VI. KUNNAT JA POLYNOMIT

VI.1 Kunnat

Määr.: Kommutatiivinen rengas $K \neq \{0_K\}$ (siis $1_K \neq 0_K$) on **kunta**, jos $K^* = K \setminus \{0_K\}$, ts. jokaisella $a \in K$, $a \neq 0_K$, on käänteisalkio $a^{-1} \in K$.

Siis $(K, +, \cdot)$ on kunta $\Leftrightarrow$ $(K, +)$ ja $(K \setminus \{0_K\}, \cdot)$ ovat Abelin ryhmiä, ja $a(b+c) = ab + ac$ $\forall a, b, c \in K$.

Esim. 1: $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kuntia. $\mathbb{Q}$:n konstruoidaan yksityiskohtaisesti VI.3:ssa.

Lause 1: a) Jokainen kunta on kokonaisalue, samoin jokainen kunnan alirengas.
b) Jokainen äärellinen kok.alue on kunta.

Tod.: a) V.6:ssa todettiin: yleisemmin $a \in K \setminus \{0\} = K^*$ ei ole nollanjakaja.
b) Ol. R äärell. kok.alue ja $a \in R$, $a \neq 0$. Osoitetaan, että $a \in R^*$. a ei nollanjakaja $\Rightarrow$ $x \mapsto ax$ on injektio $R \to R$; R äärell. $\Rightarrow$ kok. injektio on myös surjektio (Lause II.13) $\Rightarrow$ $\exists x \in R$ s.e. $ax = 1$; tällöin x on a:n käänt. alkio (R kommut.!). $\square$

Esim. 3: p alkuluku $\Rightarrow$ äärell. kok. alue $\mathbb{Z}_p$ on kunta (on myös suoraan osoitettu, että $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$). n ei alkuluku $\Rightarrow$ $\mathbb{Z}_n$ ei kok.alue, siis ei kunta.

Ol. K kunta. Kun $a, b \in K$, $b \neq 0$, määr. **osamäärä** $\frac{a}{b} = a/b = ab^{-1} = b^{-1}a \in K$. a/b on se 1-käs. alkio $x \in K$, jolla $bx = a$. Laskusääntöjä:

$$
\begin{aligned}
(a/b) + (c/d) &= (ad+bc)/(bd) && (b,d \neq 0)\\
(a/b)\cdot(c/d) &= (ac)/(bd) && (b,d \neq 0)\\
-(a/b) &= (-a)/b = a/(-b) && (b \neq 0)\\
(a/b)^{-1} &= b/a && (a,b \neq 0)\\
a/b = c/d &\Leftrightarrow ad = bc && (b,d \neq 0).
\end{aligned}
$$

Tod. vaikkeivat ensimm.: $(a/b) + (c/d) = ab^{-1} + cd^{-1} =$

$= ad b^{-1}d^{-1} + bc b^{-1}d^{-1} = (ad+bc)\cdot(bd)^{-1}$
$= (ad+bc)/(bd)$ (Huom.: käytettiin mm. kertolaskun vaihdannaisuutta.)

Esim. 4: Koska $\mathbb{Z}_5$ on $\bar{2}\cdot\bar{3} = \bar{6} = \bar{1}$ ja $\bar{4}\cdot\bar{4} = \bar{16} = \bar{1}$ $\Rightarrow$ $\bar{2}^{-1} = \bar{3}$, $\bar{4}^{-1} = \bar{4}$ $\Rightarrow$

$(\bar{1}/\bar{2}) + (\bar{1}/\bar{4}) = \bar{1}\cdot\bar{2}^{-1} + \bar{1}\cdot\bar{4}^{-1} = \bar{3} + \bar{4} = \bar{7} = \bar{2}$,

$(\bar{1}/\bar{2}) + (\bar{3}/\bar{4}) = \bar{1}\cdot\bar{2}^{-1} + \bar{3}\cdot\bar{4}^{-1} = \bar{3} + \bar{3}\cdot\bar{4} = \bar{15} = \bar{0}$.

Määr.: Kunnan K alirengas L on K:n alikunta, jos $a^{-1} \in L$ aina, kun $a \in L$, $a \neq 0_K$. Myös san., että K on L:n laajennuskunta.

Alikunta on itsekin kunta indus. laskutoimitusten suhteen.

Lause 4 (Alikuntakriteeri): Kunnan K osajoukko L on K:n alikunta $\Leftrightarrow$

i) L:ssä on vähintään kaksi alkiota,
ii) $a - b \in L$ aina, kun $a, b \in L$, ja
iii) $ab^{-1} \in L$ aina, kun $a, b \in L$, $b \neq 0$. $\square$

Esim.: a) $\mathbb{Q}$ on $\mathbb{R}$:n alikunta, $\mathbb{R}$ $\mathbb{C}$:n.
b) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ on $\mathbb{R}$:n alikunta (harj. tehtävä).

Lause 2: Komm. rengas $R \neq \{0\}$ on kunta $\Leftrightarrow$ R:n ainoat ideaalit ovat $\{0\}$ ja R.

Tod.: $\Rightarrow$: Ol. R kunta ja $\{0\} \neq I \subset R$ ideaali. Val. $a \in I$, $a \neq 0$. R kunta $\Rightarrow$ $\exists a^{-1} \in R$; I ideaali $\Rightarrow$ $1 = \underset{\in R}{a^{-1}} \cdot \underset{\in I}{a} \in I \Rightarrow I = R$.

$\Leftarrow$: Ol. R:n ainoat ideaalit ovat $\{0\}$ ja R. Olk. $a \in R$, $a \neq 0$. Tark. pääideaalia $\langle a \rangle = \{xa \mid x \in R\} \subset R$. $0 \neq a \in \langle a \rangle \Rightarrow \langle a \rangle \neq \{0\}$; ol. $\Rightarrow$ $\langle a \rangle = R$ $\Rightarrow$ $1 \in \langle a \rangle \Rightarrow \exists x \in R$ s.e. $xa = 1$. Tällöin x on a:n kääntäj. alkio. $\square$

Lause 3: K kunta, $R \neq \{0\}$ rengas $\Rightarrow$ jokainen rengashomom. $f: K \to R$ on injektio.

Tod.: f rengashomom. $\Rightarrow$ $\ker(f) \subset K$ K:n ideaali.
$f(1_K) = 1_R \neq 0_R \Rightarrow 1_K \notin \ker(f) \Rightarrow \ker(f) \neq K$.
Lause 2 $\Rightarrow$ $\ker(f) = \{0_K\} \Rightarrow f$ on injektio. □

Erityisesti jokainen kuntahomomorfismi (eli kuntien välinen rengashomom.) on injektio.

Ol. K kunta. K myös kok. alue $\Rightarrow$ karakteristika $\mathrm{char}(K)$ on määritelty. 2 tapausta:

1) $\mathrm{char}(K) = 0$. Tällöin $\mu : \mathbb{Z} \to K$, $\mu(m) = m \cdot 1_K$ $\forall m \in \mathbb{Z}$, on injekt. rengashomom. VI.3 $\Rightarrow$ μ indusoi kuntahomom. $\bar{\mu} : \mathbb{Q} \to K$, jonka kuva $\mathrm{Im}(\bar{\mu})$ on K:n alikunta, $\mathrm{Im}(\bar{\mu}) \cong \mathbb{Q}$.

2) $\mathrm{char}(K) = p$ alkuluku. Em. μ indusoi kuntahomom. $\mathbb{Z}_p \to K$; $\mathrm{Im}(\mu)$ on K:n alikunta, $\mathrm{Im}(\mu) \cong \mathbb{Z}_p$.

VI.3 Kokonaisalueen osamääräkunta

Olkoon R kokonaisalue. Osoitamme, että R voidaan tulkita sellaisen kunnan $Q(R)$ alirenkaaksi, että kaikki $Q(R)$:n alkiot ovat muotoa a/b, $a, b \in R$, $b \neq 0$.

Merk. $S = R \setminus \{0\}$. R kok. alue $\Rightarrow$ S on suljettu R:n kertolaskun suhteen, ts. $b, d \in S \Rightarrow bd \in S$.

Lemma 1: jos on $R \times S$ relaatio E,

$$(a,b)\,E\,(c,d) \Leftrightarrow ad = bc \quad (a,c \in R,\ b,d \in S)$$

on ekvivalenssi.

Tod.: Refl.: $(a,b)\,E\,(a,b)$, koska $ab = ba$.
Symm.: $(a,b)E(c,d) \Rightarrow ad = bc \Rightarrow cb = da$
$\Rightarrow (c,d)\,E\,(a,b)$.
Transit.: $(a,b)\,E\,(c,d)$, $(c,d)\,E\,(e,f) \Rightarrow ad = bc$, $cf = de$
$\Rightarrow adf = bcf = bde \Rightarrow d \cdot af = d \cdot be$;
R kok. alue, $d \neq 0 \Rightarrow af = be$ eli $(a,b)\,E\,(e,f)$. □

Merk. $Q(R) = (R \times S)/E$ ja $\langle a,b \rangle \in Q(R)$ alkion $(a,b) \in R \times S$ ekv. luokka.

Lemma 2: $(a,b),(a',b'),(c,d),(c',d') \in R \times S$ s.e. $\langle a,b\rangle = \langle a',b'\rangle$ ja $\langle c,d\rangle = \langle c',d'\rangle$

$$\Rightarrow \quad \langle ad+bc, bd\rangle = \langle a'd'+b'c', b'd'\rangle,$$
$$\langle ac, bd\rangle = \langle a'c', b'd'\rangle .$$

Tod.: $b,b',d,d' \in S \Rightarrow bd, b'd' \in S$ (tuotettu ylhää).
$\langle a,b\rangle = \langle a',b'\rangle$, $\langle c,d\rangle = \langle c',d'\rangle \Rightarrow ab' = ba'$, $cd' = dc'$. Näin ollen

$$\begin{aligned}(ad+bc)\cdot b'd' &= adb'd' + bcb'd' = ab'\cdot dd' + bb'\cdot cd' \\ &= ba'\cdot dd' + bb'\cdot dc' = bd\,a'd' + bd\,b'c' \\ &= bd\cdot(a'd'+b'c'),\end{aligned}$$
$$ac\cdot b'd' = ab'\cdot cd' = ba'\cdot dc' = bd\cdot a'c',$$

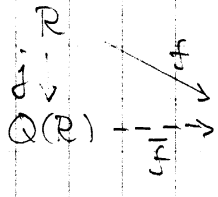
joten $\langle ad+bc, bd\rangle = \langle a'd'+b'c', b'd'\rangle$, $\langle ac, bd\rangle = \langle a'c', b'd'\rangle$. ∎

Le 2 $\Rightarrow$ $Q(R)$:ssä voidaan määr. laskutoimitukset $+$ ja $\cdot$ kaavoilla

$$\begin{aligned}\langle a,b\rangle + \langle c,d\rangle &= \langle ad+bc, bd\rangle \qquad (a,c\in R,\ b,d\in S)\\ \langle a,b\rangle \cdot \langle c,d\rangle &= \langle ac, bd\rangle\end{aligned}.$$

Lause 9: a) $(Q(R),+,\cdot)$ on kunta, kokonais-alueen R *osamääräkunta* (l. *jakokunta*). Kaavan $j(a) = \langle a,1\rangle$ $\forall a\in R$ määrittelemä kuvaus $j: R \to Q(R)$ on injektiivinen rengashomom. Kaikki $Q(R)$:n alkiot ovat muotoa $j(a)/j(b)$, $a,b\in R$, $b\neq 0$.

b) Jos K on kunta ja $f: R\to K$ on injekt. rengashomom., niin $\exists$ 1-käs. kuntahomom. $\bar{f}: Q(R)\to K$ s.e. seur. kaavio kommutoi:



Tod.: a) Rengasaksioomista tod. mallikin osittelulaki:

$$\begin{aligned}(\langle a,b\rangle + \langle c,d\rangle)\cdot\langle e,f\rangle &= \langle ad+bc, bd\rangle\cdot\langle e,f\rangle \\ &= \langle (ad+bc)\cdot e, bd\cdot f\rangle,\end{aligned}$$
$$\langle a,b\rangle\cdot\langle e,f\rangle + \langle c,d\rangle\cdot\langle e,f\rangle = \langle ae, bf\rangle + \langle ce, df\rangle$$

$= \langle ae\cdot df + bf\cdot ce\,,\ bf\cdot df\rangle$;

nämä ovat yhtäs., koska

$$(ad+bc)e\cdot bfdf = abd^2ef^2 + b^2cdef^2$$
$$= bdf\cdot(aedf + bfce)\,.$$

Selvästi $0_{Q(R)} = \langle 0,1\rangle$, $-\langle a,b\rangle = \langle -a,b\rangle$ ja $1_{Q(R)} = \langle 1,1\rangle$. Kun $\langle a,b\rangle \in Q(R)$ (eli $a,b\in R$, $b\neq 0$), niin $\langle a,b\rangle \neq 0 = \langle 0,1\rangle \Leftrightarrow a\neq 0$; tällöin myös $\langle b,a\rangle \in Q(R)$ ja

$$\langle a,b\rangle\cdot\langle b,a\rangle = \langle ab, ba\rangle = \langle 1,1\rangle = 1\,,$$

koska $ab\cdot 1 = ba\cdot 1$; eli $\langle b,a\rangle = \langle a,b\rangle^{-1}$ $Q(R)$:ssä.

Kuvaus $j: R\to Q(R)$ on rengashomom., koska
$j(a+b) = \langle a+b,1\rangle = \langle a\cdot 1 + 1\cdot b, 1\cdot 1\rangle = \langle a,1\rangle + \langle b,1\rangle$
$= j(a) + j(b)$, $j(ab) = \langle ab,1\rangle = \langle ab, 1\cdot 1\rangle$
$= \langle a,1\rangle\cdot\langle b,1\rangle = j(a)\cdot j(b)$, ja $j(1) = \langle 1,1\rangle = 1$.
j on inj., sillä $j(a) = 0 \Rightarrow \langle a,1\rangle = \langle 0,1\rangle$
$\Rightarrow a\cdot 1 = 1\cdot 0 \Rightarrow a = 0$.
Kun $\langle a,b\rangle \in Q(R)$ $(a,b\in R,\ b\neq 0)$, on

$$\langle a,b\rangle = \langle a\cdot 1, 1\cdot b\rangle = \langle a,1\rangle\cdot\langle 1,b\rangle$$
$$= \langle a,1\rangle\cdot(\langle b,1\rangle)^{-1} = j(a)\cdot j(b)^{-1} = j(a)/j(b)\,.$$

b) Ol. K kunta, $f: R\to K$ injekt. rengashomom.; silloin $f(b)\neq 0$ $\forall b\in R$, $b\neq 0$, ts. $b\in R\setminus\{0\} \Rightarrow \exists f(b)^{-1}\in K$.
jos $\bar f: Q(R)\to K$ on kuntahomom. ja $\bar f\circ j = f$, niin $\bar f(\langle a,b\rangle) = \bar f(j(a)\cdot j(b)^{-1}) = \bar f(j(a))\cdot\bar f(j(b))^{-1}$
$= \bar f(j(a))\cdot\bar f(j(b))^{-1} = f(a)\cdot f(b)^{-1}$ $\forall\langle a,b\rangle\in Q(R)$
$\Rightarrow \bar f$ on 1-käs. määrätty.
Käänteen, kaava $\bar f(\langle a,b\rangle) = f(a)\cdot f(b)^{-1}$ $\forall\langle a,b\rangle\in Q(R)$ määr. kuvauksen $\bar f: Q(R)\to K$, sillä $\langle a,b\rangle = \langle a',b'\rangle \Rightarrow ab' = ba' \Rightarrow$
$f(ab') = f(ba') \Rightarrow f(a)\cdot f(b') = f(b)\cdot f(a')$
$\Rightarrow f(a)\cdot f(b)^{-1} = f(a')\cdot f(b')^{-1}$.
Näin saatu $\bar f$ on (selvästi?) vaadittu kuntahomom. □

Huom.: a) jos R on jo valmiiksi kunta, niin

j on isomorfismi $R \xrightarrow{\sim} Q(R)$ ($\langle a,b\rangle \in Q(R) \Rightarrow$ $\langle a,b\rangle = j(a)\,j(b)^{-1} = j(ab^{-1}) \in \mathrm{Im}(j)$, kun $\exists b^{-1} \in R$).

b) Kun samastetaan R ja $\mathrm{Im}(j) \subset Q(R)$ s.e. $R \ni a$ "$=$" $\langle a,1\rangle = j(a) \in \mathrm{Im}(j)$ $\forall a \in R$, on siis $R \subset Q(R)$ ja

$$Q(R) = \{j(a)/j(b) \mid a,b \in R,\ b \neq 0\} = \{a/b \mid a,b \in R,\ b \neq 0\}.$$

Määr.: Kok. alueen $\mathbb{Z}$ osamäärärakenta on rationaalilukujen kunta $\mathbb{Q}$.

VI.6 Polynomit

Ol. R komm. rengas. Tark. joukkoa $R^{\mathbb{N}} = \{f \mid f$ on kuvaus $\mathbb{N} \to R\}$. Alkio $f \in R^{\mathbb{N}}$ esitetään seuraavassa yleensä muodossa

$$f = (f_0, f_1, f_2, \dots), \quad f_n = f(n) \in R \quad \forall n \in \mathbb{N}.$$

Ehk., jos $f, g \in R^{\mathbb{N}}$, niin $f = g \iff f_n = g_n\ \forall n \in \mathbb{N}$.

Olk. $f, g \in R^{\mathbb{N}}$. Määr. $f+g \in R^{\mathbb{N}}$ ja $f*g \in R^{\mathbb{N}}$ s.e. kaikilla $n \in \mathbb{N}$ on

$$\begin{aligned}(f+g)_n &= f_n + g_n,\\ (f*g)_n &= f_0 g_n + f_1 g_{n-1} + \dots + f_n g_0\\ &= \sum_{i=0}^{n} f_i g_{n-i} = \sum_{i+j=n} f_i g_j.\end{aligned}$$

(Huom.: Tässä $+$ = funktiorenkaan $R^{\mathbb{N}}$ yht.laskun
$*$ ≠ -"- -"- kertolaskun.)

Lemma 1: $(R^{\mathbb{N}}, +, *)$ on kommutatiivinen rengas (sen alkioita kutsutaan R-kertoimisiksi formaaleiksi potenssisarjoiksi).

Tod.: Kuten funktiorenkaalla, $(R^{\mathbb{N}}, +)$ on Ab. ryhmä. Selvästi R komm. $\Rightarrow$ $*$ on vaihdannainen.

$\bar{1} = (1,0,0,\dots) \in R^{\mathbb{N}}$ on $*$:n neutr. alkio, sillä jos $f \in R^{\mathbb{N}}$, niin

$$(\bar{1}*f)_n = \underbrace{1}_{=\bar{1}_0} f_n + \underbrace{0}_{=\bar{1}_1} f_{n-1} + \dots + \underbrace{0}_{=\bar{1}_n} f_0 = f_n \quad \forall n \in \mathbb{N},$$

jolloin $\bar{1} * f = f \ (= f * \bar{1})$.

$*$:n liitännäisyys: $f, g, h \in R^{\mathbb{N}} \Rightarrow$

$$[f*(g*h)]_n = \sum_{i+m=n} f_i \cdot (g*h)_m = \sum_{i+m=n} \left[f_i \cdot \left(\sum_{j+k=m} g_j h_k \right) \right]$$

$$= \sum_{i+j+k=n} f_i \cdot (g_j \cdot h_k) = \sum_{i+j+k=n} (f_i \cdot g_j) \cdot h_k$$

$$= \sum_{m+k=n} \left[\left(\sum_{i+j=m} f_i \cdot g_j \right) \cdot h_k \right] = \sum_{m+k=n} (f*g)_m \cdot h_k$$

$$= [(f*g)*h]_n \quad \forall n \in \mathbb{N}$$

$\Rightarrow f*(g*h) = (f*g)*h$. Osittelulait väitteen todistaa vastaavasti. $\square$

Kuvaus $a \mapsto (a, 0, 0, \dots)$ määr. selvästi injektiivisen rengashomom. $R \to (R^{\mathbb{N}}, +, *)$; tämän välityksellä tulkitaan R renkaan $(R^{\mathbb{N}}, +, *)$ alirenkaaksi samastamalla $a \in R$ ja $(a, 0, 0, \dots) \in R^{\mathbb{N}}$ keskenään $\forall a \in R$.

Määr.: $f \in R^{\mathbb{N}}$ on R-kertoiminen polynomi, jos $f_n \neq 0$ vain äärell. monella $n \in \mathbb{N}$, ts. jos $\exists\, m = m_f \in \mathbb{N}$ s.e. $f_n = 0 \ \forall n > m$. Merk. $R^{(\mathbb{N})} = \{ f \in R^{\mathbb{N}} \mid f \text{ on polynomi} \}$.

Lemma 2: $R^{(\mathbb{N})}$ on renkaan $(R^{\mathbb{N}}, +, *)$ alirengas.

Tod.: Selvästi $1 = (1, 0, 0, \dots) \in R^{(\mathbb{N})}$ (ja $a = (a, 0, \dots, 0) \in R^{(\mathbb{N})} \ \forall a \in R$). Olk. sitten $f, g \in R^{(\mathbb{N})}$; $f_n = 0 \ \forall n > m_f \in \mathbb{N}$, $g_n = 0 \ \forall n > m_g \in \mathbb{N}$. Silloin

$$(f-g)_n = f_n - g_n = 0 \quad \forall n > \max\{m_f, m_g\},$$
$$(f*g)_n = \sum_{i+j=n} f_i \cdot g_j = 0 \quad \forall n > m_f + m_g$$

($i+j = n > m_f + m_g \Rightarrow i > m_f$ tai $j > m_g \Rightarrow f_i = 0$ tai $g_j = 0 \Rightarrow f_i g_j = 0$). Siispä $f-g, f*g \in R^{(\mathbb{N})}$. $\square$

Merk. $x = (0, 1, 0, 0, \dots) \in R^{(\mathbb{N})}$ (muom.: $x \notin R$!). Lasketaan $x^k = \underbrace{x * x * \dots * x}_{k \text{ kpl}} \in R^{(\mathbb{N})}$, kun $k \in \mathbb{N}$.

V. $x^k = (0, \dots, 0, 1, 0, 0, \dots)$, ts. $(x^k)_k = 1$ ja $(x^k)_n = 0 \ \forall n \neq k$.

T. $x^0 = 1 = (1, 0, 0, \dots)$. Jnd. ol.: kuvaus pätee x^k:lle, missä $k \in \mathbb{N}$. Silloin

$$(x^{k+1})_n = (x^k * x)_n = \sum_{i+j=n} (x^k)_i \cdot x_j \quad ; \quad$$

$$(x^k)_i \cdot x_j = \begin{cases} 1 \cdot 1 = 1, & \text{kun } i=k, j=1, n=i+j=k+1 \\ 0 & \text{muulloin.} \end{cases} \quad \square$$

Kun $a \in R \subset R^{(\mathbb{N})}$ ja $k \in \mathbb{N}$, on $a * x^k =$
$= (a,0,0,\dots) * (0,\dots,0,\frac{1}{k},0,0,\dots) = (0,\dots,0,\frac{a}{k},0,0,\dots)$.

Merkitään tämän jälkeen yksinkertaisesti $* = \cdot$; erityisesti $a * x^k = ax^k$. Kun $n \in \mathbb{N}$ ja $f_0, f_1, \dots, f_n \in R$, on siis

$$\begin{aligned} f_0 + f_1 x + \dots + f_n x^n &= (f_0, 0, \dots) + (0, f_1, 0, \dots) + \\ &+ (0,0,f_2,0,\dots) + \dots + (0,\dots,0,f_n,0,\dots) \\ &= (f_0, f_1, \dots, f_n, 0, 0, \dots). \end{aligned}$$

Siten $R^{(\mathbb{N})} = \{ f_0 + f_1 x + \dots + f_n x^n \mid n \in \mathbb{N};\ f_0, \dots, f_n \in R \}$, ja on tapana merkitä $R[x] = R^{(\mathbb{N})}$.

Lause 12: $(R[x], +, \overset{*}{\cdot})$ on kommutatiivinen rengas, R-sisältävä polynomirengas. $\square$

Ol. $f = f_0 + f_1 x + \dots \in R[x]$, $g = g_0 + g_1 x + \dots \in R[x]$. Tällöin siis

$$f = g \iff f_n = g_n \ \forall n \in \mathbb{N}.$$

Tulo $f \cdot g$ ($= f * g$!) voidaan laskea "tavallisemmalla tapaan" $R[x]$:n rengasoman. avulla:

Esim.: $\mathbb{Z}[x]$:ssä on $(2+3x+x^3)\cdot(5+4x^3) =$
$= 2\cdot 5 + 2\cdot 4x^3 + 3x\cdot 5 + 3x\cdot 4x^3 + x^3\cdot 5 + x^3 \cdot 4x^3 =$
$= 10 + 8x^3 + 15x + 12x^4 + 5x^3 + 4x^6$
$= 10 + 15x + 13x^3 + 12x^4 + 4x^6$.

Kun $f = f_0 + f_1 x + \dots + f_n x^n \in R[x]$ ja $c \in R$, R:n alkio

$$f(c) = f_0 + f_1 c + \dots + f_n c^n \in R$$

on f:n arvo c:ssä. Kun f pid. kiinteänä, saadaan kuvaus $c \mapsto f(c)$, polynomin f määräämä polynomikuvaus $R \to R$.

Huom.: Kahteen eri polynomiin voi liittyä sama polynomikuvaus, ts. voi olla $f \neq g \in R[x]$, vaikka $f(c) = g(c)$ $\forall c \in R$.

Esim.: Olk. p alkuluku ja $f = x^p - x \in \mathbb{Z}_p[x]$. Silloin $f \neq 0$, mutta $f(c) = c^p - c = 0$ $\forall c \in \mathbb{Z}_p$ (Fermat).

Kun pidetään yllä $c \in R$ kiinteänä, saadaan kaavan $f \mapsto f(c)$ määrittelemä kuvaus $R[x] \to R$.

Lause: Kun $c \in R$, niin kuvaus $f \mapsto f(c)$ on rengashomomorfismi $R[x] \to R$.

Tod.: Selvästi valiopolyn. $1 \mapsto 1 \in R$. Olk. sitten $f = \sum_{i \in \mathbb{N}} f_i x^i \in R[x]$ ja $g = \sum_{i \in \mathbb{N}} g_i x^i \in R[x]$. Silloin

$$(f+g)(c) = \sum_{i \in \mathbb{N}} (f_i + g_i) c^n = \sum_{i \in \mathbb{N}} f_i c^i + \sum_{i \in \mathbb{N}} g_i c^i$$

$$= f(c) + g(c), \text{ ja}$$

$$(f \cdot g)(c) = \sum_{k \in \mathbb{N}} \left(\sum_{i+j=k} f_i g_j \right) c^k = \sum_{i \in \mathbb{N}} \sum_{j \in \mathbb{N}} f_i g_j c^{i+j}$$

$$= \left(\sum_{i \in \mathbb{N}} f_i c^i \right) \cdot \left(\sum_{j \in \mathbb{N}} g_j c^j \right) = f(c) \cdot g(c);$$

huom., että summissa $\sum_{i \in \mathbb{N}}$ jne. vain äärell. moni termi on $\neq 0$. $\square$

Ol. $f \in R[x]$, $f \neq 0$ $\Rightarrow$ vaik. kirj. $f = f_0 + f_1 x + \dots + f_n x^n$, missä $n \in \mathbb{N}$, $f_0, \dots, f_n \in R$ ja $f_n \neq 0$ (siis $f_k = 0$ $\forall k > n$). Tässä $n = \deg(f) \in \mathbb{N}$ on polynomin $f \in R[x] \setminus \{0\}$ aste ja f_n on f:n johtava kerroin.

Lisäksi määr. $\deg(0) = -\infty$ ($\notin \mathbb{N}$!). Sovimme, että $-\infty < k$ $\forall k \in \mathbb{N}$ ja $-\infty + k = k + (-\infty) = -\infty$ $\forall k \in \mathbb{N} \cup \{-\infty\}$. Kun $f \in R[x]$, on siis $f \neq 0 \iff \deg(f) \geq 0$.

Lause 13: $f, g \in R[x] \Rightarrow$

a) $\deg(f+g) \begin{cases} = \max\{\deg(f), \deg(g)\}, & \text{jos } \deg(f) \neq \deg(g) \\ \leq \quad - " - , & \text{jos } \deg(f) = \deg(g); \end{cases}$

b) $\deg(f\cdot g) \begin{cases} \leq \deg(f)+\deg(g) \\ = \deg(f)+\deg(g), \text{ jos } R \text{ on kok. alue.} \end{cases}$

Tod.: jos $g=0$, niin $f+g=f$ ja $f\cdot g=0$
$\Rightarrow$ väitteet pätevät; samoin, jos $f=0$.
Ol. $f\neq 0\neq g$, $\deg(f)=m\in\mathbb{N}$, $\deg(g)=n\in\mathbb{N}$,
$f=f_0+f_1x+\ldots+f_mx^m$, $g=g_0+g_1x+\ldots+g_nx^n$, $f_m\neq 0\neq g_n$.
a) jos $m=n$, niin $f+g=(f_0+g_0)+\ldots+(f_n+g_n)x^n$
$\Rightarrow \deg(f+g)\leq n=\deg(f)=\deg(g)$ ($<$, jos $f_n=-g_n$).
jos taas esim. $m>n$, niin $f+g=(f_0+g_0)+\ldots$
$\ldots+(f_n+g_n)x^n+f_{n+1}x^{n+1}+\ldots+f_mx^m$, joten
$\deg(f+g)=m=\deg(f)=\max\{\deg(f),\deg(g)\}$.

b) $f\cdot g=f_0g_0+(f_0g_1+f_1g_0)x+\ldots+(f_{m-1}g_n+f_mg_{n-1})x^{m+n-1}+$
$+f_mg_nx^{m+n} \Rightarrow \deg(f\cdot g)\leq m+n=\deg(f)+\deg(g)$.
jos R on kok. alue, niin $f_m\neq 0\neq g_n \Rightarrow f_mg_n\neq 0$
$\Rightarrow \deg(f\cdot g)=m+n=\deg(f)+\deg(g)$. $\square$

<u>Seuraus</u>: R kokonaisalue $\Rightarrow R[x]$ kokonaisalue.

Tod.: $f\neq 0\neq g \Rightarrow \deg(f)\geq 0$, $\deg(g)\geq 0$
$\Rightarrow \deg(f\cdot g)=\deg(f)+\deg(g)\geq 0+0=0$ (koska R kok.alue)
$\Rightarrow f\cdot g\neq 0$. $\square$

<u>Lause</u>: R kokonaisalue $\Rightarrow R[x]^*=R^*$

Tod.: $R\subset R[x]$ aitosti $\Rightarrow R^*\subset R[x]^*$.
Toisaalta $f\in R[x]^* \Rightarrow \exists\, g\in R[x]$ s.e. $f\cdot g=1$
$\Rightarrow 0=\deg(1)=\deg(f\cdot g)=\deg(f)+\deg(g)$
$\Rightarrow \deg(f)=\deg(g)=0 \Rightarrow f,g\in R$; koska $f\cdot g=1$,
on siis $f,g\in R^*$. $\square$

Jos R on kok.alue, ovat sen käänteyvät alkiot aitoat $R[x]$:n käänteyvät alkiot. Yleisesti näin ei ole:

<u>Esim.</u>: $\mathbb{Z}_4[x]$: sen $(1+2x)\cdot(1+2x)=1+4x+4x^2=1$,
joten $1+2x\in\mathbb{Z}_4[x]^*$.
(Tässä tulkitaan, että $1=[1]_4$, $2=[2]_4$ jne.)