№ 1	Кольцо многочленов над полем. Наибольший общий
P. 1	делитель. Алгоритм Евклида. Лин. выражение нод.

Def. Многочлен над $\mathbb{R}$ наз-ся алгебр. выражение вида
$f(x) = a_0 + a_1 x + \ldots + a_n x^n$, где $a_i \in \mathbb{R}$, $a_n \neq 0$, $a_n x_n$ — старший член мн-на

$\deg f = n$

$(f \cdot g) \cdot h = f(g \cdot h)$

$(f+g) \cdot h = f \cdot h + g \cdot h$.

Def. Пусть R — комм. кольцо с 1
многочлен из R наз-ся посл-ть
$(a_0 \ldots a_n \ldots)$
такие, что $\exists N : \forall n > N \hookrightarrow a_n = 0$ — финитные посл-ти

Def. $A(a_i)$ $B(a_i)$
$A + B = C(a_i + b_i)$

Def. $A \cdot B = C$, $C_k = \sum_{i=0}^{k} a_i b_{k-i}$

Def. λA, $\lambda \in \mathbb{R}$
$\lambda A = (\lambda a_i)$

Утв. $R[x]$ — комм.

Д-во.

1. Относ сложения $R[x]$ — лин. пр-во
$0 = (0 \ldots 0 \ldots)$
$A(a_i) \Rightarrow -A(-a_i)$

2. Асс. умн-я
$(AB)C \stackrel{?}{=} A(BC)$
$(A)_k$ — k-й коэф. A

$((AB)C)_k = \sum_{n=0}^{k} (AB)_n C_{k-n} = \sum_{n=0}^{k} \sum_{i=0}^{n} A_i B_{n-i} C_{k-n}$ (1)

$(A(BC))_k = \sum_{n=0}^{k} A_n (BC)_{k-n} = \sum_{n=0}^{k} A_n \sum_{i=0}^{k-n} B_i C_{k-n-i} =$

$= \sum_{n=0}^{k} \sum_{m=0}^{k-n} A_n B_i C_{k-n-i} = \sum_{i+j+e=k} A_i B_j C_e = (1)$

Аналогично

$(A+B)C = AC + BC$

$AB = BA$

$1 = (1 \ldots 0 \ldots)$ ▪

Def. Комм. кольцо наз.-ся обл.-ю целостности или цел. кольцом, если
$\forall a, b \in R: a \neq 0, b \neq 0 \Rightarrow a \cdot b \neq 0$

Def. P – мн $(a_0 \ldots a_n \ldots)$

$\deg P - \max\{n \mid a_n \neq 0\}$

$a_n x^n = (0 \ldots a_n)$ – старший член

$HT(P) = a_n x^n$

Note. Здесь $x = (0, 1, \ldots)$

Note. $\deg(0) = -\infty$

Утв. $\forall P, Q \in R[x]$, R – ком. кольцо с 1

а) $\deg(P+Q) \leq \max(\deg P, \deg Q)$

б) $\deg(PQ) \leq \deg P + \deg Q$

в) Если R – цел. кольцо, то $\deg(PQ) = \deg P + \deg Q$

Д-во.

а) Пусть $\deg P = a$, $\deg Q = b$

Пусть $n > \max(a, b)$

$(P+Q)_n = a_n + b_n = 0 \Rightarrow \deg(P+Q) \leq \max(\deg P, \deg Q)$

б) Пусть $n > a+b$ $\quad (P \cdot Q)_n \overset{?}{=} 0$

$(P \cdot Q)_n = \sum_{i=0}^{n} P_i Q_{n-i} = \underbrace{\sum_{i=0}^{a} P_i Q_{n-i}}_{=0} + \overbrace{\sum_{i=a+1}^{n} P_i Q_{n-i}}^{=0} = 0$

в) $(PQ)_{a+b} = \sum_{i=0}^{a+b} P_i Q_{a+b-i} = \underbrace{\sum_{i=0}^{a-1} P_i Q_{a+b-i}}_{=0} + P_a Q_b + \sum_{i=a+1}^{a+b} P_i Q_{a+b-i} =$

$= P_a Q_b \neq 0$ ▪

Сл-е. Если R – обл. цел., то кольцо мн-в $R[x]$ – обл. цел.

Д-во.

$P \neq 0$, $Q \neq 0$

$\deg P \geq 0$, $\deg Q \geq 0 \rightarrow \deg(P \cdot Q) \geq 0 \rightarrow P \cdot Q \neq 0$ ▪

№1
P 2

Th (св-во унив. кольца многочленов)

Пусть A-кольцо, сод-е R.

Пусть $\forall a \in A, \forall r \in R \ ar = ra$

Тогда $\exists!$ гомоморфизм $\varphi_a : R[x] \to A$:

а) $\varphi_a(x) = a \in A$

б) $\varphi_a(r) = r \ \forall r \in R$

Д-во

а) Д-м единственность φ_a в предположении, что он $\exists$.

φ_a гомоморфизм $\Leftrightarrow$

$\varphi_a(\sum p_i x^i) = \sum_i \varphi_a(p_i)\varphi_a(x)^i = \sum_i p_i a^i \ (*)$

б) Покажем, что опр. таким образом φ_a - гомоморфизм.

$\varphi_a(P+Q) = \varphi_a(\sum (p_i + q_i) x^i) \overset{*}{=} \varphi_a(P) + \varphi_a(Q)$

$\varphi_a(PQ) = \varphi_a(\sum_i P_i Q_{n-i} x^i) = \varphi_a(P)\cdot\varphi_a(Q)$ ⊠

Note Св-во унив. позволяет определить значение мн-на

Def Пусть P-мн-н из $R[x]$ $R \subset A$.

Тогда знач. мн-на P на $a \in A$

наз-ся $P(a) \overset{def}{=} \varphi_a(P)$

Th (о $\exists$ делении с остатком в $F[x]$) (F-поле)

а) Пусть $A, B \in F[x]$, $B \neq 0$. Тогда $\exists$ Q и $R \in F(x)$:

$A = Q \cdot B + R$, где либо $R = 0$, либо $\deg R < \deg B$

б) Мн-ны Q и R опр-ны однозначно

Д-во

а) Инд-я по $\deg A$

База Если $A = 0$, или $\deg A < \deg B$

$\Rightarrow A = 0 \cdot B + A$ все вып.

Шаг Пусть $\deg A \geq \deg B$. Пусть $\deg A = a$, $\deg B = b$

$HT(A) = \alpha x^a, \alpha \neq 0$

$HT(B) = \beta x^b, \beta \neq 0$

Моном M: $HT(A) = M \cdot HT(B)$

$M = \frac{\alpha}{\beta} x^{a-b}$

$A' = A - MB$

При вычитании $MT(A)$ сохр-ся

$\deg A' < \deg A$

$\exists Q', R' \in F[x]: A' = Q'B + R'$, где $R' = 0$ либо $\deg R' < \deg B$

$A = Q' + MB + R' = (Q' + M)B + R' \Rightarrow$

$\Rightarrow$ часть A д-на

б) Пусть $A = Q_1 B + R_1 = Q_2 B + R_2$

$\deg R_1 < \deg B$
$\deg R_2 < \deg B$ $\Rightarrow \deg(R_1 \pm R_2) < \deg B$

$R_1 - R_2 = (Q_2 - Q_1) \cdot B \Rightarrow (R_1 - R_2) = \deg(Q_2 - Q_1) + \deg B \geq B$?! $\blacksquare$

Def Если $\exists Q: A = QB$ (т.е. $R = 0$)

$\Rightarrow A$ делится на B

Def Если $A \vdots B$ и $B \vdots A$, то

A и B наз-ся ассоц. мн-ми

$A \sim B$

Def Пусть $f, g \in F[x]$, причем $f, g \neq 0$.

Мн-н $d \in F[x]$ – НОД(f, g), если

а) $f \vdots d$ и $g \vdots d$

б) Если d' – общ. делитель, то $d \vdots d'$

Th 3 Для $\forall$ двух $f, g \in F[x]: f, g \neq 0$

$\exists d = $ НОД(f, g)

Более того, $\exists u, v \in F[x]: uf + u \cdot g = d$

Д-во

а) Если $f = 0$

Тогда $d = g = 0 \cdot f + 1 \cdot g$

б) 1) $f = q_1 \cdot g + r_1$, где либо $r_1 = 0$ либо $\deg r_1 < \deg g$

2) $g = q_2 \cdot r_1 + r_2$, где либо $r_2 = 0$ либо $\deg r_2 < \deg r_1$

3) $r_1 = q_3 r_2 + r_3$ –//–.

Рано или поздно остаток будет равен 0

$\vdots$

n) $r_{n-2} = q_n r_{n-1} + r_n$, $r_n \neq 0$ – посл-й ненул. ост-к

n+1) $r_{n-1} = q_{n+1} r_n$

№1 P3) Покажем, что $f \vdots r_n$, $g \vdots r_n$

$r_n \mid r_{n-1}$

Из р-ва n) r_n - делитель r_{n-2}

...

r_n - делитель g, f.

Проверим, что если $d' \mid f$, $d' \mid g \Rightarrow d' \mid r_n$

Из $1 \Rightarrow d' \mid r_1 \Rightarrow d' \mid r_2 \ldots \Rightarrow d' \mid r_n \Rightarrow d = \text{НОД}(f, g)$

В) 2-ю часть д-м индукцией по числу шагов в ал-ме Евклида

Из д-го $\text{НОД}(f, g) \overset{1}{=} \text{НОД}(g, r_1) \overset{2}{=} \text{НОД}(r_1, r_2) =$

$\ldots = \text{НОД}(r_{n-1}, r_n) \overset{n}{=} r_n$

<u>База</u>

$n = 1$ $r_{n-1} = q_{n+1} \cdot r_n \Rightarrow r_n = 0 \cdot r_{n-1} + 1 \cdot r_n$

<u>Предп инд-ии</u> (для ал-ма из n-1 шага)

$r_n = d = u_1 g + v_1 \cdot r_1 = | r_1 = f - q_1 g | =$

$= u_1 g + v_1 (f - q_1 g) = v_1 f + (u_1 - v_1 q_1) g$ ☒