VI.7 Polynomien jaollisuus

Ol. R komm. rengas, $f, g \in R[x]$. Kuten koh. luvuilla, f on jaollinen g:llä ($\ell.$ g on f:n tekijä $\ell.$ ...), merk. $g \mid f$, jos $\exists\, h \in R[x]$ s.e. $f = g \cdot h$.

Esim. 1: a) $(x-1)\cdot(x+1) = x^2 - 1 \Rightarrow (x-1) \mid (x^2+1)$ $R[x]$:ssä (R mieliv. komm. rengas).

b) $\mathbb{Z}_2[x]$:ssä $(x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1$
$\Rightarrow (x+1) \mid (x^2+1)$ $\mathbb{Z}_2[x]$:ssä.

c) $(x+1) \nmid (x^2+1)$ $\mathbb{R}[x]$:ssä (vastoin: $\exists\, h \in \mathbb{R}[x]$ s.e. $x^2+1 = (x+1)\cdot h$. Lasketaan arvot alkiolla $-1 \in \mathbb{R}$: $(-1)^2 + 1 = ((-1)+1)\cdot h(-1) \Rightarrow 2 = 0$, RR.)

Jaollisuusrelaatiolla $\mid$ $R[x]$:ssä on seur. ominaisuudet:

$f \mid f \quad \forall f \in R[x]$;
$f \mid g$ ja $g \mid h \Rightarrow f \mid h$;
$f \mid g$ ja $f \mid h \Rightarrow f \mid (g+h)$.

Kun $f \in R[x]$, merk. $\langle f \rangle = R[x]\cdot f = \{h \cdot f \mid h \in R[x]\}$ f:n virittämä $R[x]$:n pääidealli. Siispä

$$g \in \langle f \rangle \iff f \mid g.$$

Lemma: Ol. R koh. alue ja $f, g \in R[x]$. Seur. ehdot ovat yhtäpitävät:

a) $f \mid g$ ja $g \mid f$;
b) $\langle f \rangle = \langle g \rangle$;
c) $\exists$ käänteinen alkio $a \in R^*$ s.e. $g = a \cdot f$.

(a) $\Leftrightarrow$ b) pätee mieliv. komm. renkaalla R.)

Tod.: a) $\Leftrightarrow$ b). $f \mid g \Leftrightarrow g \in \langle f \rangle \Leftrightarrow \langle g \rangle \subset \langle f \rangle$; samoin $g \mid f \Leftrightarrow \langle f \rangle \subset \langle g \rangle$.

c) $\Rightarrow$ a). $g = u \cdot f$, $u \in R[x]^* \Rightarrow f \mid g$ ja $f = u^{-1} \cdot g$, joten myös $g \mid f$.

a) $\Rightarrow$ c). Ol. $g = f \cdot h_1$, $f = g \cdot h_2$ $(h_1, h_2 \in R[x])$. Jos $g = 0$, niin myös $f = 0$, ja väite pätee. Ol. $g \neq 0$. $g \cdot 1 = g = f \cdot h_1 = (g \cdot h_2)\cdot h_1 = g \cdot (h_2 h_1)$

$\Rightarrow \quad 1 = h_2 h_1 \quad (R[x] \text{ kok. alue})$

$\Rightarrow \quad h_1, h_2 \in R[x]^* = R^* \qquad \square$

Lause 14 (Polynomien jakoyhtälö): Ol. R komm. rengas ja $f = f_0 + f_1 x + \ldots + f_m x^m \in R[x]$, $g = g_0 + g_1 x + \ldots + g_n x^n \in R[x]$, $n = \deg(g) \in \mathbb{N}$ ($\Leftrightarrow g_n \neq 0$). Jos $g_n \in R^*$, niin on olemassa yksikäsitteiset $q, r \in R[x]$ s.e.

$$f = q \cdot g + r \quad \text{ja} \quad \deg(r) < \deg(g) \ (= n).$$

Tod.: Olem.olo tod. induktiolla luvun $\deg(f)$ suhteen. Jos $\deg(f) < \deg(g)$, väit. val. $q = 0$, $r = f$.

Olk. sitten $\deg(f) = m \geq n = \deg(g)$ ($\Leftrightarrow f_m \neq 0$).

Ind. ol.: jos $f' \in R[x]$, $\deg(f') < m$, niin $\exists\, q', r' \in R[x]$ s.e. $f' = q' \cdot g + r'$ ja $\deg(r') < \deg(g)$. Koska

$$f_m g_n^{-1} x^{m-n} \cdot g = f_m g_n^{-1} g_0 x^{m-n} + \ldots + \underbrace{f_m g_n^{-1} g_n x^{m-n} \cdot x^n}_{= f_m x^m},$$

on $\deg(f - f_m g_n^{-1} x^{m-n} \cdot g) < m$; ind. ol. $\Rightarrow \exists\, q', r' \in R[x]$ s.e.

$$f - f_m g_n^{-1} x^{m-n} \cdot g = q' \cdot g + r' \quad \text{ja} \quad \deg(r') < \deg(g).$$

Merk. $q = q' + f_m g_n^{-1} x^{m-n}$, $r = r'$; tällöin on $f = q \cdot g + r$ ja $\deg(r) < \deg(g)$.

Yksikäs.: Ol. $f = q \cdot g + r = q' \cdot g + r'$, missä $q, q', r, r' \in R[x]$ ja $\deg(r) < \deg(g)$, $\deg(r') < \deg(g)$.

V. $q = q'$.

T. Vastaol.: $q \neq q' \Rightarrow q - q' \neq 0$, $q - q' = a_0 + a_1 x + \ldots + a_k x^k$, $k \in \mathbb{N}$, $a_k \neq 0 \Rightarrow$

$$r' - r = (f - q' \cdot g) - (f - q \cdot g) = (q - q') \cdot g = a_0 g_0 + (a_0 g_1 + a_1 g_0) x + \ldots + a_k g_n x^{k+n}$$

Tässä $a_k g_n \neq 0$ (sillä $a_k g_n = 0 \Rightarrow a_k = (a_k g_n) \cdot g_n^{-1} = 0 \cdot g_n^{-1} = 0$, RR) $\Rightarrow \deg(r' - r) = k + n \geq n$.

Toisaalta $\deg(r' - r) \leq \max\{\underbrace{\deg(r')}_{<n}, \underbrace{\deg(r)}_{<n}\} < n$, RR. $\square$

Näin ollen myös $r = f - q \cdot g = f - q' \cdot g = r'$. $\square$

Huom.: a) Jakoyht. oletukset ovat voimassa, jos $R = K$ on kunta ja $f, g \in K[x]$, $g \neq 0$ ($g_n \in K \setminus \{0\} = K^*$).

b) Ehto $g_n \in R^*$ on välttämätön: Val. $f = x \in \mathbb{Z}[x]$, $g = 2 \in \mathbb{Z}[x]$. Jos $f = q \cdot g + r$, $q, r \in \mathbb{Z}[x]$, $\deg(r) < \deg(g) = 0$, niin $r = 0$, $f = q \cdot g$ ja $1 = f(1) = q(1) \cdot g(1) = q(1) \cdot 2$, ts. $2 \mid 1$ $\mathbb{Z}$:ssä, RR.

c) Seuraus myös käytännön laskumenetelmää q:n ja r:n löytämiselle ("jako jakokulmassa"): jos $m \geq n$, lasketaan $f_m x^m / g_n x^n = f_m g_n^{-1} \cdot x^{m-n}$, ja korvataan f polynomilla $f - f_m g_n^{-1} \cdot x^{m-n} \cdot g$.

Esim. $\mathbb{Z}_2[x]$:ssä on

$$\begin{array}{rl} x^4 + x^2 + 1 & \mid\, x+1 \\ \hline -x^4 - x^3 & \\ \hline x^3 + x^2 & \\ -x^3 - x^2 & \\ \hline 1 & \end{array} \qquad \begin{array}{l} x^3 + x^2 \\ \hline \end{array}$$

$\therefore\ x^4 + x^2 + 1 = (x^3 + x^2)(x+1) + 1$ renkaassa $\mathbb{Z}_2[x]$.

Alkio $c \in R$ on polynomin $f \in R[x]$ nollakohta (R:ssä), jos f:n arvo c:ssä $f(c) = 0$.

Lause 15: Ol. R komm. rengas, $f \in R[x]$, $c \in R$. Tällöin c on f:n nollakohta $\Leftrightarrow$ $(x-c) \mid f$.

Tod.: $\Leftarrow$: $f = (x-c) \cdot g$, $g \in R[x]$ $\Rightarrow$ $f(c) = (c-c) \cdot g(c) = 0$.

$\Rightarrow$: Ol. $f(c) = 0$. Koska $(x-c)$:n johtava kerroin $1 \in R^*$, jakoyhtälö $\Rightarrow$ $\exists\, q, r \in R[x]$ s.e. $f = q \cdot (x-c) + r$ ja $\deg(r) < \deg(x-c) = 1$. Siispä $r \in R$ on vakio, ja $r = r(c) = (f - q \cdot (x-c))(c)$ $= f(c) - q(c) \cdot (c-c) = f(c) = 0$. $\therefore f = q \cdot (x-c)$. □

Esim. 1 (jatkoa): $(x+1) \mid (x^2+1)$ $R[x]$:ssä $\Leftrightarrow$ -1 on polynomin $x^2+1 \in R[x]$ nollakohta $\Leftrightarrow$ $(-1)^2 + 1 = 0$ R:ssä $\Leftrightarrow$ $2\ (= 1+1) = 0$ R:ssä.

Seuraus: R kokonaisalue, $f \in R[x]$, $\deg(f) = n \geq 0$ ($\Rightarrow f \neq 0$) $\Rightarrow$ f:llä on korkeintaan n nollakohtaa.

Tod.: Olkoot $c_1, c_2, \ldots, c_k \in R$ f:n eri nollakohtia. $f(c_1) = 0 \Rightarrow (x-c_1) \mid f$ (Lause 15) $\Rightarrow f = (x-c_1) \cdot f_1$ eräällä $f_1 \in R[x]$. Edelleen $0 = f(c_2) = (c_2 - c_1) \cdot f_1(c_2)$; $c_2 - c_1 \neq 0$, R kok. alue $\Rightarrow$ $f_1(c_2) = 0$ $\Rightarrow$

$(x-c_2) \mid f_1 \Rightarrow (x-c_1)(x-c_2) \mid f$. Jatkamalla nähdään, että $(x-c_1)\cdot\ldots\cdot(x-c_k) \mid f$; $f = (x-c_1)\cdot\ldots\cdot(x-c_k)\cdot g$ eräällä $g \in R[x]$, ja siten

$$n = \deg(f) = \deg(x-c_1) + \ldots + \deg(x-c_k) + \deg(g) \quad (R \text{ kok. alue})$$
$$= k + \deg(g) \geq k. \quad \square$$

Huom.: Yo. todistuksessa näkyi siis, että jos R on kok. alue ja polynomilla $f \in R[x]$ on eri nollakohdat $c_1, \ldots, c_k \in R$, niin $(x-c_1)\cdot\ldots\cdot(x-c_k) \mid f$.

Esim. 4: Ol. p alkuluku, $f = x^{p-1} - 1 \in \mathbb{Z}_p[x]$.
Fermat $\Rightarrow$ $1, 2, 3, \ldots, p-1 \in \mathbb{Z}_p$ ovat f:n nollakohtia
$\Rightarrow$ $(x-1)(x-2)\cdot\ldots\cdot(x-(p-1)) \mid f$ $\mathbb{Z}_p[x]$:ssä;
$f = x^{p-1} - 1 = a\cdot(x-1)(x-2)\cdot\ldots\cdot(x-(p-1))$ $\mathbb{Z}_p[x]$:ssä, missä $\deg(a) = 0$, ts. $a \in \mathbb{Z}_p \setminus \{0\}$ on vakio. f:n johtava kerroin $= 1 \Rightarrow a = 1 \Rightarrow$

$$f = x^{p-1} - 1 = (x-1)(x-2)\cdot\ldots\cdot(x-(p-1)) \in \mathbb{Z}_p[x].$$

Lask. arvot alkiolla $0 \in \mathbb{Z}_p$: $-1 = f(0) = (-1)\cdot(-2)\cdot\ldots\cdot(-(p-1))$
$= (-1)^{p-1}\cdot(p-1)! = (p-1)! \in \mathbb{Z}_p$ $((-1)^{p-1} = 1 \in \mathbb{Z}_p)$. Siis:

Lause (Wilson): $(p-1)! \equiv -1 \pmod p$, kun p on alkuluku. $\square$

Ed. seurauksesta saadaan

Seuraus: R ääretön kok. alue, $f, g \in R[x]$, $f(c) = g(c)$ $\forall c \in R$ (ts. f:ään ja g:hen liittyy sama polynomikuvaus $R \to R$) $\Rightarrow$ $f = g$.

Tod.: Vastaol. $f \neq g \Rightarrow h = f - g \neq 0$. Ed. seur. $\Rightarrow$ h:lla on vain äärell. monta nollakohtaa $c_1, c_2, \ldots, c_k \in R$ $(k \geq 0)$. R ääretön $\Rightarrow$ $\exists\, c_0 \in R$ s.e. $c_0 \neq c_i$ $\forall i \geq 1$. Tällöin $h(c_0) \neq 0$ eli $f(c_0) \neq g(c_0)$. $\square$

Huom.: Äskeinen pätee ent., kun $R = \mathbb{R}$. Sen vuoksi analyysissä (esim. Anal. I) voidaan samastaa polynomit $\in \mathbb{R}[x]$ ja polynomikuvaukset $\mathbb{R} \to \mathbb{R}$.

Jatkossa tark. polynomirengasta $K[x]$, K kunta.

Lause: $K[x]$:n jokainen ideaali on pääideaali

Tod.: Ol. $I \subset K[x]$ ideaali. Os., että $I = \langle g \rangle$ on g:n virittämä pääideaali sopivalla $g \in K[x]$.

Jos $I = \{0\}$, $I = \langle 0 \rangle$ ja ana on selvä. Siis void. ol. $I \neq \{0\}$ $\Rightarrow$ $\mathbb{N}$:n osajoukko $A = \{\deg(f) \mid f \in I, f \neq 0\}$ on $\neq \emptyset$. Merk. $d = \min A \in \mathbb{N}$, ja val. $g \in I$, $g \neq 0$, s.e. $\deg(g) = d$.

V. $I = \langle g \rangle$.

T. $g \in I \Rightarrow \langle g \rangle \subset I$.

Käänteen, ol. $f \in I$. Jakoyht. $\Rightarrow$ $\exists\, q, r \in K[x]$ s.e. $f = q \cdot g + r$ ja $\deg(r) < \deg(g) = d$. I ideaali, $f, g \in I$ $\Rightarrow$ $r = f - q \cdot g \in I$. Jos olisi $r \neq 0$, niin $\deg(r) \in A$, vaikka $\deg(r) < d = \min A$, RR. Siis $r = 0$ ja $f = q \cdot g \in \langle g \rangle$.

$\therefore I \subset \langle g \rangle$. $\square$

Ol. $f, g \in K[x]$. Tark. $K[x]$:n ideaalia $\langle f \rangle + \langle g \rangle = \{u \cdot f + v \cdot g \mid u, v \in K[x]\}$. Ed. lause $\Rightarrow$ $\exists\, d \in K[x]$ s.e.

$$\langle f \rangle + \langle g \rangle = \langle d \rangle \quad (= \{w \cdot d \mid w \in K[x]\}).$$

Tällöin: 1) $f, g \in \langle f \rangle + \langle g \rangle = \langle d \rangle \Rightarrow d \mid f$ ja $d \mid g$; siis d on f:n ja g:n yhteinen tekijä, ja

2) $d \in \langle d \rangle = \langle f \rangle + \langle g \rangle \Rightarrow d = u \cdot f + v \cdot g$ eräillä $u, v \in K[x]$; jos $e \in K[x]$ on jokin f:n ja g:n yht. tekijä, ts. $e \mid f$ ja $e \mid g$, on siis $e \mid d$.

$\therefore$ d on f:n ja g:n (eräs) suurin yhteinen tekijä $K[x]$:ssä, merk. $d = syt(f, g)$.

Huom.: d ei ole (aivan) 1-käsitteinen, sillä $\langle d \rangle = \langle d' \rangle \Leftrightarrow \exists$ vakio $a \in K \setminus \{0\}$ s.e. $d' = a \cdot d$. Jos $d \neq 0$, ja d valitaan niin, että johtava kerroin $= 1$ (ts. d on pääpolynomi), d on 1-käs.

Yo. mukaan $d = syt(f, g)$ $K[x]$:ssä $\Rightarrow$ $\exists\, u, v \in K[x]$ s.e. $d = u \cdot f + v \cdot g$; erityisesti $1 = syt(f, g)$ (eli f ja g ovat keskenään jaottomat) $\Leftrightarrow$ $\exists\, u, v \in K[x]$ s.e. $1 = u \cdot f + v \cdot g$.

Kuten kok.-lukujen tapauksessa, $syt(f,g) \in K[x]$ (ja jotkin u, v kuten yllä) voidaan etsiä Euklideen algorithmilla, so. soveltamalla täsmennystä jakoyhtälöä

Esim.: Olk. $f = x^4+x^2+x \in \mathbb{Z}_2[x]$, $g = x^2+x+1 \in \mathbb{Z}_2[x]$. Etsi $syt(f,g)$ $\mathbb{Z}_2[x]$:ssä ja esitä se muodossa $u \cdot f + v \cdot g$ sopivilla $u, v \in \mathbb{Z}_2[x]$.

Ratk.: $f = (x^2+x+1)\cdot g + (x+1)$
$g = x(x+1) + 1$
$\Rightarrow 1 = syt(f,g)$. Edelleen
$x+1 = f + (x^2+x+1)\cdot g$,
$1 = g + x(x+1) = g + x\cdot(f + (x^2+x+1)\cdot g)$
$= x\cdot f + (x^3+x^2+x+1)\cdot g$. □

Polynomi $f \in K[x]$ on jaoton, jos f ei ole vakio (ts. $\deg(f) > 0$) ja f:llä ei ole tekijöitä $g \in K[x]$ s.e. $0 < \deg(g) < \deg(f)$.
Siis f ei jaoton $\Leftrightarrow$ f vakio tai $f = g\cdot h$, missä $g, h \in K[x]$ ja $\deg(g) > 0$, $\deg(h) > 0$.

Lause: Ol. $f \in K[x]$.
a) $\deg(f) = 1 \Rightarrow f$ jaoton
b) $\deg(f) > 1$, f:llä nollakohta $c \in K$
$\Rightarrow f$ ei jaoton.
c) Jos $\deg(f) = 2$ tai 3, niin f on jaoton
$\Leftrightarrow$ f:llä ei ole nollakohtia K:ssa.

Tod.: a) $f = g\cdot h \Rightarrow 1 = \deg(f) = \deg(g) + \deg(h)$
$\Rightarrow \deg(g) = 0$ tai $\deg(h) = 0$.
b) Ol. $f(c) = 0$. Lause 15 $\Rightarrow (x-c) \mid f$;
$f = (x-c)\cdot g \Rightarrow 1 + \deg(g) = \deg(x-c) + \deg(g) =$
$= \deg(f) > 1 \Rightarrow \deg(g) > 0$. $\therefore f$ ei jaoton.
c) $\Rightarrow$: jos f:llä on nollakohta, niin b) $\Rightarrow f$ ei jaoton.
$\Leftarrow$: Ol. f ei jaoton, ts. $f = g\cdot h$, $\deg(g) \geq 1$, $\deg(h) \geq 1$.
$\deg(g) + \deg(h) = \deg(f) = 2$ tai $3 \Rightarrow \deg(g) = 1$ tai $\deg(h) = 1$. Olk. esim. $g = g_0 + g_1 x$, $g_1 \neq 0$.
Silloin $f(-g_0/g_1) = \underbrace{g(-g_0/g_1)}_{=0}\cdot h(-g_0/g_1) = 0$
$\Rightarrow -g_0/g_1 \in K$ on f:n nollakohta. □

Huom.: jos $\deg(f) \geq 4$, nollakohtien puuttuminen ei takaa f:n jaottomuutta; esim. $\mathbb{R}[x]$: sillä on
$x^4 + 1 = (x^2 - \sqrt{2}\cdot x + 1)\cdot(x^2 + \sqrt{2}\cdot x + 1)$.

Esim.: a) $f = x^3 + x + 1 \in \mathbb{Z}_2[x]$ on jaoton, sillä
$f(c) = 1 \neq 0 \quad \forall c \in \mathbb{Z}_2$.

b) Olk. $f = x^3 + x + 1 \in \mathbb{Z}_3[x]$. $f(1) = 0 \Rightarrow$
$(x-1) \mid f$; $f = (x-1)(x^2 + x + 2)$. Merk. $g = x^2 + x + 2 \in \mathbb{Z}_3[x]$.
$g(0) = 2 \neq 0$, $g(1) = 4 = 1 \neq 0$, $g(2) = 8 = 2 \neq 0$
$\Rightarrow g$ on jaoton. Siis $f = (x-1)\cdot g = (x+2)(x^2+x+2)$
$\in \mathbb{Z}_3[x]$ jaott. pol. tulo.

c) $f = x^2 + 2x + 2 \in \mathbb{R}[x]$ jaoton, sillä $f(c) = (c+1)^2 + 1 > 0$
$\forall c \in \mathbb{R}$.

d) Pätee: $f \in \mathbb{C}[x]$ jaoton $\Leftrightarrow \deg(f) = 1$
(sillä Algebran peruslause $\Rightarrow$ jokaisella $f \in \mathbb{C}[x] \setminus \mathbb{C}$ on nollakohta $\in \mathbb{C}$).

K-kertoimisille polynomeille pätee Aritmetiikan peruslauseen (Lause I.5) vastine:

Lause: Jokainen ei-vakio $f \in K[x]$ voidaan tekijöiden järjestystä vaille 1-käsitteisesti esittää muodossa

$$f = u \cdot p_1 p_2 \cdots p_r,$$

missä $u \in K \setminus \{0\}$, ja $p_1, \ldots, p_r \in K[x]$ ovat jaottomia pääpolynomeja.

Tod.: Esityksen olem. olo tod. induktiolla $\deg(f)$:n suhteen. $\deg(f) = 1 \Rightarrow f$ jaoton, ana selvä (val. $u = f$:n johtava kerroin).

Ol. sitten $\deg(f) > 1$. Jos f on jaoton, ana on taas selvä. Muuten $f = g \cdot h$, $\deg(g) < \deg(f)$, $\deg(h) < \deg(f)$.
Ind. ol. $\Rightarrow g = u' \cdot p_1' \cdots p_{r'}'$, $h = u'' \cdot p_1'' \cdots p_{r''}''$
$\Rightarrow f = g \cdot h = (u'u'') \cdot p_1' \cdots p_{r'}' \cdot p_1'' \cdots p_{r''}''$.

1-käs. tod. kuten kok. luvuilla; ensin apulause
$p \in K[x]$ jaoton, $p \mid (g \cdot h) \Rightarrow p \mid g$ tai $p \mid h$. $\square$

VI. 8. Eräitä muita kuntia

Olk. K kunta, $p \in K[x]$ jaoton pääpolynomi.
p ei nolla $\Rightarrow \deg(p) = n \in \mathbb{N}_+$ (siis $n \geq 1$);
$p = p_0 + p_1 x + \dots + p_{n-1} x^{n-1} + x^n$, $p_0, \dots, p_{n-1} \in K$.
Merk.

$$I = \langle p \rangle = \{ h \cdot p \mid h \in K[x] \}$$

p:n virittämä $K[x]$:n pääideaali.

Lemma: $K[x]/I$ on kunta.

Tod.: jokin tapauksessa $K[x]/I$ on komm. rengas.
$\deg(p) \geq 1 \Rightarrow p \neq 1 \Rightarrow 1 \notin I \Rightarrow 1 + I \neq 0 + I$
$\Rightarrow K[x]/I \neq \{0 + I\}$.
Olk. $f + I \in K[x]/I$ $(f \in K[x])$, $f + I \neq 0 + I$
$\Rightarrow f \notin I \Rightarrow p \nmid f$. Koska p on jaoton, tästä seuraa, että $\operatorname{syt}(f, p) = 1$ (ts. f ja p ovat kesk. jaottomat) $\Rightarrow \exists g, h \in K[x]$ s.e. $f \cdot g + h \cdot p = 1$. Tällöin

$$(f+I) \cdot (g+I) = (fg) + I = (fg + hp) + I \overset{\psi}{=} 1 + I$$

$\Rightarrow f + I \in (K[x]/I)^*$, $g + I = (f+I)^{-1}$. $\square$

Merk. $L = K[x]/I$, $\pi : K[x] \to L$ kan. sur.,
$i : K \hookrightarrow K[x]$ kan. inj. Tällöin $j = \pi \circ i : K \to L$,
$j(a) = a + I$ $\forall a \in K$, on kuntahomom., ent. injektio.
Samastetaan j:n välityksellä K ja $\operatorname{Im}(j) \subset L$
(ts. tulkitaan a "$=$" $j(a) = a + I \in L$ $\forall a \in K$). Tällöin
K on L:n alikunta, ja L K:n laajennus.
Kun $f \in K[x]$, niin jakoyht. $\Rightarrow \exists$ 1-kert. $h, r \in K[x]$ s.e. $f = h \cdot p + r$ ja $\deg(r) < \deg(p) = n$;
tästä $h \cdot p \in I$, joten $f + I = r + I$.

$$\therefore \quad L = \{ r + I \mid r \in K[x],\ \deg(r) \leq n-1 \}.$$

Lisäksi r:n 1-kert. $\Rightarrow$ jos $r + I = r' + I$, niissä $\deg(r) \leq n-1$ ja $\deg(r') \leq n-1$, niin $r = r'$.

Merk. $\omega = x + I \in L$. Olk. $r = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in K[x]$ $(a_0, \ldots, a_{n-1} \in K)$. Silloin

$$\begin{aligned} r + I &= (a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}) + I \\ &= (a_0 + I) + (a_1 + I)\cdot(x + I) + \ldots + (a_{n-1} + I)\cdot(x + I)^{n-1} \\ &= a_0 + a_1 \omega + \ldots + a_{n-1} \omega^{n-1} \end{aligned}$$

(kun samast. $a = a + I$ $\forall a \in K$ kuten yllä). Näin ollen pkaisella $\alpha \in L$ on 1-käs. esitys

$$\alpha = a_0 + a_1 \omega + \ldots + a_{n-1} \omega^{n-1} \; ; \; a_0, a_1, \ldots, a_{n-1} \in K$$

(siis $(1, \alpha, \ldots, \alpha^{n-1})$ on K-vektoriavaruuden L kanta).

Tässä esitysmuodossa yhteenlasku on helppoa:

$$\left(\sum_{i=0}^{n-1} a_i \omega^i\right) + \left(\sum_{i=0}^{n-1} b_i \omega^i\right) = \sum_{i=0}^{n-1} (a_i + b_i)\, \omega^i .$$

Kertolasku: $\left(\sum_{i=0}^{n-1} a_i \omega^i\right) \cdot \left(\sum_{j=0}^{n-1} b_j \omega^j\right) = \sum_{k=0}^{2n-2} \left(\sum_{i+j=k} a_i b_j\right) \omega^k ;$

tämä voidaan saattaa muotoon $\sum_{i=0}^{n-1} c_i \omega^i$ (ts. päästä eroon potensseista ω^k, $k > n-1$) käyttäen "relaatiota"

$$\omega^n = -p_0 - p_1 \omega - \ldots - p_{n-1} \omega^{n-1} .$$

(Tod.: $p_0 + p_1 \omega + \ldots + p_{n-1} \omega^{n-1} + \omega^n = (p_0 + I) + (p_1 + I)\cdot(x + I) + \ldots$
$\ldots + (p_{n-1} + I)\cdot(x + I)^{n-1} + (x + I)^n = (p_0 + p_1 x + \ldots + p_{n-1} x^{n-1} + x^n) + I$
$= p + I = 0 + I$, koska $p \in I$. $\square$)

$p \in K[x]$ jaoton $\Rightarrow$ p:llä ei ole nollakohtia K:ssa (jos $n > 1$). $K \subset L$ aiheuttaa $\Rightarrow$ $K[x] \subset L[x]$ aiheuttaa. Sitten void. tulkita, että $p \in L[x]$.

V. $\omega \in L$ on p:n nollakohta laajennuksessa L.
T. $p(\omega) = p_0 + p_1 \omega + \ldots + p_{n-1} \omega^{n-1} + \omega^n = 0 + I$, kuten yllä jo laskettiin. $\square$

Esim. 1: $K = \mathbb{R}$, $p = x^2 + 1 \in \mathbb{R}[x]$ (jaoton, koska $p(c) \neq 0$ $\forall c \in \mathbb{R}$), $I = \langle p \rangle \subset \mathbb{R}[x]$, $L = \mathbb{R}[x]/I$, $\omega = x + I \in L \Rightarrow \omega^2 = -1$, $L = \{a_0 + a_1 \omega \mid a_0, a_1 \in \mathbb{R}\}$.
Tässä

$$a_0 + a_1 \omega = b_0 + b_1 \omega \iff a_0 = b_0 \text{ ja } a_1 = b_1 ,$$

$$(a_0+a_1\omega)+(b_0+b_1\omega) = (a_0+b_0)+(a_1+b_1)\omega,$$
$$(a_0+a_1\omega)\cdot(b_0+b_1\omega) = (a_0b_0)+(a_0b_1+a_1b_0)\omega +$$
$$+(a_1b_1)\omega^2 = (a_0b_0-a_1b_1)+(a_0b_1+a_1b_0)\omega.$$

Kun merk. $\omega = i$ ("imaginaariyksikkö"), näkidään, että $L = \mathbb{C}$, kompleksilukujen kunta.

Huom.: jos yllä K on äärellinen, niin samoin on L, ja $|L| = |K|^n$. jos erim. $K = \mathbb{Z}_q$ (q alkuluku), niin $|L| = q^n$.

Esim. 2: $K = \mathbb{Z}_2$, $p = 1+x+x^2 \in \mathbb{Z}_2[x]$ (jaoton, koska $p(\bar{0}) = \bar{1} \neq \bar{0}$ ja $p(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$), $I = \langle p \rangle \subset \mathbb{Z}_2[x]$, $L = \mathbb{Z}_2[x]/I$, $\omega = x+I \in L$
$\Rightarrow \omega^2 = 1+\omega \quad (= -1-\omega)$, $L = \{a_0+a_1\omega \mid a_0, a_1 \in \mathbb{Z}_2\} =$
$= \{0, 1, \omega, 1+\omega\}$ 4-alkioinen kunta. Laskutoim.:

$$(a_0+a_1\omega)+(b_0+b_1\omega) = (a_0+b_0)+(a_1+b_1)\omega,$$
$$(a_0+a_1\omega)\cdot(b_0+b_1\omega) = (a_0b_0)+(a_0b_1+a_1b_0)\omega +$$
$$+(a_1b_1)\cdot\omega^2 = (a_0b_0+a_1b_1)+(a_0b_1+a_1b_0+a_1b_1)\omega.$$

jos q on alkuluku, ja löydetään jaoton $p \in \mathbb{Z}_q[x]$ s.e. $\deg(p) = n \in \mathbb{N}_+$, niin saadaan q^n-alkioinen kunta L.

Pätee: jos q on alkuluku ja $n \in \mathbb{N}_+$, niin on olem. (isom. vaille) 1-käs. q^n-alkioinen kunta $GF(q^n)$. Kääntäen, jos L on äärell. kunta, niin $\mathrm{char}(L) \neq 0$ (muuten $\mathbb{Q} \subset L$); $\mathrm{char}(L) = q$ alkuluku, ja tällöin $|L| = q^n$ jollakin $n \in \mathbb{N}_+$.