Renkaat ja Kunnat 22.2.2021

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

1) $(J,+)$ on $(R,+)$:n aliryhmä. (J on vakaa ja $\forall\ a \in J$ myös $-a \in J$)
2) jos $r \in R$ ja $a \in J$, niin $ra,\ ar \in J$

Esim. 1) $q \in \mathbb{N} \rightsquigarrow q\mathbb{Z}$ on $\mathbb{Z}$:n ideaali.
Prop. 7.6: jos $J \subset \mathbb{Z}$ on ideaali, niin $J = q\mathbb{Z}$ jollain $q \in \mathbb{N}$.

2) Jos K on komm. rengas ja $a \in K$, niin

$$(a) = aK = Ka = \{ ka : k \in K \}$$

on ideaali (seuraa Harj. 7.6:sta), alkion a virittämä pääideaali.

Määr. Jos K on komm. rengas, jonka kaikki ideaalit ovat pääideaaleja, niin K on pääideaalialue.

Esim.
- $\mathbb{Z}$ on pääideaalialue
- Jos k on kunta ja J on k:n ideaali, niin (Prop. 7.10) $J = k = 1k$ tai $J = \{0\} = 0k$

Kunta on pääideaalialue

Lause 7.16 Jos K on kunta, niin $K[x]$ on pääideaalialue.

Tod. Olk. J $K[x]$:in ideaali. Jos $J = \{0\}$, niin $J = 0\,K[x] = (0)$, OK.

Ol. että $J \neq \{0\}$. Olk. $B(x) \in J - \{0\}$ s.e. $\deg B(x) = \min\{\deg C(x) : C(x) \in K[x] - \{0\}\}$

Ideaalin määr $\Rightarrow$ $(B(x)) = B(x)\,K[x] \subset J$.

Os. että $J \subset (B(x))$. Olk. $A(x) \in J$. Jakoyhtälö: $\exists\, Q(x), R(x) \in K[x]$

s.e. $A(x) = Q(x)B(x) + R(x)$ ja $\deg R(x) < \deg B(x)$.

$$\Leftrightarrow R(x) = \underbrace{\underbrace{A(x)}_{\in J} - \underbrace{Q(x)\underbrace{B(x)}_{\in J}}_{\in J}} \in J. \quad \Rightarrow \quad R(x) = 0$$

$$\Rightarrow A(x) = Q(x)B(x) \in (B(x)).$$ Siis $J \subset (B(x))$. $\square$

Esim. 7.17: $\mathbb{Z}[x]$:in ideaali $(2, x) = \{2K_1(x) + xK_2(x) : K_1(x), K_2(x) \in \mathbb{Z}[x]\}$ ei ole pääideaali.

(2)

Tekijärenkaat.

Esim. $q\mathbb{Z}$ on $\mathbb{Z}$:n ideaali $\leadsto$ $\mathbb{Z}/q\mathbb{Z} = \{\underline{\underline{a+q\mathbb{Z}}} : a \in \mathbb{Z}\}$

laskutoimitukset $(a+q\mathbb{Z})+(b+q\mathbb{Z}) = (a+b)+q\mathbb{Z}$

$$(a+q\mathbb{Z})(b+q\mathbb{Z}) = ab + q\mathbb{Z}.$$

(tarkastettiin, että jos $a \equiv a'$ ja $b \equiv b' \mod q$, niin $\Leftrightarrow a-a' \in q\mathbb{Z}$

$$\left.\begin{array}{l} a+b \equiv a'+b' \mod q \\ ab \equiv a'b' \mod q \end{array}\right\} \leadsto \text{laskutoimitukset hyvin määriteltyjä.}$$

Määr. Olk. R rengas, $J \subset R$ ideaali. relaatio $x \sim y \Leftrightarrow x-y \in J$.

$\sim$ on ekvivalenssirelaatio:

$$\left.\begin{array}{l} x \sim x \quad \forall\, x \in J \\ x \sim y \Rightarrow y \sim x \quad \forall\, x,y \in J \\ (x \sim y \text{ ja } y \sim z) \Rightarrow x \sim z \quad \forall\, x,y,z \in J \end{array}\right\} \text{Harj.}$$

(3) Lemma 2.4: kongruenssi mod q on ekvivalenssirelaatio.

Huom. Renkaassa $\mathbb{Z}$ pätee: jos $a+q\mathbb{Z} \cap a'+q\mathbb{Z}$, niin $a+q\mathbb{Z} = a'+q\mathbb{Z}$.

Olk. R rengas, $J \subset R$ ideaali

$a+J = \{a+j : j \in J\}$ a:n ekvivalenssiluokka.

Huom $a' \in a+J \iff a' = a+j$
$\iff a'-a = j \in J$.
$\iff a' \sim a$

Jos $(a+J) \cap (b+J) \neq \emptyset$, niin $a+J = b+J$:

Ol $\exists\, x \in (a+J) \cap (b+J)$. Tällöin $x \sim a$ ja $x \sim b$ $\iff b \sim x$ $\Rightarrow b \sim a \Rightarrow b \in a+J$

Jos $y \in b+J$, niin $y \sim b \Rightarrow y \sim a \Rightarrow y \in a+J \Rightarrow b+J \subset a+J$. Vast. os. $a+J \subset b+J$.

$\rightsquigarrow R/J = \{r+J : r \in R\}$ tekijäjoukko.

Prop. 7.18. R rengas, J ideaali. R:n laskutoimitukset ovat yhteensopivia J:n määräämän ekv. relaation kanssa: Jos $a \sim a'$ ja $b \sim b'$, niin

$a+J = a'+J$ $\quad$ $b+J = b'+J$

$a+b \sim a'+b'$ $\quad (a+b)+J = (a'+b')+J$

ja $ab \sim a'b'$ $\quad ab+J = a'b'+J$

Prop. 7.18 $\rightsquigarrow$ laskutoimitukset joukkoon R/J:

$$(a+J)+(b+J) = (a+b)+J$$
$$(a+J)(b+J) = ab+J.$$

$a-a' \in J \quad b-b' \in J.$

$\Updownarrow \quad \Updownarrow$

Prop. 7.18:n tod. (kertolasku) Olk. $a, a', b, b' \in R$ s.e. $a \sim a'$, $b \sim b'$.

$$ab - a'b' = \underline{ab - ab'} + \underline{ab' - a'b'} = \underbrace{a\underbrace{(b-b')}_{\in J}}_{\in J} + \underbrace{\underbrace{(a-a')}_{\in J}b'}_{\in J} \in J \quad \square$$

$\pi : R \to R/J$

Prop. 7.19. Tekijäjoukko R/J on rengas ja tekijäkuvaus $\underset{\in R}{r} \longmapsto \underbrace{r+J}_{\in R/J}$ on renkashomomorfismi.

$$\pi(r+s) = (r+s)+J \overset{\uparrow}{=} (r+J)+(s+J) = \pi(r)+\pi(s)$$

laskut määr.

(5) Tod. ks. luvun 1 tulokset ja L. 2.12. Harj.

Lause 7.26. Olk. K kunta, $P(x) \in K[X]$. Ol. $\# K = q$. Tällöin

$$\#\left(K[X] / (P(x)) \right) = q^{\deg P(x)}.$$

Tod. Jakoyhtälö: Jos $Q(x) \in K[X]$, niin jakoyhtälön nojalla on $S(x), \bar{Q}(x) \in K[X]$ s.e.

$$Q(x) = S(x)P(x) + \bar{Q}(x) \quad \text{s.e.} \quad \deg \bar{Q}(x) < \deg Q(x)$$

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

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

Siis jokaisella ekv. luokalla $Q(x) + (P(x))$ on edustaja, jonka aste on $< \deg Q(x)$. Jos $A(x), B(x) \in K[X]$ ja $A(x) - B(x) \in (P(x))$

$\deg A(x), \deg B(x) < \deg P(x)$.

ainoa $(P(x))$:n alkio, jonka aste $< \deg P(x)$ on 0

$$\implies A(x) = B(x).$$

$\implies$ ekv. luokkia on yhtä monta kuin joukon $\overbrace{\{A(x) \in K[X], \deg A(x) < \deg P(x)\}}^{\# = q^{\deg P(x)}}$ alkioita.

$$\sum_{k=0}^{\deg P(x)-1} a_k X^k$$

$\square$

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

Renkaassa $(\mathbb{Z}/2\mathbb{Z})[X]/(P(x))$ on 4 alkiota:

$$\{0 + (P(x)),\ 1 + (P(x)),\ X + (P(x)),\ X+1 + (P(x))\} = (\mathbb{Z}/2\mathbb{Z})[X]/(P(x))$$

Laskutaulut (edustajien avulla)

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X+1	1
X+1	0	X+1	1	X

$\underline{X^2} - (X^2+X+1)$

$= \underline{\underline{X+1}}$

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