Renkaat ja kunnat 9.2.2021

Muista: Renkaassa $\mathbb{Z}$ alkualkiot ja jaottomat alkiot ovat sama asia.

Eilinen esim. 5.11. ja 5.14

P.5.12: Kokonaisalueen alkualkiot ovat jaottomia

$2 \in \mathbb{Z}[\sqrt{-3}]$ on jaoton mutta ei ole alkualkio

Jos $ab = 2$, niin a tai b on yksikkö

Jos $a \mid 2$, niin $n(a) \mid n(2)$
$$n(2) = 4$$

Tark. kaikki alkiot, joiden normi on $\underline{1}$, 2 tai $\underline{\underline{4}}$

Jos $n(a) = 1$, niin a on yksikkö.

Ei ole alkiota, jonka normi on 2

Jos $n(a) = 4$ ja $ab = 2$, niin $n(b) = 1$ ja b on yksikkö.

Jos $2 \mid cd$, niin $2 \mid c$ tai $2 \mid d$

$2 \mid 4$, $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$

Jos 2 olisi alkualkio, niin $2 \mid 1 + i\sqrt{3}$ tai $2 \mid 1 - i\sqrt{3}$

Mutta $n(2) = 4 = n(1 \pm i\sqrt{3})$

Jos $(1 + i\sqrt{3}) = 2u$, niin

$4 = n(1 + i\sqrt{3}) = n(2u) = 4n(u)$

$\Rightarrow \boxed{n(u) = 1 = u\bar{u}}$ Jos $u \in \mathbb{Z}[\sqrt{-3}]$, niin $\bar{u} \in \mathbb{Z}[\sqrt{-3}]$. Siis u on yksikkö $\Rightarrow u = \pm 1$

$\Rightarrow 2 = \pm(1 + i\sqrt{3})$, ristiriita.

①

$\mathbb{Z}/q\mathbb{Z}$.

P. 5.15. $a+q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z})^\times \iff \operatorname{syt}(a,q)=1$

P. 5.17 Jos $\operatorname{syt}(a,q) \geq 2$, niin $a+q\mathbb{Z}$ on nollan jakaja.

$a+q\mathbb{Z} \neq 0$

Tod.

Jos $a=bc$ ja $q=bq'$ (siis b jakaa a:n ja q:n),

niin $(a+q\mathbb{Z})(q'+q\mathbb{Z}) = \underbrace{aq'}_{\substack{\parallel \\ bcq' = c(bq') = cq}} + q\mathbb{Z} = 0+q\mathbb{Z}$

Jos $1<a<q$, niin $1<q'<q$, joten $a+q\mathbb{Z}$ on nollan jakaja.

$\boxed{b\neq 1}$

Huom. Riittää, että a:lla ja q:lla on yhteinen tekijä >1.

② Harj. 5.8 $\mathbb{Z}/10\mathbb{Z}$:n yksiköt ja nollan jakajat: $\cancel{0}$ 1 2 3 4 5 6 7 8 9

yks -1 $\parallel$

nollan jakajia.

Seuraus. Jos $a+q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z} - \{0\}$, niin $a+q\mathbb{Z}$ on yksikkö tai nollan jakaja.

Seuraus Jos p on alkuluku, niin $\mathbb{Z}/p\mathbb{Z}$ on kunta.

Tod. Ol. että $(a+p\mathbb{Z})(b+p\mathbb{Z}) = 0$.

$= ab+p\mathbb{Z}$

Tällöin $p \mid ab$. Koska p on alkuluku, pätee $p \mid a$ tai $p \mid b$

$\Rightarrow a+p\mathbb{Z} = 0$ tai $b+p\mathbb{Z} = 0$. Siis renkaassa $\mathbb{Z}/p\mathbb{Z}$ ei ole nollan jakajia: $\mathbb{Z}/p\mathbb{Z}$ on äärellinen kokonaisalue, siis kunta L 5.8 nojalla. □

Lause 5.19 $\boxed{p \text{ alkuluku} \Leftrightarrow \mathbb{Z}/p\mathbb{Z} \text{ on kunta}}$

6 Polynomirenkaat

Määr. K komm. rengas, $n \in \mathbb{N}$, $a_0, a_1, \dots, a_n \in K$.

$$P(X) = \sum_{k=0}^{n} a_k X^k = a_0 + a_1 X + \dots + a_n X^n$$

on K-kertoiminen polynomi.

Jos $m > n$ ja $a_j = 0 \ \forall j > n$, niin

$$\sum_{k=0}^{m} a_k X^k = \sum_{k=0}^{n} a_k X^k$$

$$K[X] = \left\{ \sum_{k=0}^{n} a_k X^k : n \in \mathbb{N},\ a_k \in K \ \forall\, 0 \le k \le n \right\}.$$

$\sum_{k=0}^{n} a_k X^k = P(X) \in K[X]$ määrää polynomifunktion $P: K \to K$,

$$P(x) = \sum_{k=0}^{n} a_k x^k \quad \forall\, x \in K.$$

4

Esim. Olk. $K = \mathbb{Z}/2\mathbb{Z}$. Joukko $(\mathbb{Z}/2\mathbb{Z})[X]$ on ääretön, sillä $X^k \in (\mathbb{Z}/2\mathbb{Z})[X]$ $\forall\, k \geq 0$.

Montako funktiota joukosta $\mathbb{Z}/2\mathbb{Z}$ itseensä on? 4 kpl.

$\{0,1\}$

$$\begin{array}{cccc} 0 \to 0 & 0 \mapsto 0 & 0 \mapsto 1 & 0 \mapsto 1 \\ 1 \to 1 & 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 0. \\ \text{id}. & 0 & 1 & \end{array}$$

Polynomifunktioita $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ on korkeintaan 4.

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

$$\| $$

$$3X^2 + 1$$

käytetään edustajia

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

$= 2X^4 - X + 1$

Määr. K komm. rengas. $P(X) = \sum_{k=0}^{n} a_k X^k$, $Q(X) = \sum_{k=0}^{n\,m} b_k X^k$.

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

$$P(X)\,Q(X) = \sum_{k=0}^{\cancel{2n}\ n+m} \Big(\sum_{i+j=k} a_i b_j \Big) X^k$$

Merkintä $a_0 X^0$ merk. usein a_0:lla

tämä on vakiotermi

Esim

$$(a_1 X + a_0)(b_2 X^2 + b_1 X + b_0)$$

$a_0 X^0$

$$= a_1 b_2 X^3 + a_1 b_1 X^2 + a_1 b_0 X^1 + a_0 b_2 X^2 + a_0 b_1 X + a_0 b_0$$

$$= a_1 b_2 X^3 + (a_1 b_1 + a_0 b_2) X^2 + (a_1 b_0 + a_0 b_1) X + a_0 b_0$$

Polynomien +:n n.a. on polynomi

0 kaikki kertoimet $= 0$

$\cdot$:n n.a. on polynomi 1:

X^k:n kerroin $= 0\ \forall k \geq 1$

X^0:n —"— $= 1$.

6 Prop. 6.2. $K[X]$ näillä laskutoimituksilla on komm. rengas.

Prop. 6.5. Olk. K komm. rengas. Olk. $\mathrm{Fun}: K[x] \to \{ f: K \to K \} = \mathcal{F}(K,K)$

Esim 3.8

$\mathrm{Fun}(\underbrace{P(x)}_{\text{polynomi}}) = \underbrace{P}_{P(x)\text{:n määräämä funktio}}$. Fun on rengashomomorfismi.

Tod. Harj.

$K[X]$ on K-kertoimisten polynomien rengas, polynomirengas.

K on tämän polynomirenkaan kerroinrengas.

Määr. Jos $P(X) \in K[X]$ ja $c \in K$ s.e. $\underbrace{P(c)}_{\text{Polynomin } P(X) \text{ määräämän polynomifunktion } P \text{ arvo pisteessä } c \in K} = 0$, niin c on $P(X)$:n juuri.

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

$P(0) = 1 \qquad P(1) = 1^2+1 = 0$. 1 on ainoa juuri.