Renkaat ja kunnat 16.2.2021

Lause 6.11 (Jakoyhtälö). *Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Olkoot $A(X)$, $B(X) \in K[X]$ siten, että $B(X) \neq 0$ ja polynomin $B(X)$ korkeimman asteen termin kerroin on yksikkö. Tällöin on yksikäsitteiset polynomit $Q(X), J(X) \in K[X]$, joille pätee*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$.

$Fun : P[x] \to \mathcal{F}(K,K)$

$Fun(P(x)) = P$

$c \in K$ on polynomin $P(X)$ **juuri**, jos $P(c) = 0$

polynomin $P(x)$ määräämä polynomifunktio $P: K \to K$.

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

c on $P(x)$:n 'juuri' $\Leftrightarrow (X-c) \mid P(X)$ ($\Leftarrow$) $\exists\, Q(X) \in K[X]$ s.e. $P(X) = (X-c)Q(X)$

Tod. "$\Leftarrow$" Jos $P(X) = (X-c)Q(X)$, niin $P(c) = \underbrace{(c-c)}_{=0} Q(c) = 0$.

"$\Rightarrow$" Ol. $P(c) = 0$. Jakoyhtälö $\Rightarrow$ $P(X) = (X-c)Q(X) + bX^0$ jollain $Q(x) \in K[X]$, $b \in K$. $\Rightarrow$ $0 = P(c) = \underbrace{(c-c)}_{=0} Q(c) + b = b \Rightarrow P(X) = (X-c)Q(X)$ □

①

Seuraus 6.17 Olk. K kunta, $P(X) \in K[X]$, $\deg P(X) \in \{2,3\}$. Tällöin

$P(X)$ on jaoton $\Leftrightarrow$ $P(X)$:llä ei ole juurta.

Tod. Hain.

Esim. 1) $P(X) = X^2+1 \in \mathbb{R}[X]$ on jaoton, sillä $c^2+1 \geq 1 > 0 \ \forall c \in \mathbb{R}$.

$P(X) = X^2+1 \in \mathbb{C}[X]$ ei ole jaoton, sillä $X^2+1 = (X-i)(X+i)$.

2) $(X^2+1)^2 \in \mathbb{R}[X]$ ei ole jaoton mutta sillä ei ole juuria.

$\vee$

$(X^2+1)(X^2+1)$

Prop. 6.23. Jos K on äärellinen kokonaisalue, niin $\mathrm{Fun}: K[X] \to \mathcal{F}(K,K)$ on injektio.

Lause 6.20. Jos K on kokonaisalue, niin polynomilla $P(x) \in K[x]$ on korkeintaan $\deg P(x)$ juurta.

Tod. Jos $c_1, \dots, c_k$ ovat $P(x)$:n juuria, niin $(x-c_1), \dots, (x-c_k)$ jakavat $P(x)$:n $\Rightarrow$ $\underbrace{(x-c_1)\cdot\dots\cdot(x-c_k)}_{\deg = k} \mid P(x)$

$\Rightarrow k \leq \deg P(x)$. $\square$ ei ole kokonaisalue

Esim. Polynomilla $x^2 \in (\mathbb{Z}/16\mathbb{Z})[x]$ on 4 juurta:

0, 4, 8 ja 12.

Prop. 6.23:n tod. Prop. 3.21: Fun on injektio $\Leftrightarrow \ker(\mathrm{Fun}) = \{0\}$.

Jos $\mathrm{Fun}(P(x)) = 0$, niin $P(c) = 0 \ \forall c \in K$ $\Rightarrow$ $P(x)$:llä on ääretön monta juurta. $\Rightarrow P(x) = 0$. $\Rightarrow \ker(\mathrm{Fun}) = \{0\}$. $\square$

Lause 6.26 (Algebran peruslause) Jokaisella polynomilla $P(X) \in \mathbb{C}[X]$, $\deg P(X) \geq 1$, on juuri.

Tod. ks $\mathbb{C}$-analyysi 1.

$\rightsquigarrow$ $\mathbb{C}$ on algebraallisesti suljettu.

7. Ideaalit ja kuntalaajennukset

vakaa osajoukko, joka on ryhmä indusoidulla laskutoimituksella.

Prop. 7.2. Olk. $\varphi : R \to R'$. Tällöin $\ker\varphi$ on $(R,+)$ aliryhmä.

Lisäksi, jos $r \in R$ ja $a \in \ker\varphi$, niin $ra \in \ker\varphi$. (ar)

$\rightsquigarrow$ Määr. Renkaan R osajoukko $J \subset R$, $J \neq \emptyset$, on ideaali, jos
$(J,+)$ on $(R,+)$:n aliryhmä ja
kaikille $r \in R$ ja kaikille $a \in J$ pätee $ra \in J$. (ar)

Tod. Olk. $x, y \in \ker\varphi$. Tällöin $\varphi(x+y) \overset{\varphi \text{ homom.}}{=} \varphi(x) + \varphi(y) = 0 + 0 = 0$, joten $x+y \in \ker\varphi$. Siis $\ker\varphi \subset (R,+)$ on vakaa.

L. 3.18: $\varphi(0_R) = 0_{R'} \Rightarrow 0_R \in \ker\varphi$.

Prop. 3.5(2): $\varphi(-x) = -\underbrace{\varphi(x)}_{=0} = 0 \quad \forall x \in \ker\varphi \Rightarrow -x \in \ker\varphi \ \forall x \in \ker\varphi$

$\Rightarrow (\ker\varphi, +)$ on ryhmä. $\rightsquigarrow (R,+)$:n aliryhmä.

Olk. $r \in R$, $a \in \ker\varphi$. Tällöin $\varphi(ra) \overset{\varphi \text{ homom.}}{=} \varphi(r)\underbrace{\varphi(a)}_{=0} = 0 \Rightarrow ra \in \ker\varphi$

$\varphi(ar) = \underbrace{\varphi(a)}_{=0}\varphi(r) = 0 \rightarrow ar \in \ker\varphi$. □

$\rightarrow$ Rengashomomorfismin ydin on ideaali.

Lemma 7.3 Jos $J \subset R$ on ideaali, niin $0_R \in J$.

Tod. 0_R on +:n n.a. R:ssä $\rightsquigarrow$ J:ssä } Jos 0_J on +:n n.a. J:ssä, niin $\forall a \in J$ pätee $a + 0_R = a + 0_J \overset{\text{supista}}{\Rightarrow} 0_R = 0_J$. □

Esim. $\{0\}$ ja R ovat R:n ideaaleja.

Prop. 7.6. Jos J on $\mathbb{Z}$:n ideaali, niin $J = a\mathbb{Z} = \{ka : k \in \mathbb{Z}\}$ jollain $a \in \mathbb{Z}$.

Tod. Jos $a \in \mathbb{Z}$, niin $a\mathbb{Z}$ on ideaali: Jos $k, l \in \mathbb{Z}$, niin

$\underbrace{ka}_{\in a\mathbb{Z}} + la = \underbrace{(k+l)a}_{a\mathbb{Z}}$ $\Rightarrow$ $a\mathbb{Z}$ on vakaa, $0 = 0a \in a\mathbb{Z}$, $\underbrace{ka}_{\in a\mathbb{Z}} + \underbrace{(-k)a}_{a \in \mathbb{Z}} = 0$.

Jos $r \in \mathbb{Z}$, $ak \in a\mathbb{Z}$, niin $r(ak) = (rk)a \in a\mathbb{Z}$.

Olk. $J \subset \mathbb{Z}$ ideaali. Jos $J = \{0\}$, niin $J = 0\mathbb{Z}$. OK.

Jos $J \neq \{0\}$, niin on $b \in J - \{0\} \Rightarrow -b \in J \Rightarrow J \cap (\mathbb{N} - \{0\}) \neq \emptyset$.

Olk. $a = \min(J \cap (\mathbb{N} - \{0\}))$. Os. että $J = a\mathbb{Z}$.

$a \in J$, J on ryhmä $\Rightarrow ka \in J \ \forall k \in \mathbb{Z} \Rightarrow a\mathbb{Z} \subset J$.

⑥ Ol. $b \in J - a\mathbb{Z}$. Kokonaislukujen jakoyhtälö: $\exists\, k \in \mathbb{Z}$, $0 < r < a$: $b = ka + r$
$\Rightarrow r \in J$ ja $0 < r < a$, ristiriita. Siis $J \subset a\mathbb{Z}$. ∎

Prop. 7.7 (Ideaalitesti) R rengas, $A \subset R$, $A \neq \emptyset$. A on ideaali, jos ja vain jos

1) $a - b \in A \quad \forall\, a, b \in A$.

2) $ra, ar \in A \quad \forall\, r \in R \;\forall\, a \in A$

Tod. Harj.

Lemma 7.8 Jos $J \subset R$ on ideaali ja $J \cap R^\times \neq \emptyset$, niin $J = R$.

Tod. Olk. $u \in J \cap R^\times \Rightarrow$ $1 = u u^{-1} \in J$ ($u \in J$, $u^{-1} \in R$). Olk. $r \in R$, $1 \in J$ $\Rightarrow r = r \cdot 1 \in J$. $\square$

Prop. 7.9. Jos $J \subset R$ on alirengas, niin $J = R$.

Tod. alirengas sisältää alkion $1_R \overset{L.7.8}{\Rightarrow}$ väite.

Prop. 7.10. Kunnan K ideaalit ovat $\{0\}$, K.

Tod. Jos $k \in K - \{0\}$, niin $k \in K^\times$.

Prop. 7.12. Olk. $\varphi: R \to S$ rengashomomorfismi.

1) Jos $J \subset R$ on ideaali, niin $\varphi(J)$ on $\varphi(R)$:n ideaali.

2) Jos $J \subset S$ on ideaali, niin $\varphi^{-1}(J)$ on R:n ideaali.

Tod. $\varphi(0_R) = 0_S \in J \Rightarrow 0_R \in \varphi^{-1}(J) \Rightarrow \varphi^{-1}(J) \neq \emptyset$.

Olk. $a, b \in \varphi^{-1}(J)$ $\quad \varphi(a-b) = \underbrace{\varphi(a)}_{\in J} - \underbrace{\varphi(b)}_{\in J} \in J \Rightarrow a-b \in \varphi^{-1}(J)$.

Olk. $r \in R$. $\quad \varphi(ra) = \underbrace{\varphi(r)}_{\in S}\underbrace{\varphi(a)}_{\in J} \in J$

$$\varphi(ar) = \varphi(a)\,\varphi(r) \in J$$

Ideaalitesti: $\varphi^{-1}(J)$ on ideaali. $\square$