2 Неприводимость многочленов. Основная теорема арифметики для многочленов

Опр Пусть P ∈ F[x] и deg P > 0. Многочлен P называется *неприводимым над полем F*, если из условия P = QR, где Q,R ∈ F[x], следует, что deg Q = 0 или deg P = 0.
Иначе, P неприводим над полем F, если deg P > 0 и P не преставим в виде произведения двух многочленов меньших степеней, ∈ F[x]

Утверждение

Пусть P неприводим над полем F. B*C ⋮ P; B,C,F ∈ F[x], тогда B ⋮ P, или C ⋮ P.

▲

Пусть

$$\begin{cases} \text{B} \not\vdots \text{P} \\ \text{C} \not\vdots \text{P} \end{cases}$$

$\Longrightarrow$ НОД(B,D) = 1 $\Longrightarrow \exists\ u_1, v_1 : \text{B}u_1 + \text{P}v_1 = 1\ \exists\ u_2, v_2 : \text{C}u_2 + \text{P}v_2 = 1$
Перемножим:

$\text{BC}u_1u_2 + \text{BP}u_1v_2 + \text{C}u_2v_1\text{P} + v_1v_2P^2 = 1 \Longrightarrow 1 \vdots \text{P}$, но deg P > 0. Противоречие. ■

Теорема 2 (Основная теорема арифметики для многочленов)
Пусть A - ненулевой многочлен из кольца F[x]. Тогда

1. Найдутся $\alpha \in \text{F}^*$ и неприводимые многочлены $P_1...P_n \in$ F[x]: $\text{A} = \alpha P_1 * P_2 * ... * P_n$
2. Если, кроме того,

   $\text{A} = \alpha P_1 * P_2 * ... * P_n = \beta Q_1 * Q_2 * ... * Q_m$, где Q_i и P_i неприводимые многочлены над F, то m = n и $\exists\sigma : \{1, 2, ...n\} -> \{1, 2, ...n\} : P_i \sim Q_{\sigma(i)}$

▲

1. Если A = const, то $\text{A} = \alpha \in \text{F}^*$. Пусть degA > 0. Докажем индукцией по степени A.
База:
Если A неприводим над F, то A = P и все доказано. Если A приводим над F, то A = QR, deg Q, deg R < deg A. $\Longrightarrow$ к Q и R применимо предположение индукции.

2. Индукция по n.

1. Если n = 0, то $\text{A} = \alpha \Longrightarrow$ m = 0
2. Пусть утверждение доказано для многоченов разлагающихся в произведение менее n неприводимых многочленов.
   Пусть $\text{A} = \alpha P_1 * P_2 * ... * P_n = \beta Q_1 * Q_2 * ... * Q_m$, где Q_i и P_i неприводимые многочлены над F
   n >= 1. $Q_1, Q_2, ..., Q_m$ кратны $P_n \Longrightarrow \exists\gamma : Q_j$ кратно $P_n \Longrightarrow Q_j = \gamma * P_n$ (ассоциат)
   $\alpha P_1 * P_2 * ... * P_n = \beta\gamma Q_1 * Q_2 * Q_j\hat{} ... * Q_m * P_n$. ($Q_j\hat{}$ = пропуск этого элемента) $\Longrightarrow$ (делится на P_n)
   $\alpha P_1 * P_2 * ... * P_{n-1} = \beta\gamma Q_1 * Q_2 * Q_j\hat{} ... * Q_m \Longrightarrow$ по предположению индукции n - 1 = m - 1 $\Longrightarrow$ n = m
   По предположению индукции $\exists\sigma : \{1, 2, ...n-1\} -> \{1, 2, ...n-1\} : P_i \sim Q_{\sigma(i)}$
   Положим $\sigma(i) =$ j $\sigma : \{1, 2, ...n\} -> \{1, 2, ...n\}$ - биекция. $P_n \sim Q_{\sigma(n)} = Q_j$

■

Следствие
Пусть A ∈ F[x] и $\text{A} = \alpha {P_1}^{k_1} * {P_2}^{k_2} * ... * {P_n}^{k_n}$, где $P_i \not\sim P_j, i \neq j$, тогда любой делитель многочлена A имеет вид:
$\text{D} = \gamma {P_1}^{m_1} {P_2}^{m_2} ... {P_n}^{m_n}$, где $0 <= m_i <= k_i$

▲

Пусть A кратно D и A = DQ. D и Q содержат в качестве неприводимых многочленов только $P_1, ...P_n$. D = $\gamma {P_1}^{m_1} {P_2}^{m_2} ... {P_n}^{m_n}$ Q = $\gamma' {P_1}^{l_1} {P_2}^{l_2} ... {P_n}^{l_n}$.
DQ = $\alpha {P_1}^{k_1} {P_2}^{k_2} ... {P_n}^{k_n} = \gamma\gamma' {P_1}^{m_1+l_1} {P_2}^{m_2+l_2} ... {P_n}^{m_n+l_n}$, $k_i = l_i + m_i \Longrightarrow 0 <= m_i <= k_i$ ■