

$\parallel$

$g(z_0)\cdot h(z_0)$ . . . — $g(z_n)h(z_n)$

последовательность значений?

$h(z_0), \dots, h(z_n)$

состоит из целых делителей чисел

$f(z_0), \dots, f(z_n)$

Вычислим все такие последовательности

$d_0, d_1, \dots, d_n \in \mathbb{Z}$

(в которых $d_i \mid f(z_i)$ при каждом i)

$\forall$ набора чисел $d_0, \dots, d_n$ $\exists!$

многочлен h с $\deg h \le n$: $h(z_i) = d_i$

$$\boxed{1 \quad 0 \; \dots \dots \; 0}$$

$$\frac{(x-z_1)\dots(x-z_n)}{(z_0-z_1)\dots(z_0-z_n)}$$

$$0 \; 1 \; 0 \; \dots \dots \; 0$$

$$\boxed{h(x) = \sum_{i=0}^{n} f(z_i) \frac{\prod\limits_{\nu \ne i}(x - z_\nu)}{\prod\limits_{\nu \ne i}(z_i - z_\nu)}}$$

делитель $h \in \mathbb{Z}(x)$ многочлена f если $\exists$

то содержится среди тех многочленов

у которых целые коэфф-ты.

Делим f на все такие мн-ны и либо видим, что f неприводим, либо получаем разложение

Редуцируем к-тов по какому-нибудь модулю.

$$\rho: \mathbb{Z}[x] \longrightarrow \boxed{\frac{\mathbb{Z}}{(m)}[x]}$$

$$a_0 + a_1 x + \dots + a_n x^n \longmapsto [a_0]_m + [a_1]_m x + \dots$$

если $f \in \mathbb{Z}[x]$ приводим в $\mathbb{Z}[x]$

$f = gh$, то $\rho(f) = \rho(g)\rho(h)$

$m = p$ - простое, то $\frac{\mathbb{Z}}{(p)}$ - поле $\mathbb{F}_p$

$\mathbb{F}_p[x]$ - факториальное кольцо.

Критерий Эйзенштейна: Если у $f \in \mathbb{Z}[x]$ старший к-т 1, а все остальные к-ты делятся на p, но при этом свободный член (делясь на p) не делится на p^2, то f неприводим в $\mathbb{Z}[x]$ (и в $\mathbb{Q}[x]$)

Док-во: $f = gh \xrightarrow{\rho} \boxed{\mathbb{F}_p[x]}$

$$\begin{array}{ccc} \rho(f) & = & \rho(g)\,\rho(h) \\ \parallel & & \parallel \quad\ \ \parallel \\ x^n & = & x^k \ \ x^l \end{array}$$

У g и у h все к-ты, кроме старшего, делятся на p $\Rightarrow$ у gh свободный член делится на p^2