Renkaat ja kunnat 15.2.2021

Polynomit. K komm. rengas. K-kertoiminen polynomi: $\sum_{k=0}^{n} a_k X^k$, $a_k \in K$.

Jos $a_n \neq 0$, niin polynomin $P(X) = \sum_{k=0}^{n} a_k X^k$ aste on n, merk. $\deg P(X) = n$

$$\left(\sum_{k=0}^{n} a_k X^k\right) + \left(\sum_{k=0}^{n} b_k X^k\right) = \sum_{k=0}^{n} (a_k + b_k) X^k$$

$$\left(\sum_{k=0}^{n} a_k X^k\right)\left(\sum_{k=0}^{n} b_k X^k\right) = \sum_{k=0}^{2n} \left(\sum_{i+j=k} a_i b_j\right) X^k$$

$K[X]$ on komm. rengas

$0_{K[X]} = 0_K X^0 = 0$

$1_{K[X]} = 1_K X^0 = 1$

$$\begin{aligned}(X^2 + X)(X+3) &= X^3 + 3X^2 \\ &\quad + X^2 + 3X \\ \hline &X^3 + 3X^2 + 3X\end{aligned}$$

renkaassa $\mathbb{Z}[X]$.

$\deg 0_{K[X]} = -\infty$

$-\infty < a \quad \forall a \in \mathbb{Z}$

$(-\infty) + (-\infty) = -\infty$

$(-\infty) + a = -\infty \quad \forall a \in \mathbb{Z}$.

Esim. $(3X^2+1)^2 = 9X^4+6X^2+1 = 2X^4+6X^2+1$
$\in (\mathbb{Z}/7\mathbb{Z})[X]$ ks. s. 6
$= 2X^4 - X + 1$

$9 \equiv 2 \mod 7$ $\quad 9+7\mathbb{Z} = 2+7\mathbb{Z}$.

$-1 \equiv 6 \mod 7$

$(3+7\mathbb{Z})X + (1+7\mathbb{Z})$

Helposti nähdään: $\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X)$ (*)

erisuuruus mahd., jos K:ssa on nollan jakajia

Erityisesti, jos K on kunta

Esim. $2X \in (\mathbb{Z}/4\mathbb{Z})[X]$

$(2X)^2 = 4X^2 = 0$

$4 \equiv 0 \mod 4$

Prop. 6.8. Jos K on kokonaisalue, niin kaikille $P(X), Q(X) \in K[X]$ pätee

$\deg(P(X)Q(X)) = \deg P(X) + \deg Q(X)$.

Tod. $P(X) = \sum_{k=0}^{m} a_k X^k$, $Q(X) = \sum_{k=0}^{n} b_k X^k$ s.e. $a_m \neq 0$, $b_n \neq 0$. $P(X)Q(X) = \underbrace{a_m b_n}_{\neq 0} X^{m+n} + \ldots$

2

Huom. $0_{K[x]} P(x) = 0_{K[x]}$

$$\deg(\underbrace{0_{K[x]}}_{-\infty} \underbrace{P(x)}_{\deg P(x)}) = \deg(0_{K[x]}) = -\infty$$

$$\geq -\infty + \deg P(x)$$

(*) pätee myös, kun kerrotaan 0-polynomilla.

Prop. 6.10 Olk. K kunta. $P(x) \in K[x]^{\times} \iff \deg P(x) = 0$.

Tod. Olk. $P(x) \in K[x]$ s.e. $\deg P(x) = 0$. Tällöin $P(x) = aX^0$, $a \in K^{\times}$.

Huomaa: $(aX^0)(a^{-1}X^0) = (aa^{-1})X^0 = 1_K X^0 = 1_{K[x]}$. Siis $P(x) \in K[x]^{\times}$.

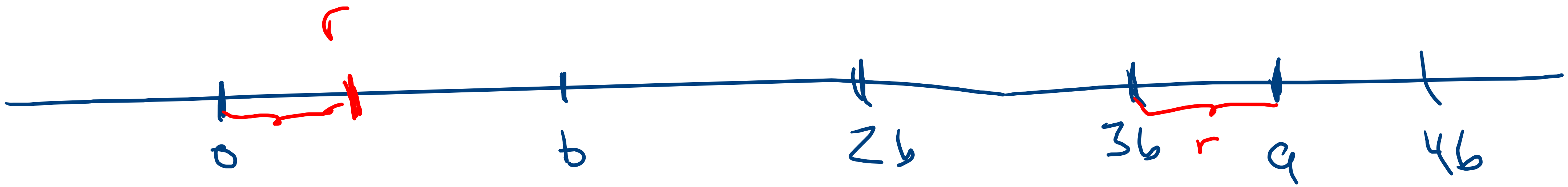
Olk. $Q(x) \in K[x] - \{0\}$.

$$\boxed{\deg(P(x)Q(x)) = \deg P(x) + \underbrace{\deg Q(x)}_{\geq 0} \geq \deg P(x)}$$

Jos $P(x)Q(x) = 1_{K[x]}$, niin

$P(x) \leq \deg(P(x)Q(x)) = \deg 1_{K[x]} = 0 \Rightarrow \deg P(x) = 0$ $\square$

Jakoyhtälö: Jos $a \in \mathbb{N}$, $b \in \mathbb{N} - \{0\}$. (**liite P.A.1**)



$a = 3b + r$

$$\exists \begin{cases} 0 \le r < b \\ q \in \mathbb{N} \end{cases} \text{ s.e. } \underline{a = qb + r}$$

Lause 6.11 (Jakoyhtälö) Olk. K $\begin{cases} \text{kunta} \\ \text{komm. rengas}, \#K \geq 2. \end{cases}$ Olk. $A(x), B(x) \in K[X]$, $B(x) \neq 0$. (Ol. että $B(x)$:n kork. asteen termin kerroin on yksikkö.)
Tällöin $\exists$ 1-käs. polynomit $Q(X)$, $J(X) \in K[X]$ s.e.

$$A(x) = Q(X)B(x) + J(x) \quad \text{ja} \quad \deg J(x) < \deg B(x).$$

Tod. Os. ensin, että polynomit $Q(X)$ ja $J(x)$ on. Jos $A(x) = Q(x)B(x)$ jollain $Q(x) \in K[X]$, niin OK. (val. $J(x) = 0$, $\deg J(x) = -\infty < \underbrace{\deg B(x)}_{\geq 0}$)

"jako menee tasan."

Ol. että jako ei mene tasan.

$$S = \{ A(x) - D(x)B(x) : D(x) \in K[x] \} \neq \emptyset$$

Huom $0 \notin S$. $\Rightarrow$ $\deg S = \{ \underbrace{\deg P(x)}_{\in \mathbb{N}} : P(x) \in S \} \subset \mathbb{N}$

$\deg S$ on $\mathbb{N}$:n epätyhjä osajoukko, joten sillä on pienin alkio $m \in S$. (induktioperiaate!)

Olk. $Q(x) \in K[X]$ s.e. $\deg (A(x) - Q(x)B(x)) = m$

$$J(x) = A(x) - Q(x)B(x) = a_m X^m + \dots + a_0, \quad a_m \neq 0.$$

$$\rightsquigarrow \quad A(x) = Q(x)\underbrace{B(x)} + J(x) \quad \text{OK}$$

$$= \underbrace{b_d}_{\in K^\times} X^d + b_{d-1} X^{d-1} + \dots + b_0$$

Väite: $m < d$.

Jos olisi $m \geq d$, niin $J(x) - a_m b_d^{-1} X^{\overbrace{m-d}^{\geq 0}} B(x) = \underbrace{A(x) - (Q(x) - a_m b_d^{-1} X^{m-d})B(x)}_{\in S}$

ja $\deg(J(x) - a_m b_d^{-1} X^{m-d} B(x)) < \deg J(x)$. $\lightning$.

(5) Siis polynomit $Q(x)$, $J(x)$ on.

Os. yksikäsitteisyys: olk. $\tilde{Q}(x), \tilde{J}(x) \in K[X]$ s.e.

$$A(x) = \boxed{\tilde{Q}(x)B(x) + \tilde{J}(x)} \quad \text{ja} \quad \deg \tilde{J}(x) < \deg B(x).$$

$$\boxed{= Q(x)B(x) + J(x)}$$

$$\Rightarrow \left(Q(x) - \tilde{Q}(x)\right)B(x) = \tilde{J}(x) - J(x)$$

Jos $Q(x) \neq \tilde{Q}(x)$, niin $\deg\left[\underbrace{\left(Q(x) - \tilde{Q}(x)\right)}_{\geq 0}\underbrace{B(x)}_{=d}\right] \geq d$.

mutta $\deg\left(\tilde{J}(x) - J(x)\right) \leq m < d$. $\lightning$ $\Rightarrow Q(x) = \tilde{Q}(x)$.

$\tilde{J}(x) = J(x)$. $\square$

Esim. $A(x) = X^2 + 2X + 2$
$B(x) = X + 1$ $\Big\} \in \mathbb{Z}[X]$

$$A(x) = \underset{Q(x)}{(X+1)}\underbrace{(X+1)}_{B(x)} + \underbrace{1}_{\in J(x)}$$

$$\deg B(x) = 1 > 0 = \deg 1$$

$$\begin{array}{r|l} & \overbrace{X + 1}^{Q(x)} \\ \hline X+1 & X^2 + 2X + 2 \\ & \mp X^2 \mp X \\ \hline & X + 2 \\ & \mp X \mp 1 \\ \hline & 1 = J(x) \end{array}$$

6

Prop. 6.16 Olk. K komm. rengas, $\#K \geq 2$. $P(X) \in K[X]$, $c \in K$.

$$\underbrace{c \text{ on } P(X)\text{:n juuri}}_{P(c)=0} \iff (X-c) \mid P(X).$$