Renkaat ja kunnat 23.2.2021

L. 7.26 Jos K on kunta, $P(x) \in K[x]$, $\#K = q$. Tällöin $\#\left(K[x]/(P(x))\right) = q^{\deg P(x)}$

Tod. idea: Jakoyhtälö: $Q(x) \in K[x]$

$$Q(x) = S(x)P(x) + \bar{Q}(x)$$

joillain $S(x), \bar{Q}(x) \in K[x]$, $\deg \bar{Q}(x) < \deg P(x)$

$$Q(x) - \bar{Q}(x) = S(x)P(x) \in (P(x))$$

$\Rightarrow$ $\bar{Q}(x)$ edustaa samaa luokkaa kuin $Q(x)$: $\bar{Q}(x) + (P(x)) = Q(x) + (P(x))$

$\Rightarrow \#\left(K[x]/(P(x))\right) \leq q^{\deg P(x)}$

Jos $\deg A(x), \deg B(x) < \deg P(x) \Rightarrow \deg\left(A(x) - B(x)\right) < \deg P(x)$

$\Rightarrow$ jos $A(x) - B(x) \in (P(x))$, niin $A(x) - B(x) = 0$. $\Rightarrow \#\left(K[x]/(P(x))\right) \geq q^{\deg P(x)}$.

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

	0	1	X	$X+1$
0				
1		1		
X			$x+1$	1
$X+1$			1	

Osoittautuu, että

$k = (\mathbb{Z}/2\mathbb{Z})[X]/(P(X))$

on kunta.

Syy selviää pian!

② (Voi tarkastaa myös käsipelillä: Luvun 7.3 tulokset $\Rightarrow$ k on kommut. rengas.
Laskutaulu: Jokaisella $a \in k-\{0\}$ $\exists\, a^{-1}$.

$$X^2+(P(X)) = \_\_\_ +(P(X)).$$

$$\begin{array}{r|l} X^2+X+1 & X^2 \\ \cline{2-2} \mp X^2 \mp X \mp 1 & 1 \\ \cline{1-1} x+1 & \end{array}$$

$$\rightsquigarrow X^2 = \underbrace{(X^2+x+1)}_{\in (P(X))} + x+1$$

$$\Rightarrow X^2-(x+1) \in P(X)$$

$$\Rightarrow X^2+(P(X)) = (x+1)+(P(X))$$

Tavoite: Seuraus 7.32: K kunta, $p(x) \in K[x]$ jaoton $\Rightarrow$ $K[x]/(p(x))$ on kunta.

$\rightsquigarrow$ Lause 7.34 Jos $q \geq 1$ ja p on alkuluku, niin on kunta, jossa on p^q alkiota. Jos k on ääretön kunta, niin $\#k = p^q$ jollain $q \geq 1$ ja p alkuluku.

Tod. Ei todisteta kokonaan....

$\rightsquigarrow$ sovelluksia salakirj, koodaus, lukuteoria, kombinatoriikka,...

Määr. R rengas. Ideaali $J \subset R$ on aito ideaali, jos $J \neq R$.

Jos $M \subset R$ on aito ideaali, joka ei ole minkään aidon ideaalin aito osajoukko, niin M on maksimaalinen ideaali.

Jos $W \subset R$ on aito ideaali ja $M \subset W$, niin $M = W$.

Prop. 7.28 $\mathbb{Z}$:n ideaali $q\mathbb{Z}$ on maksimaalinen $\Leftrightarrow$ q on alkuluku.

Tod. Jos q ei ole alkuluku, niin $q = ab$, $a, b \geq 2$.

Tällöin $a \mid q \Rightarrow q \in a\mathbb{Z}$, $a\mathbb{Z}$ aito ideaali.

$a \notin q\mathbb{Z}$

$\Rightarrow q\mathbb{Z} \subsetneq a\mathbb{Z}$ $\Rightarrow$ $q\mathbb{Z}$ ei ole maksimaalinen.

($a\mathbb{Z}$: aito ideaali)

ai to osajoukko.

$A \subsetneq B$ tarkoittaa $A \subset B$ ja $A \neq B$

Jos q on alkuluku ja $r\mathbb{Z}$ on ideaali, jolle pätee $q\mathbb{Z} \subsetneq r\mathbb{Z}$, $\Rightarrow r \neq q$

niin $q \in r\mathbb{Z} \Rightarrow r \mid q \Rightarrow r = 1 \Rightarrow r\mathbb{Z} = \mathbb{Z}$.

(q alkuluku)

Siis $q\mathbb{Z}$ on maksimaalinen.

L. 5.19: $\mathbb{Z}/q\mathbb{Z}$ on kunta $\Leftrightarrow$ q on alkuluku $\Leftrightarrow$ $q\mathbb{Z}$ on maks.

Lause 7.29 Olk. K komm. rengas, $M \subset K$ maksimaalinen ideaali.

Tällöin K/M on kunta.

Tod. Prop. 7.21 $\Rightarrow K/M$ on komm. rengas.

(P. 7.19, P. 1.10)

M on aito ideaali $\Rightarrow \#(K/M) \geq 2$.

Kysymys $6X^2+3X+1 \in (\mathbb{Z}/7\mathbb{Z})[X]$

oikeasti tämä on $(6+7\mathbb{Z})X^2+(3+7\mathbb{Z})X+(1+7\mathbb{Z})$

Olk. $a+M \in K/M - \{0\}$. Harj: $N = \{ak+m : k \in K, m \in M\}$ on ideaali.

$a \notin M$
$a \in N$
$M \subset N$

$\Rightarrow M \subsetneq N \Rightarrow N = K$ (M maks, N ideaali)

$\Rightarrow 1_K \in N$

$\Rightarrow \exists k \in K, m \in M : 1_K = ak+m$

$1 = ak + m. \iff ak = 1 - m$

$(a+M)(k+M) = ak + M = (1-m) + M = 1 + M = 1_{K/M}$

Siis $(a+M)^{-1} = k + M.$ □

Seurauksen 7.32 todistuksesta puuttuu enää:

Seuraus 7.31 Jos K on kunta ja $P(x) \in K[x]$ on jaoton, niin $(P(x))$ on maksimaalinen.

S. 7.31 seuraa tästä:

L. 7.16 ⟹ pääid. alue

Lause 7.30 Olk. $\mathcal{K}$ pääideaali alue, $a \in \mathcal{K} - \{0\}$. Tällöin (a) on maksimaalinen $\iff$ a on jaoton.

Tod. Olk. $a \in \mathcal{K}$ jaoton. Olk. $b \in \mathcal{K}$ s.e. $(a) \subset (b) \Rightarrow a = qb$ jollain $q \in \mathcal{K}$.

a on jaoton $\Rightarrow$ $q \in \mathbb{K}^\times$ tai $b \in \mathbb{K}^\times$.

Jos $b \in \mathbb{K}^\times$, niin $(b) = \mathbb{K}$

Jos $q \in \mathbb{K}^\times$, niin $(b) = (qb) = (a)$.

(↑ pieni harj.)

} Siis (a) on maksimaalinen.

Toinen suunta Harj.

Saatiin siis: K kunta, $p(x) \in K[x]$ jaoton $\Rightarrow$ $K[x]/(p(x))$ on kunta

---

Muista: Jos φ on rengashomom, niin $\ker \varphi$ on ideaali.

Prop. 7.20 Jokainen ideaali on jonkin rengashomomorfismin ydin.

Tod. $J \subset R$ ideaali. $\pi : R \to R/J$ rengashomom: $\pi(r) = r + J$.

Jos $j \in J$, niin $\pi(j) = j + J = 0 + J \Rightarrow j \in \ker \pi$.

$r \notin J$, niin $\pi(r) = r + J \neq 0 + J$ koska $r - 0 = r \notin J$. □

Lause 7.22 (Renkaiden isomorfismilause) Jos $\psi : R \to S$ on rengashomom, niin $R/\ker\psi$ on isomorfinen renkaan $\psi(R)$ kanssa.

Tod. $\Phi : R/\ker\psi \longrightarrow \psi(R)$

$$\Phi(r + \ker\psi) = \psi(r).$$

ψ homom

Φ on bijektivinen homomorfismi. ↓

$$\Phi(x+\ker\psi)\,\Phi(y+\ker\psi) = \psi(x)\,\psi(y) = \psi(xy)$$

$$= \Phi(xy+\ker\psi) = \Phi((x+\ker\psi)(y+\ker\psi))$$

muut homom. ominaisuudet tarkistamaan tapaan.

Φ on surjektio: $\psi(r) = \Phi(r+\ker\psi)$. $\forall\, r \in R$. (OK).

injektio: olk. $r+\ker\psi \in \ker\Phi \Rightarrow \psi(r) = 0 \Rightarrow r \in \ker\psi$

$$\Rightarrow r + \ker\psi = 0 + \ker\psi = 0_{R/\ker\psi}. \qquad \square$$

Seuraus 7.24. Jos K on kunta ja $\chi(K) = p$, niin K:lla on alikunta, joka on isom. $\mathbb{Z}/p\mathbb{Z}$ kanssa.

Tod. $\varphi : \mathbb{Z} \to K$ se ainoa rengashomom.

Kar. määr. $\Rightarrow \ker \varphi = p\mathbb{Z}$

Isom. lause: $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$

$K \supseteq \varphi(\mathbb{Z})$ on isomorfinen $\square$

$\rightsquigarrow$ Jokaisen äär. kunnan K alkioiden lkm on p^d jollain p alkuluku, $d \geq 1$. (K on $(\mathbb{Z}/p\mathbb{Z})$-vektoriavaruus $\longrightarrow$ ks. luku 4.5)