3.2 Polynomialgebra

Edellisessä luvussa törmättiin polynomifunktioihin ja polynomiyhtälöihin kunnan yli luonnollisella tavalla, nimittäin tutkimalla kuvauksen ominaisarvoja. Tämä antaa meille hyvän syyn tutkia polynomeja yleisesti (muitakin syitä löytyy).

Tähän asti olemme käsitteleet polynomeja yksinkertaisesti **funktioina** $K \to K$, joilla on tietty muoto. Nykyalgebrassa kuitenkin preferoidaan abstraktimpi ja algebrallisempi tapaa ajatella polynomit.
Määritelmän mukaan *polynomifunktio* kunnassa K on kuvaus $p\colon K \to K$ jonka voi kirjoittaa muodossa

$$p(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$$

joillakin $c_0, \ldots, c_n \in K$ (joita sanotaan p *kertoimiksi*, $c_n \neq 0$. Tällaisen polynomin aste on n (toki yleisemmin voimme puhua polynomista renkaassa R, mutta rajotutaan tässä kunta-tapaukseen). Haluasimme, että polynomin kertoimet määräytyisivät sen yksikäsitteisesti, jolloin olisimme voineet identifioida p sen kertoimien jonon $(c_0, \ldots, c_n) \in K^n$ kanssa. Valitettavasti tämä ei aina pidä paikkansa - erilaiset polynomilauseekkeet voivat määritellä saman kuvauksen. Esimerkiksi olkoon $K = \{x_0, \ldots, x_n\}$ jokin *äärellinen* kunta, $n \geq 1$, esimerkiksi $\mathbb{Z}_p$ (missä p alkuluku). Tällöin polynomifunktio $p\colon K \to K$,

$$p(x) = (x - x_0)(x - x_1)\ldots(x - x_n)$$

on polynomilausekkena $(n+1)$-asteinen polynomi, mutta kuvauksena onkin nollakuvaus. Nähdään, että tässä tapauksessa polynomikuvauksen aste ei ole edes hyvinmääritelty - se riippuu siitä, miten kuvaus esitetään polynomilausekkeena. Itse asiassa, jos K on äärellinen, on selvää, että erilaisia kuvauksia $f\colon K \to K$ on vain äärellinen määrä, mutta erinäköisiä *polynomilausekkeita* on pakko olla ääretön määrä - ainakin yksi jokaisella $n \in \mathbb{N}$ (kuvaus $x \mapsto x^n$).
Voidaan osoittaa (harjoitustehtävä), että äärettömän kunnan tapauksessa näin ei voi käydä - jos K on ääretön, niin kaksi polynomikuvausta $p, q\colon K \to K$ ovat kuvauksina samat jos ja vain jos niillä on sama aste ja samat kertoimet.

Polynomikuvaukset, jonka kertoimet ovat kunnan K alkiot yleistyvät luonnollisella ja ja tuottoisalla tavalla *K-algebroihin*. Tämän näkökulman kautta päädytään luonnollisella tavalla algebrallisen abstraktiin polynomiin käsitteseen.

K-Algebrat.
Palautetaan mieleen, että K-algebra A on K-vektoriavaruus, jossa on määritelty myös kertolasku $\cdot\colon A \times A \to A$, joka on K-bilineaarinen kuvaus ja laskutoimituksena assosiatiivinen. Bileneaarisuus-ehto tarkoittaa tasan sitä, että

$$(a+b)\cdot c = a\cdot c + b\cdot c,$$

$$a\cdot(b+c) = a\cdot b + a\cdot c,$$

$$(ka)b = a(kb) = k(ab)$$

kaikilla $a, b, c \in A, k \in K$. Kaksi ensimmäistä ehtoa (muiden algebran ehtojen kanssa) takaavat silloin, että $(A, +, \cdot)$ on rengas. Algebra on siis samanaikaan vektoriavaruus ja rengas. Yleensä käsittelemme vain *ykkösellisiä* algebroja, joissa kertolaskulla on neutraalialkio $1 \in A$. Algebran kertolasku ei ole vältämättä vaihdannainen. Jos se on, puhumme *vaihdannaisesta algebrasta*.
Aina kun törmätään uudenlaiseen algebralliseen struktuuriin, luonnollisiksi nousevat kysymykset mikä on tämäntyyppisiin struktuurien välinen morfismi, mikä on alistruktuuri ja miten saadaan tekijästruktuurit konstruoitua. Olkoot A, B K-algebrat. Kuvaus $f\colon A \to B$ on K-algebrojen homomorfismi, jos se on K-lineaarinen A:n ja B:n K-vektoriavaruuden suhteen ja säilyttää kertolaskun, toisinsanoen on lisäksi rengashomomorfismi $f\colon (A, +, \cdot) \to (B, +, \cdot)$, kun unohdetaan skalaarikertolaskua.
K-Algebran A osajoukko B on K-alialgebra, jos se on K-vektoriavaruuden A aliavaruus ja renkaan A alirengas. Algebran *ideaali* on sellainen renkaan A ideaali, joka on myös aliavaruus K-vektoriavaruuden suhteen. Jos I on A:n ideaali, niin voimme muodostaa *tekijäalgebran* A/I. Yleisen teorian (kts. Luku 1) nojalla A/I on sekä K-vektoriavaruus (jos käsitellään A vektoriavaruutena), että rengas (jos A ajatellaan renkaana). Helposti verifioidaan, että kun A/I varustetaan indusoinneilla K-vektoriavaruuden ja renkaan struktuureilla, yhdessä ne todellakin muodostavat K-algebran (pitää tarkistaa vain, että indusoitu kertolasku on K-bilineaarinen, harjoitustehtävä).
Olkoon $f\colon A \to B$ (ykkösellisten) algebrojen homomorfismi. Tällöin yleisen teorian (kts. Luku 1) mukaan $\operatorname{Ker} f$ on A:n ideaali, $\operatorname{Im} f$ on B:n alialgebra ja isomorfialauseen nojalla f indusoi algebraisomorfismin $A/\operatorname{Ker} f \cong B$. Yleisemmin hajotelmalause takaa, että jos I on A:n ideaali jolle $I \subset \operatorname{Ker} f$, niin f indusoi agebrahomomorfismin $\bar{f}\colon A/I \to B$.

Oletetaan, että A on ykkösellinen K-algebra. Määritelemme kuvauksen $\phi\colon K \to A$ kaavalla $\phi(k) = k \cdot 1$, missä $\cdot$ tarkoittaa skalaarituloa. Helposti nähdään, että ϕ on K-algebrojen välinen homomorfismi (harjoitustehtävä). Tässä siis ajattelemme K itse K-algebrana ilmeisella tavalla. Itse asiassa ϕ

on jopa injektio, eli upotus, sillä vektoriavaruuden supistusääntö takaa sen, että $k \cdot 1 = k' \cdot 1$ jos ja vain jos $k = k'$. Tästä syystä **samastamme** K:n alkio k A:n alkion $\phi(k)$ kanssa ja puhumme siis algebran A alkiosta k.

Olkoon $x \in A$, missä A on jokin ykkösellinen K-algebra. Mietitään mikä on pienin A:n (ykkösellinen) K-aliagebra $K[x]$, joka sisältää x:n, eli x:n virittämä alialgebra. Koska sen täytyy olla ykkösellinen alistruktuuri, sen täytyy sisältää x:n lisäksi ainakin alkion $1 \in A$. Koska se on algebra, eli suljettu kertolaskun suhteen, sen täytyy sisältää lisäksi kaikki x:n potenssit x^n, $n \in \mathbb{N}$ (tapaus $n = 0$ vastaa alkiota 1). Toisaalta, koska $K[x]$:n täytyy olla vektoriaaliavaruus A:ssä, se on suljettu skalaarikertolaskun suhteen, joten se sisältää myös kaikki muotoa kx^n olevat alkiot, $k \in K$, $n \in \mathbb{N}$. Lopuksi, koska se on suljettu myös yhteenlaskun suhteen, sen täytyy sisältää kaikkien tällaista muotoa olevien alkioiden summat, eli mielivaltaiset **polynomilausekkeet**

$$c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0,$$

joissa kertoimet $c_0, \ldots, c_n \in K, c_n \neq 0$. Määritelemme A:ssa kuvauksen $p\colon A \to A$ kaavalla

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0.$$

Tälläinen kuvaus sanotaan algebran A K-kertoimiseksi *polynomikuvauksek-si* ja se on siis suora yleistys edellä tarkasteltuvasta polynomikuvauksesta $p\colon K \to K$ kunnassa K.
Olemme näyttäneet, että alialgebra $K[x]$ sisältää kaikki muotoa $p(x)$ olevia lausekkeita, missä p on K-kertoiminen polynomi A:ssä. Nämä riittää ja tähän voidaan lopettaa, sillä kääntäen voidaan osoittaa, että kääntäen jokainen $K[x]$:n alkio on tätä muotoa. Saamme siis seuraavan tuloksen, jonka todistus jää lukijalle harjoitustehtäväksi.

Lemma 3.15. *Olkoon A (ykkösellinen) K-algebra ja $x \in A$. Tällöin x:n virittämä alialgebralle $K[x]$ pätee*

$$K[x] = \{p(x) \mid p\colon A \to A \text{ on } K\text{-kertoiminen polynomi}\}.$$

Esimerkiksi $\mathbb{C}$ on $\mathbb{R}$-algebra. Polynomikuvauksen $p(x) = x^2 + 1$ voimme ajatella polynomina $p\colon \mathbb{R} \to \mathbb{R}$ tai polynomina $\mathbb{C} \to \mathbb{C}$. Riippuen siitä, missä joukossa tämä kuvaus tarkastellaan, se käyttäytyy eri tavalla - esim. $\mathbb{R}$:ssä se on *jaoton* mutta $\mathbb{C}$:ssä sillä on juuri ja voimme jakaa se tekijöihin, $x^2 + 1 = (x - i)(x + i)$. ”Polynomilausekkena” se on kuitenkin sama.

Koska K-kertoimisen polynomilausekkeen käyttäytyminen riippuu siitä, missä K-algebrassa se tarkastellaan, haluamme konstruoida abstraktin, "universaalin" polynomialgebran, johon kaikki mahdolliset polynomitilanteet voidaan vertailla.

Polynomialgebran konstruuktio.

Ajatus on seuraava. Koska haluamme, että polynomin kertoimet määritelisivat sen yksikäsitteisesti, kutsumme K-kertoimiseksi (*algebralliseksi*) polynomiksi jono $(c_0, \ldots, c_n) \in K^n$, jollakin $n \in \mathbb{N}$. Koska haluamme tarkastella kaikkien mahdollisten asteiden olevia polynomia, n saa käydä läpi kaikki mahdolliset arvot $\mathbb{N}$:stä. Toisin sanoen meidän on tarkisteltavaa kaikki mahdolliset *äärellispituiset jonot*. Toisaalta voimme silloin yhtä hyvin käyttää kaikki *äärelliskantaiset* jonot!

Siirrymme nyt formaaliin konstruktioon, jonka idean pitäisi olla tässä vaiheessa jo hyvin selvä lukijalle. Olkoon K kunta. Muodostamme K-vektoriavaruus $K^{(\mathbb{N})}$, jonka alkiot ovat siis äärelliskantaiset jonot $(c_n)_{n\in\mathbb{N}}$ (huom., meille $0 \in \mathbb{N}$!). Proposition 2.79 nojalla tämä on vapaa, ääretönulotteinen K-vektoriavaruus, jolla on kanta $(e_n)_{n\in\mathbb{N}}$. Tässä e_m on sellainen jono $(c_n)_{n\in\mathbb{N}}$, jolle $c_m = 1$ ja muut koordinaatit ovat nolleja. Koska tämä on kanta, määritelmän mukaan voimme kirjoittaa jokainen $K^{(\mathbb{N})}$ alkio muotoon

$$c_0e_0 + c_1e_1 + \ldots + c_ne_n$$

jollakin $n \in \mathbb{N}$, $c_0, \ldots, c_n \in K$, missä voimme olettaa, että $c_n \neq 0$. Tällainen esitys on yksikäsitteinen. Sanomme, että tällaisen alkion *aste* on n. Jonon $(c_n)_{n\in\mathbb{N}}$ aste on siis suurin $n \in \mathbb{N}$ jolle $c_n \neq 0$. Tällöin tama alkio c_n sanotaan f:n *johtavaksi kertoimeksi*. Jonon f aste merkitään $\deg f$. Se on määritelty kaikille $K^{(\mathbb{N})}$ alkioille, paitsi nollaalkiolle, jonka kaikki koordinaatit ovat nolleja. Tämä alkio sanotaan nollapolynomiksi ja asetetaan sen asteeksi $-\infty$ (eli miinus ääretön) teknisistä syistä.

Sanomme $K^{(\mathbb{N})}$:n alkiot K-kertoimisiksi (algebrallisiksi) polynomeiksi. Merkitään $K^{(\mathbb{N})} = K[X]$. Koska $K[X]$ on määritelmän mukaan K-vektoriavaruus, polynomit voi laskea yhteen ja kertoa K:n alkioilla. Haluamme myös kertoa polynomit keskenään, joten meidän on määriteltävää kertolasku joukossa $K[X]$.
Koska $(e_n)_{n\in\mathbb{N}}$ on $K[X]$:n kanta, Lauseen 2.80 nojalla on olemassa tasan yksi K-bilineaarinen kuvaus $\Phi\colon K[X] \times K[X] \to K[X]$, jolle $\Phi(e_n, e_m) = e_{n+m}$ kaikilla $n, m \in \mathbb{N}$. Merkitään $\Phi(f, g) = f \cdot g$, $\cdot$ on siis laskutoimitus joukossa $K[X]$. Kutsumme sitä polynomien kertolaskuksi. Määritelmästä seuraa (harjoitustehtävä), että jos $f = (a_n)$ ja $g = (b_n)$ ovat polynomeja, niin $f \cdot g$ on

polynomi (c_n), jolle

$$c_n = \sum_{k+l=n, k,l \in \mathbb{N}} a_k b_l$$

jokaisella $n \in \mathbb{N}$.

Lemma 3.16. *Polynomien kertolaskulla varustettuna $K[X]$ on ykkösellinen ja vaihdannainen K-algebra. Kertolaskun neutraalialkio on e_0.*

Todistus. Kuvaus Φ on konstruktioon perustella bilineaarinen, joten jäljellä on kertolaskun osoittaminen vaihdannaiseksi ja liitännäiseksi.
Tarkastellaan kuvaukset $\Psi_1 \colon K[X] \times K[X] \times K[X] \to K[X]$, $\Psi_2 \colon K[X] \times K[X] \times K[X] \to K[X]$, $\Psi_1(f,g,h) = (fg)h$, $\Psi_2(f,g,h) = f(gh)$. Kertolasku on assosiatiivinen jos ja vain jos $\Psi_1 = \Psi_2$. Helposti nähdään (tarkista!), että molemmat kuvaukset Ψ_1 ja Ψ_2 ovat 3-lineaariset. Koska $K[X]$ on vapaa moduli, Propositiosta 2.80 seuraa, että nämä kuvaukset ovat samat jos ja vain jos ne ovat samat, kun rajoidutaan kanta-alkioihin (e_n). Mutta kanta-alkioille assositivisuus pätee, sillä

$$\Psi_1(e_n, e_m, e_k) = e_{n+m}e_k = e_{(n+m)+k} = e_{n+(m+k)} = e_n e_{m+k} = \Psi_2(e_n, e_m, e_k).$$

Liitännäisyys on todistettu. Vaihdannaisuus todistetaan samalla tavalla - riittää huomata, että se pätee kanta-alkioille.
Algebran $K[X]$ neutraalialkio on kanta-alkio e_0. □

Algebraa $K[X]$ sanomme K:n *polynomialgebraksi*.
Koska e_0 on kertolaskun neutraalialkio, merkitsemme sen symbolilla 1. Alkio e_1 puolestaan merkitsemme symbolilla X. Induktiolla helposti nähdään, että

$$e_n = \underbrace{e_1 + \ldots + e_1}_{n \text{ kertaa}} = e_1^n = X^n$$

jokaisella $n \in \mathbb{N}$. Näin ollen voimme kirjoittaa jokainen (nollasta eroava) polynomi $f = (c_n)$ muotoon

$$f = c_0 + c_1 X + c_2 X^2 + \ldots + c_n X^n,$$

missä $n = \deg f$ yksikäsitteisellä tavalla. Näin päästään muotoon, joka näyttää samalta kuin vanha tuttu "polynomi". Tällä kertaa se ei kuitenkaan ole enää mikään kuvaus ja X ei ole mikään muuttuja.
Kuten yleensä algebrassa, määritelemme kuvausta $\phi \colon K \to K[X]$, $k \mapsto kX^0 = k$, missä $k \in K[X]$ on nolla-asteinen polynomi, jonka nollas komponentti on k. Sanomme tällaiset polynomit *vakiopolynomeiksi*. Tämä kuvaus on agrebrojen välinen homomorfismi, ja lisäksi injektio, joten voimme

identifioida $k \in K$ ja vastaava nolla-asteinen polynomi $k \in K[X]$. Ajatellemme siis kunta K polynomialgebransa $K[X]$ osajoukkona.

Olkoon A ykkösellinen K-algebra ja $p = (c_n)_{n\in\mathbb{N}}$ polynomialgebran alkio. Tällöin voimme määritellä sitä vastaava polynomikuvaus $p\colon A \to A$ (merkitsemme se samalla symbolilla) kaavalla

$$p(x) = \sum_{k=0}^{\deg p} c_k x^{\cdot}$$

Voimme ajatella, että ”sijoitamme” symbolin X paikalle algebran alkion x. Täsmällisemmin sama ajatus voidaan muotoilla polynomialgebran universaaliksi ominaisuudeksi.

Propositio 3.17. *Olkoon A ykkösellinen K-algebra ja $x \in A$ mielivaltainen. Tällöin on olemassa tasan yksi (ykkösellisten) K-algebrojen homomorfismi $S_x\colon K[X] \to A$ jolle $S_x(X) = x$. Kutsumme sitä* alkion x määrittelemäksi sijoitushomomorfismiksi. *Sille pätee $S_x(p) = p(x)$, kaikilla $p \in K[X]$.*

Todistus. Jos $S_x\colon K[X] \to A$ on ykkösellinen algebrahomomorfismi, jolle $S_x(X) = x$, niin $S_x(e_0) = S_x(1) = 1$ ja lisäksi induktiolla $S_x(e_n) = S_x(X^n) = x^n$. Koska S_x on erityisesti lineaarinen kuvaus, niin nämä arvot $K[X]$:n kannan alkiolle määrävät sen yksikäsitteisesti.
Kääntäen määritellään K-lineaarinen kuvaus $S_x\colon K[X] \to A$ asettamalla sen arvot kanta-alkiolla $S_x(e_n) = x^n$, jolloin siis erityisesti $S_x(1) = S_x(e_0) = x^0 = 1$ ja $S_x(X) = S_x(e_1) = x^1 = x$. Lemman 2.22 nojalla tällainen K-lineaarinen kuvaus on olemassa ja yksikäsitteinen.
Jäljellä on sen osoittaminen, että S_x on yhteensopiva myös kertolaskun kanssa eli $S_x(pq) = S_x(p)S_x(q)$ kaikilla $p, q \in K[X]$. Yhtälön $S_x(pq) = S_x(p)S_x(q)$ molemmilla puoleella esiintyy eräs kahden muuttujan kuvaus $K[X]\times K[X] \to A$ ja helposti nähdään, että molemmat nämä kuvaukset ovat K-bilineaarisia. Näin ollen, Lemman 2.80 nojalla, riittää osoittaa, että nämä kuvaukset saavat samat arvot kun $p = e_n, q = e_m$ ovat kanta-alkioita. Mutta potenssisääntöjen nojalla pätee

$$S_x(e_n e_m) = S_x(e_{n+m}) = x^{n+m} = x^n x^m = S_x(e_n)S_x(e_m).$$

Väite on todistettu.
Sen osoittamiseksi, että $S_x(p) = p(x)$ riittää huomata, että kaavalla $p \mapsto p(x)$ määritelty kuvaus on K-lineaarinen ja kuvaa kannan alkion e_n alkiolle x^n kaikilla $n \geq 0$. Näin ollen sen on pakko olla kuvaus S_x. □

Kuten universaalit ominaisuudet yleensäkin, edellisessä propositiossa mainittu polynomialgebran ominaisuus määrää sen yksikäsitteisesti algebra-isomorfismin vaille. Jätämme tämän väitteen formulointi ja todistus lukijalle harjoitustehtäväksi.

Sijoitushomomorfismin avulla voimme soveltaa polynomialgebraan liityvät tulokset mielivaltaisessa algebrassa. Tämän takia alamme nyt tutkimaan $K[X]$:n teoriaa.

Lemma 3.18. *Olkoot $f, g \in K[X]$. Tällöin*
1)$\deg(f+g) \leq \max\{\deg f, \deg g\}$,
2)$\deg fg = \deg f + \deg g$.
3) $K[X]$ on renkaana niin sanottu kokonaisalue *eli $fg = 0$ jos ja vain jos $f = 0$ tai $g = 0$. Tässä tulkitaan $-\infty + n = -\infty$ ja $-\infty < n$ jokaisella $n \in \mathbb{N}$.*

Todistus. Harjoitustehtävä. □

Vaihdannaisen renkaan R alkiota $x \neq 0$ sanotaan R:n *nollan jakajaksi*, jos on olemassa $y \in R, y \neq 0$ siten, että $xy = 0$. Vaihdannainen rengas sanotaan *kokonaisalueeksi*, jos siinä ei ole nollan jakajia, eli kaikilla $x, y \in R, x, y \neq 0$ pätee $xy = 0$. Esimerkiksi jokainen kunta on kokonaisalue. Kokonaislukujen rengas $\mathbb{Z}$ ei ole kunta, mutta on kokonaisalue (tästä esimerkistä nimitys "kokonaisalue" tuleekin). Kokonaisalueessa on voimassa tärkeä *supistussääntö*, joka sanoo, että jos $ab = ac$ ja $a \neq 0$, niin $b = c$.

Seuraus 3.19. *Rengas $K[X]$ on kokonaisalue.*

Todistus. Oletetaan, että $f, g \in K[X]$, $f, g \neq 0$. Tällöin edellisen lemman nojalla $\deg fg = \deg f + \deg g$ on äärellinen luonnollinen luku, joten tulo ei voi olla 0. □

Olkoot $f, g \in K[X]$. Sanomme, että polynomi f on *jaollinen* polynomilla g:llä, jos on olemassa $h \in K[X]$ siten, että $f = gh$. Polynomi g on tällöin f:n *tekijä*. Edellisen lemman nojalla tällöin on pakko olla $\deg g + \deg h = \deg f$, joten erityisesti $\deg g, \deg h \leq \deg f$, jos $f \neq 0$. Polynomien jaollisuusteorialla on paljon yhteistä kokonaislukujen jaollisuusteorian kanssa. Esimerkiksi seuraavassa propositiossa todistettava tärkeä *jaollisuusalgoritmi* on täysin analoginen kokonaislukujen vastaavan ominaisuuden kanssa.

Propositio 3.20. *Olkoot $f, g \in K[X]$, $g \neq 0$. Tällöin on olemassa yksikäsitteiset polynomit $q, r \in K[X]$ siten, että*

$$f = qg + r$$

ja $\deg r < \deg g$.

Todistus. Osoitetaan ensin q:n ja r:n olemassaolo. Todistus on formaalisaatio koulusta tutusta jakokulma - algoritmissa. Jos $\deg f < \deg g$, valitaan yksinkertaisesti $f = r$, $q = 0$. Oletetaan siis, että f:n aste on vähintään yhtä suuri kuin g:n aste.
Otetaan ensin menetelmän valaistamiseksi joku konkrettinen esimerkki vaikkapa $\mathbb{Q}$:ssä. Olkoon esim. $f = X^4 + 1$ ja $g = 2X^2 + X + 1$. Haluamme jakaa f g:llä jakokulmassa. Ensin pitää päästää eroon f:n korkeammasta potenssista eli termistä X^4 kertomalla g sopivalla polynomilla h. Koska haluamme kumoa termin X^4 ja g:n korkeimman asteen termi on $2X^2$ meidän on nostava potenssi 2:llä ja samalla pitää mitätöidä kertoimen 2 vaikutusta, eli kertoa sen käänteisluvulla. Kerrotaan siis g polynomilla $h = \frac{1}{2}X^2$. Saadaan

$$f - hg = (X^4 + 1) - (X^4 + \frac{1}{2}X^3 + \frac{1}{2}X^2) = -\frac{1}{2}X^3 - \frac{1}{2}X^2 + 1 = f'.$$

Jatketaan samalla tavalla jakamalla uusi polynomi f' (jonka aste on nyt aidosti pienempi kuin f:n aste) g:llä. Saadaan

$$f' + \frac{1}{4}Xg = -\frac{1}{4}X^2 + \frac{1}{4}X + 1 = f'',$$

$$f'' + \frac{1}{8}g = \frac{3}{8}X + \frac{9}{8} = r.$$

Kaiken kaikkian saadaan

$$f = f' + \frac{1}{2}X^2 g = f'' - \frac{1}{4}Xg + \frac{1}{2}X^2 g = (\frac{1}{2}X^2 - \frac{1}{4}X - \frac{1}{8})g + r = qg + r,$$

missä $\deg r < \deg g$.
Yleinen todistus etenee samalla tavalla. Oletaan siis, että $m = \deg f \geq \deg g = n$. Olkoon g:n johtava kerroin a ja f:n johtava kerroin b. Tällöin

$$f - ba^{-1}X^{m-n}g = f'$$

on polynomi, jonka aste on aidosti pienempi kuin f:n aste ja $f = f' + ba^{-1}X^{m-n}g$. Koska $\deg f' < \deg f$, voimme induktio-oletuksena väittää, että f':lle väite on tiedossa, eli $f' = q'g + r$, missä $\deg r < \deg g$. Tällöin saadaan $f = qg + r$, missä $q = q' + ba^{-1}X^{m-n}$ ja $\deg r < \deg g$. Väite on

siis todistettavissa induktiolla f:n asteen suhteen, kunhan näytetään vielä, että induktion alkuaskel toimii eli väite on tosi kun $\deg f = 0$. Mutta jos $\deg g > 0$, me olemme jo yllä osoittaneet, että väite pätee kun $\deg f < \deg g$. Muuten $\deg g = 0$ eli molemmat f ja g ovat vakiopolynomit, toisin sanoen K:n alkiot. Lisäksi $g \neq 0$. Nyt $f = (fg^{-1})g$ on vaadittu esitys (missä jakojäännös $r = 0$ on asteeltaan $-\infty$ pienempi kuin g.
Olemassaolo on todistettu.
Todistetaan vielä yksikäsitteisyys. Oletetaan, että

$$qg + r = f = q'g + r',$$

missä $\deg r, \deg r' < \deg g$. Tällöin eritysesti

$$(q - q')g = r' - r.$$

Jos $q - q' \neq 0$, niin vasemmaalla puoleella on polynomi jonka aste on $\deg(q - q') + \deg g \geq \deg g$, mutta oikealla puoleella polynomi, jonka aste on $< \deg g$. Saadaan ristiriitä. Näin olleen pitää olla $q - q' = 0$. □

Huomautus: Yleisemmin polynomialgebra voidaan määritellä renkaan R yli. Konstruktio on samanlainen ja näin syntynyt R-algebra merkitään $R[X]$:llä Erityisesti, jos A on jokin K-algebra, niin A itse on rengas, joten voimme myös tarkastella abstraktit algebralliset polynomit, jonka kertoimet ovat algebran A alkiot eli $A[X]$:n alkiot.
Jotkut polynomialgebran $K[X]$ ominaisuudet ovat voimassa myös polynomeille renkaan yli, monet taas ei. Juuri todistettu juuriyhtälö ei yleisesti sellaisenaan toimi renkaan yli - esimerkiksi $\mathbb{Z}[X]$:n polynomi $X^4 + 1$ ei voi esittää muodossa $qg + r$, missä $g = 2X^2 + X + 1$, $q, r \in Z[X]$ ja $\deg r < 4$. Tämä johtuu siitä, että yhtälössä $f = qg + r$ on tällöin oikealla puoleella polynomi, jonka johtava kerroin on 2:llä jaollinen, kun taas vasemmanpuoleisen polynomi johtava kerroin on 1.
Kuitenkin jos jaettavan polynomin g johtava kerroin on 1, niin jakoalgoritmi toimii myös mielivaltaisessa renkaassa/algebrassa - itse asiassa ei edes kertolaskun vaihdannaisuutta tarvita. Tällaista polynomia, jonka johtava kerroin on 1 sanotaan yleisesti *pääpolynomiksi*.

Tarkastellaan $K[X]$ vaihdannaisena renkaana (eli unohdetaan skalaarikertolasku). Olkoon $p \in P(k)$ ja määritellään osajoukko

$$J = \{pf \mid f \in K[X]\}.$$

Toisin sanoen J on kaikkien p:llä jaollisten polynomien osajoukko. Tällöin J on $K[X]$:n *ideaali* eli sellaisen osajoukko, joka on aliryhmä yhteenlaskun suhteen ja lisäksi jos $p \in I$ ja $f \in K[X]$ niin $pf \in I$. Tämä on helppoa

tarkistaa. Tällaista muotoa olevaa ideaalia sanotaan *pääidealiksi*. Polynomi p sanotaan tällöin pääideaalin J *virittäjksi*.

Propositio 3.21. *Jokainen $K[X]$:n ideaali I on pääideaali. Pääideaalin virittäjä on yksikäsitteinen K:n alkiolla kertomista vaille, eli jos p ja q ovat molemmat saman pääidealin virittäjät, on olemassa $k \in K$ siten, että $p = kq$. Erityisesti on olemassa yksikäsitteinen pääpolynomi p siten, että $I = (p)$.*

Todistus. Olkoon J $P(K)$:n ideaali. Jos $J = \{0\}$, se on alkion 0 virittämä. Oletetaan, että J:ssä on muitakin alkioita kuin nollapolynomi. Valitaan niistä sellainen $p \in J$, jonka aste on pienin mahdollinen. Osoitetaan, että J on p:n virittämä. Riittää olettaa, että jokainen $f \in J$ voidaan esittää muodossa $f = qp$. Jakoyhtälön **??** nojalla on olemassa $q, r \in P(K)$ siten, että $f = qp+r$, missä $\deg r < \deg p$. Koska J on ideaali, $f, p \in J$, myös $r = f - qp \in J$. Jos $r \neq 0$, se, että $\deg r < \deg p$ on ristiriidassa p:n valinnan kanssa. Näin ollen $r = 0$ eli $f = qp$. Väite on todistettu.
Jos f ja g ovat molemmat virittäjät, niin $f = qg$ ja $g = q'f$, josta $f = (qq')f$. Jos f on nollapolynomi, sen virittämä ideaali on yhden alkion ideaali, joten myös $g = f = 0$. □

Edellisestä propositiosta seuraa, että polynomialgebran $K[X]$ jokainen tekijäalgebra on muotoa $K[X]/(p)$. Näitä tutkimme tarkemmin myöhemmin, kun puhumme algebrallisista alkioista.

Jokainen polynomi f on selvästi jaollinen jokaisella nollasta eroavalla 0-asteisella polynomilla $k \in K$ ja jokaisella muotoa kf olevalla polynomilla, $k \in K$. Jos nämä ovat f:n ainoat tekijät ja lisäksi $\deg f > 0$ (eli f ei ole kunnan K alkio), sanomme, että f on *jaoton* polynomi. Jos f ei ole jaoton, se on *jaollinen*. Helposti nähdään, että $f \neq 0$ on jaollinen, jos ja vain jos $\deg f = 0$ tai $f = gh$ joillakin $g, h \in K[X]$, $\deg g < f, \deg h < f$, eli f voidaan esittää kahden aidosti alemman asteisen polynomin tulona. Tällöin nämä f:n *tekijät* eivät myöskään ole vakiopolynomeja.
Jaottomilla polynomeilla on polynomien jaollisuusteoriassa sama rooli kuin alkuluvuilla on luonnollisten lukujen jaollisuusteoriassa. Muun muassa pätee hajotelmalause - jokainen polynomi voidaan ”oleellisesti” yksikäsitteisellä tavalla esittää jaottomien polynomien tulona. Ennen kuin osoittamme tämän, käydään läpi tärkeä tekninen aputulos.

Lemma 3.22. *Olkoon $p \in K[X]$ jaoton polynomi, $f, g \in K[X]$. Jos tulo fg on jaollinen p:llä, niin joko f tai g on jaollinen p:llä.*

Todistus. Oletetaan, että p jakaa tulon fg ja f ei ole jaollinen p:llä. Osoitetaan, että tällöin p jakaa polynomin g. Tarkastellaan $K[X]$:n osajoukko

$$I = \{af + bp \mid a, b \in K[X]\}.$$

Helposti nähdään, että I on $K[X]$:n ideaali, itse asiassa pienin ideaali, joka sisältää polynomit f ja p. Proposition 3.21 nojalla I on pääideaali, eli on olemassa polynomi q siten, että $I = \{aq \mid a \in K[X]\}$. Koska $p \in I$, tästä seuraa, että erityisesti p on jaollinen q:llä. Mutta p on jaoton, joten joko $q = k \in K$ on nollaasteinen polynomi, tai $q = kp$ jollakin $k \in K$. Toisaalta $f \in I$, joten jos $q = kp$, saadaan $f = aq = (ak)p$ jollakin $a \in K[X]$, mikä on ristiiriidassa oletuksen kanssa (f ei ole jaollinen p:llä). Näin ollen q:n täytyy olla 0-asteinen polynomi, eli alkio $k \in K$. Jos $k = 0$, $I = \{0\}$, mikä on mahdotonta, sillä $p \in I$ ja $p \neq 0$. Näin ollen $k \neq 0$. Koska $k \in I$, on olemassa polynomit $a, b \in K[X]$, siten, että $af + bp = k$. Kertomalla tämä k^{-1}:llä saadaan yhtälö

$$af + bp = 1$$

joillakin $a, b \in K[X]$.
Koska oletuksen nojalla fg on jaollinen p:llä, eli on olemassa $q \in K[X]$, siten, että $pq = fg$, saadaan

$$g = g \cdot 1 = g(af + bp) = a(fg) + (bg)p = p(qa + bg).$$

Näin ollen g on jaollinen p:llä. □

Nyt voimme osoittaa, että jokainen polynomi f, jolle $\deg f > 0$, on esitettävissä jaottomien polynomien tulona, vieläkin "oleellisesti" yksikäsitteisellä tavalla.
On melko selvää, että jokainen ei-vakio polynomi voidaan esittää jaottomien polynomien tulona. Nimittäin jos f ei ole jaoton, kirjoitetaan se muotoon $f = gh$, missä $\deg g < f, \deg h < f$. Jos g tai h eivät ole jaottomia, pilkotaan ne alempiasteisten polynomien tulona jne. Koska tässä prosesissa polynomien asteet aina pienenevät aidosti jokaisessa vaiheessa, sitä ei voi jatkaa loputtomiin eli loppujen lopuksi päästään esitykseen $f = f_1 \dots f_n$, missä f_i:t ovat kaikki jaottomia.
Kokonaislukujen alkulukuhajotelma on tunnetusti yksikäsitteinen. Samoin jokaisen polynomin esitys jaottomien polynomien tulona on oleellisesti yksikäsitteinen. "Oleellisesti" tässä viittää siihen, että voimme tietenkin kirjoittaa polynomit erilaisessa järjestyksessä eli permutoida ne. Lisäksi jos $f \in K[X]$ on jaoton ja $k \in K, k \neq 0$, niin myös kf on jaoton. Näin ollen tulo $f = f_1 \dots f_n$ voimme kirjoittaa myös muodossa $f = (kf_1)(k^{-1}f_2) \dots f_n$ ja niin poispäin. Tämä hankaloi yksikäsitteisyys-väitteen tarkan formuloinnin. Tämän takia muotoilemme sen hieman eri tavalla.
Polynomin $f = (c_n) \neq 0$ *johtava kerroin* on sen suurin nollasta eroava komponentti c_m, eli sellaisen, jossa $m = \deg f$. Jos polynomin johtava kerroin on 1, sanomme se *pääpolynomiksi*.

Propositio 3.23. *Jokainen polynomi $f \neq 0 \in K[X]$ voidaan esittää muodossa*

$$f = k \cdot f_1 \dots f_m \tag{3.24}$$

missä $k \in K$ ja f_i on jaoton pääpolynomi jokaisella $i = 1, \dots, m$. Tällainen esitys on sen jäsenten permutaatiota vaille yksikäsitteinen.

Todistus. Olemme yllä jo todistaneet, että f voidaan esittää muodossa $f = f_1' \dots f_m'$, missä f_i' on jaoton jokaisella $i = 1, \dots, m$. Jos jokin f_i' ei ole pääpolynomi, se voidaan kuitenkin kirjoittaa muodossa $f_i' = k_i f_i$, missä $k_i \in K$ ja f_i on pääpolynomi, edellenkin jaoton. Keräämällä kaikki kertoimet k_i eteen yhdeksi kertoimeksi k, saadaan esitys 3.24.
Osoitetaan esityksen yksikäsitteisyys. Olkoon $k' \cdot f_1' \dots f_n' = f$ toinen samanlainen hajotelma. Tällöin f:n johtava kerroin on sekä k, että k', joten $k = k' \neq 0$. Koska K on kunta, voidaan jakaa alkiolla k, jolloin saadaan

$$f_1 \dots f_m = f_1' \dots f_n'.$$

Polynomi f_m on jaoton ja se jakaa tulon $f_1' \dots f_n'$. Edellisestä lemmasta seuraa, induktiolla, että f_m jakaa yhden polynomeista $f_1', \dots, f_n'$. Koska niiden järjestyksellä ei ole merkitystä, voimme esim. olettaa, että f_m jakaa polynomin f_n'. Mutta molemmat ovat jaottomia ja vieläkin pääpolynomeja, joten $f_m = f_n'$.
Koska $K[X]$ on kokonaisalue, voimme supistaa yhtälössä

$$f_1 \dots f_m = f_1' \dots f_n'$$

samat tekijät $f_m = f_n'$. Saadaan samannäköinen yhtälö, joissa on vähemmän alkioita. Jatketaan samalla tavalla. Jokaisessa vaiheessa molemmista puolista supistuu yksi alkio ja loppujen lopuksi joudutaan tilanteseen, jossa toisella puoleella on jäljellä vain vakio 1. Näin ollen ei toisessakaan voi olla jäljellä mitään (muuten vasemmalla puoleella vakio-polynomi, oikealla taas polynomi, jonka aste vähintään 1). Näin ollen $m = n$ ja molemmat esitykset samat alkioiden järjestystä vaille. □

Olkoon $p \in K[X]$ polynomi, A jokin K-algebra ja $x \in A$. Sanomme, että x on p:n *juuri*, jos $p(x) = 0$. Tässä $p(x)$ on siis sijoitushomomorfismin arvo kun p:ssä symbolin X paikalle sijoitetaan $a \in A$.
Erityisesti kun kunta K tarkastellaan K-algebrana itseensä suhteen, voidaan erikoistapauksena puhua p:n juuresta kunnassa K.
Juuret käyttäytyvät kunnissa ja yleisissä algebroissa eri tavalla.

Propositio 3.25. *Olkoon $p \in K[X], p \neq 0$. Tällöin*
1) alkio $a \in K$ on p:n juuri jos ja vain jos p on jaollinen polynomilla $X - a$,
2) p:llä on korkeintaan $\deg p$ erilaista juurta kunnassa K.

Todistus. 1) Sovelletaan jakoyhtälö polynomeihin p ja $g = X - a$. On siis olemassa $q, r \in K[X]$ siten, että $p = gq + r$ ja $\deg r < \deg g = 1$. Näin ollen jakojäännös r on itse asiassa vakiopolynomi eli $r = b$ jollakin $b \in K$. p on jaollinen g:llä täsmälleen silloin, kun $b = 0$. Sijoitetaan yhtälöön $p = qg + r$ K:n alkio a (sijoitushomomorfismin kautta). Saadaan

$$p(a) = qg(a) + b = b,$$

sillä $g(a) = 0$ polynomin $g = X - a$ määritelmän mukaan. Näin ollen jakojäännös $r = b = 0$, eli p on jaollinen g:llä, jos ja vain jos $p(a) = 0$ eli a on p:n juuri.
2) Väite voidaan osoittaa induktiolla $\deg p$:n suhteen. Jos p on nollasta eroava vakio polynomi, sillä ei ole juuria ja sen aste onkin 0.
Otetaan jokin polynomi p. Jos sillä ei ole juuria, asia on selvä. Muuten on olemassa $a \in K$ siten, että $p(a) = 0$ eli, a)-kohdan nojalla, $p = (X - a)q$ jollakin polynomilla. Vertamaalla asteet nähdään, että $\deg q = \deg p - 1$. Induktio-oletuksen nojalla q:llä on korkeintaan $\deg p - 1$ eilaista juurta. Nyt jos b on jokin polynomin p juuri, sijoittamalla se (sijoitushomomorfismi!) polynomiyhtälöön $p = (X - a)q$ saadaan $0 = p(b) = (b - a)q(b)$. Koska K on kuntana erityisesti kokonaisalue, tästä seuraa, että joko $b = a$ tai $q(b) = 0$ eli b on q:n juuri. Induktioletuksesta seuraa, että p:n juurten lukumäärä on korkeintaan $\deg q + 1 = \deg p$. □

Olkoon $a \in K$ polynomin $p \in K[X]$ juuri, $p \neq 0$. Edellisen proposition mukaan on olemassa polynomi $q \in K[X]$ siten, että $\deg q < \deg p$ ja $p = (X - a)q$. Voi käydä niin, että a on myös polynomin q juuri. Tällöin $p = (X - a)^2 r$, missä $\deg r < \deg q$. Näin voidaan jatkaa kunnes pystyy ja lopulta päädytään esitykseen $p = (X - a)^k g$, missä a ei enää ole g:n juuri. Tätä lukua $k \in \mathbb{N}$ sanotaan juuren k *kertaluvuksi.* Se on siis suurin k jolla p on jaollinen $(X - a)^k$:llä. Kertaluku on aina olemassa ja $\leq \deg p$. Jos juuren kertaluku on 1, se on *yksinkertainen* juuri. Muuten se on monikertainen juuri.

Jos tarkastellaan yleisemmin polynomit, joiden kertoimet ovat algebran A, tai, vielä yleisemmin, renkaan R alkiot, niin edellisen proposition kohta 1) on edellenkin tosi, mutta 2) ei vältämättä enää ole. Nimittäin polynomien jakoyhtälö on voimassa renkaassa kunhan jaettava polynomi on pääpolynomi. Koska polynomi $X - a$ on sellainen, yllä annettu todistus toimii sellaisenaan

myös renkaan R yli.
Kun kohdan 2) todistus yritetään yleistää renkaseen, niin täytyy ainakin olettaa, että siinä ei ole nollan jakajia, mutta vaihdannaisuus pitää myös olettaa. Hyvä harjoitus on miettiä missä kohdassa tarkalleen vaihdannaisuutta tarvita, jos yllä annettu todistus yrittää viedä läpi renkaassa.
Alla on annettu mielenkiintoinen esimerkki renkaasta, joka toteuttaa kaikki kunnan aksioomat, paitsi kertolasku ei ole vaihdannainen, ja jolle edellisen proposition kohta 2) ei ole voimassa.

Esimerkkejä 3.26. *1) Jokainen ensimmäisen asteen polynomi $f = aX + b$, $a \neq 0$ on jaoton. Tämä seuraa siitä, että jos $f = gh$, missä $\deg g, \deg h < 1$, niin g:n ja h:n asteiden täytyy olla korkeintaan nolla, eli g ja h ovat tällöin molemmat nolla-asteiset vakiopolynomit. Mutta ei niiden tulo voi sitten olla 1-asteinen.*

2) $\mathbb{R}$:n polynomi $f = X^2 + 1$ on jaoton. Tämä nähdään seuraavasti - oletetaan, että $f = gh$, missä $\deg g, \deg h < 2, \deg f + \deg h = 2$. Tällöin ainoa mahdollisuus on $\deg g = \deg h = 1$. Jos $g = aX + b$, missä $a \neq 0$, niin $-b/a$ on g:n juurena myös f:n juuri. Mutta ei f:llä ole juuria $\mathbb{R}$:ssä.
Jos f tarkastellaan $\mathbb{C}$:n polynomilla, f on jaollinen, $f = (X-i)(X+i)$. Yleisemmin, jos $f\colon K[X]$ on korkeintaan astetta 3) oleva polynomi, niin se ei ole jaoton jos ja vain jos sillä on juuri. Tämä nähdään samalla tavalla kuin yllä, tarkastelemalla hajotelman polynomien mahdollisia asteita.
Sen sijaan kun $\deg f > 3$, voi käydä niin, että f ei ole jaoton, vaikka sillä ei ole juuria. Esimerkiksi $\mathbb{R}$:n polynomi $f = X^4 + 1$ ei ole jaoton, sillä

$$X^4 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1).$$

Selvästi f:llä ei ole juuria $\mathbb{R}$:ssä. Näin ollen juurten olemassaolo on yleiselle polynomille riittävä, mutta ei välttämätön ehto jaottomuudelle.

3) Olkoon K algebrallisesti suljettu kunta, esim. $K = \mathbb{C}$. Tällöin vain ensimmäisen asteen polynomit ovat jaottomia. Tämä seuraa Propositiosta 3.25, sillä jos f:llä on juuri k, se on jaollinen polynomilla $X - k$. Propositiosta 3.23 seuraa, että jokainen $f \in K[X]$ voidaan kirjoittaa muodossa

$$f = a(X - k_1) \dots (X - k_n)$$

yksikäsitteisellä tavalla. Tässä $k_1, \ldots, k_n$ ovat f:n juuret (eivät vältämättä erilaiset!).

4) *Käytämällä hyväksi sitä, että $\mathbb{C}$ on algebrallisesti suljettu, voidaan osoittaa, että $\mathbb{R}$:ssä jaottomat polynomit ovat tasan kaikki ensimmäisen asteen polynomit ja sellaiset toisen asteen polynomit, joilla ei ole reaalijuureja. Tästä seuraa, että $\mathbb{R}[X]$:n polynomi voidaan aina kirjoittaa ensimmäisen ja toisen asteen polynomien tulona. Yksityiskohdat harjoitustehtävänä.*
Tästä seuraa erityisesti, että paritonta astetta olevalla $\mathbb{R}[X]$:n polynomilla on aina ainakin yksi reaalinen juuri. Sama tulos voi todistaa helposti myäs käytämällä klassisen analyysin menetelmiä. Nimittäin jos $\deg p$ on pariton, niin p kasvaa rajatta, kun lähestytään toista äärettömyyttä ja pienenee rajatta, kun lähestytään toista äärettömyyttä. Erityisesti p:n on pakko saada sekä positiivisia, että negatiivisia arvoja. Toisaalta polynomi on jatkuva funktio, joten Bolzanon lauseesta seuraa, että se täytyy myös saada jossakin pisteessä arvon 0.

5) *Rengas on* jakorengas, *jos se toteuttaa kaikki kunnan aksioomat, paitsi (ehkä) kertolaskun vaihdannaisuutta. Toisin sanoen rengas on jakorengas jos se on epätriviaali, ykkösellinen ja jokaisella nollasta eroavalla alkiolla on käänteisalkio kertolaskun suhteen.*
Konstruoidaan esimerkki jakorenkaasta, jossa toisen asteen polynomiyhtälöllä $x^2 + 1 = 0$ on äärettömän monta ratkaisua. Edellenkin erittäin hyvä harjoitus on miettiä missä tarkasti väitteen "n-asteisella polynomiyhtälöllä on kunnassa korkeintaan n ratkaisua" todistuksessa käytetäään vaihdannaisuutta ja miksi se ei toimi ilman sitä oletusta.
Olkoon Q kompleksisen matriisialgebran $M(2 \times 2; \mathbb{C})$ osajoukko, jonka muodostavat muotoa

$$\begin{bmatrix} z & w \\ -\bar{z} & \bar{w} \end{bmatrix}$$

olevat matriisit. Tässä $z, w \in \mathbb{C}$ ja $\bar{z}$ on niin sanottu kompleksiluvun $z = x + iy$ konjugaatti *$\bar{z} = x - iy$.*
Voidaan osoittaa, että Q on $M(2\times 2; \mathbb{C})$:n ykkösellinen alialgebra, joten erityisesti itse $\mathbb{C}$-algebra. Lisäksi jokainen Q:n nollasta eroava alkio on kääntyvä Q:ssä. Näin ollen Q in erityisesti jakorengas. Näiden väitteiden verifioiminen jätetään lukijalle harjoitustehtäväksi.
Tätä algebra sanotaan kvartenionialgebraksi. *Se on 2-ulotteinen $\mathbb{C}$-vektoriavaruutena ja 4-ulotteinen $\mathbb{R}$-vektoriavaruutena. Erään sen $\mathbb{R}$-*

kannan muodostaa joukko $\{(1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, *missä*

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \mathbf{i} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \mathbf{j} = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Tämän kannan alkiot ja niiden vasta-alkiot muodostavat mielenkiintoisen ja tärkeän esimerkin äärellisestä 8 *alkion ei-Abelin ryhmästä* $Q_8 = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. *Sen kertotaulu on seuraava.*

Kertotaulusta nähdään suoraan, että Q:ssä yhtälöllä $x^2 + 1 = 0$ *on ainakin* 6 *ratkaisua, kaikki luvut joukosta* $\{\pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. *Näin ollen Proposition 3.25 kohta 2) ei päde Q:ssä, joka on muuten kuin kunta, paitsi, että kertolasku ei ole vaihdannainen.*
Itse asiassa voidaan osoittaa, että yhtälöllä $x^2 + 1 = 0$ *on Q:ssä jopa äärettömän monta ratkaisua.*

Algebralliset alkiot.
Olkoon A K-algebra ja $x \in A$. Sanomme, että x on algebran A *algebrallinen* alkio, jos on olemassa polynomi $p \in K[X], p \neq 0$ siten, että $p(x) = 0$. Muuten x sanotaan *traskendaaliseksi* alkioksi.
Erikoistapauksesta jossa kompleksilukujen kunta $\mathbb{C}$ ajatellaan $\mathbb{Q}$-algebrana oli jo maininta edellisessä luvussa. Kompleksiluku z sanotaan algebralliseksi luvuksi, jos on olemassa nollasta eroava $\mathbb{Q}$-kertoiminen polynomi p, jonka juurena on z. Itse asiassa määritelmässä riittää vaatia, että on olemassa kokonaislukukertoiminen nollasta eroava polynomi $p \in \mathbb{Z}[X]$ jonka juuri on z (miksi?). Jokainen rationaaliluvuista ja imaginaariyksiköstä i neljän peruslaskutoimituksen ja juurten $\sqrt[n]{}$ avullan rakenettu kompleksiluku on algebrallinen, mutta on olemassa myös algebrallisia lukuja, joita ei voi esittää tällaisessa muodossa. Tämä on seuraus kuuluisasta Galois'n teoriasta, joka tarkastellaan Algebra II kurssilla. Tunnettuja esimerkkejä transkendentteista eli ei-algebrallisista kompleksiluvuista ovat π ja e. Sen todistaminen, että jokin luku on transkendentti on yleensä suhteellisen vaikeata, joten transkendentteista luvuista on vaikeata antaa konkrettisia esimerkkejä. Sen sijaan on helppoa näyttää, että tällaisia lukuja pakko olla olemassa ja itse asiassa hyvinkin paljon. Nimittän $\mathbb{Q}$-kertoimisia polynomeja on vain numeroituva määrä ja jokaisella sellaisella on äärellinen määrä juuria. Tästä seuraa, että algebrallisia lukuja on vain numeroituvan paljon. Koska kompleksilukujen joukko ei ole numeroituva, tästä seuraa, että "suurin osa" kompleksiluvuista ovat transkendenttejä.

Puetaan algebrallisen/transkendentin alkion määritelmä abstraktimpaan muotoon. Olkoon A K-algebra ja $x \in A$. Konstruoidaan sijoitushomomorfismi $S_x \colon K[X] \to A$ joka kuvaa alkion X alkiolle x (Propositio 3.17). Tällöin

$\operatorname{Im} S(X) = K[x]$ (Lemma 3.15), pienin A:n alialgebra, joka sisältää x:n. Isomorfialauseen nojalla S_x indusoi algebraisomorfismin $K[X]/\operatorname{Ker} S_x \cong K[x]$. Määritelmän mukaan ydin $\operatorname{Ker} S_x$ koostuu niistä polynomeista p joille $p(x) = 0$.
On olemassa 2 mahdollisuutta. Jos $\operatorname{Ker} S_x = \{0\}$, niin S_x on injektio ja x on transkendenttinen alkio. Tällöin $K[x]$ on isomorfinen polynomialgebran $K[X]$ kanssa. Transkendenttinen alkio siis käyttaäytyy täsmälleen samalla tavalla kuin "geneerinen muuttujasymboli" X.
Jos taas $\operatorname{Ker} S_x \neq \{0\}$, niin x on algebrallinen alkio. Lemman 3.21 nojalla on olemassa (yksikäsitteinen) pääpolynomi $p \neq 0$ jolle $\operatorname{Ker} S_x = (p)$. Polynomi p on siis dimensioltaan *pienin* nollasta eroava polynomi, jolle $p(x) = 0$ ja jos $q(x) = 0$ jollekin polynomille q, niin $q = pg$ jollakin polynomilla g. Tästä syystä kutsumme p x:n *minimipolynomiksi*. Isomorfialauseen nojalla alialgebra $K[x]$ on isomorfinen tekijäalgebran $K[X]/(p)$ kanssa.

Esimerkiksi tarkastellaan $\mathbb{Q}$-algebran $\mathbb{C}$ alkiota $i = (0, 1)$. Tämä on algebrallinen koska $i^2 + 1 = 0$,. Itse asiassa polynomi $X^2 + 1 \in \mathbb{Q}[X]$ on i:n minimipolynomi. Näin ollen $\mathbb{Q}[i]$ on isomorfinen algebran $\mathbb{Q}[X]/(X^2+1)$ kanssa. Kohta todistettavasta tuloksesta seuraa, että tämä algebra on 2-ulotteinen ja

$$\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\},$$

mikä tässä tapauksessa voi helposti todeta suoraankin.
Korvataan edellisessä esimerkikssä kunta $\mathbb{Q}$ reaalilukujen kunnalla $\mathbb{R}$. Kaikki tulokset edelleenkin pätevät, mutta tällöin $\mathbb{C}$:n alialgebra $\mathbb{R}[i]$ onkin koko kompleksilukujen kunta $\mathbb{C}$. Näin ollen $\mathbb{R}$-algebrana (erityisesti renkaana) $\mathbb{C}$ on isomorfinen polynomialgebran tekijäalgebran $\mathbb{R}[X]/(X^2 + 1)$. Tästä saadaan jäljeen uusi tapa konstruoida/tarkastella kompleksiluvut.

Lemma 3.27. *Olkoon K kunta, $p \in K[X]$, $p \neq 0$, A jokin K-algebra ja $x \in A$. Olkoon $n = \deg p$.*
a) Tekijäalgebra $K[X]/(p)$ on K-vektoriavaruutena n-ulotteinen. Eräs sen kanta on

$$\{\bar{1}, \bar{X}, \ldots, \bar{X}^{n-1}\}.$$

b) $x \in A$ on algebrallinen jos ja vain jos alialgebra $K[x] \subset A$ on K-vektoriavaruutena äärellisulotteinen.
c) Jos algebra A on K-vektoriavaruutena äärellisulotteinen, niin jokainen sen alkio on algebrallinen.
d) Tekijäalgebra $K[X]/(p)$ on renkaana kunta jos ja vain jos se on kokonaisalue jos ja vain jos p on jaoton polynomi.

Todistus. Olkoon p n-ulotteinen polynomi, $p \neq 0$. Osoitetaan, että $\{\bar{1}, \bar{X}, \ldots, \bar{X}^{n-1}\}$ on $K[X]/(p)$:n kanta. Tekijäalgebran määritelmän mukaan kahdelle polynomille $f, g \in K[X]$ pätee $\bar{f} = \bar{g}$ algebrassa $K[X]/(p)$ jos ja vain jos $f - g$ on jaollinen p:llä eli $f - g = pq$ jollakin polynomilla q.
Oletetaan, että

$$f = a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

siten, että

$$\bar{f} = a_{n-1}\bar{X}^{n-1} + \ldots + a_1\bar{X} + a_0 = 0 \in K[X]/(p).$$

Tällöin f on siis jaollinen p:llä eli $f = pq$. Mutta $\deg f \leq n - 1 < n = \deg p$, joten vertamaalla asteet nähdään, että q:n täytyy olla nollapolynomi, jolloin $f = 0$, joten myös $a_{n-1} = \ldots = a_1 = a_0$. Näin ollen jono $\{\bar{1}, \bar{X}, \ldots, \bar{X}^{n-1}\}$ on vapaa.
Osoitetaan, että se myös virittää tekijäavaruuden $K[X]/(p)$. Olkoon f mielivaltainen $K[X]$:n alkio. Jakoyhtälön mukaan voimme kirjoittaa f muodossa

$$f = qp + r,$$

missä $qp \in (p)$ ja $\deg r \leq n - 1$. Nyt $\bar{f} = \bar{r}$ ja koska r voidaan kirjoittaa muodossa

$$r = a_{n-1}X^{n-1} + \ldots + a_1X + a_0,$$

saadaan

$$\bar{f} = \bar{r} = a_{n-1}\bar{X}^{n-1} + \ldots + a_1\bar{X} + a_0.$$

Näin ollen joukko $\{\bar{1}, \bar{X}, \ldots, \bar{X}^{n-1}\}$ virittää avaruuden.

b) Jos x on algebrallinen, $K[x] \cong K[X]/(p)$, missä $p \neq 0$. a)-kohdasta seuraa, että $K[x]$ on äärellisulotteinen.
Jos x on transkidenttinen, $K[x] \cong K[X]$, joka on ääretönulotteinen konstruuktio perusteella.

c) Jos A on äärellisulotteinen, jokaisella $x \in X$ alialgebra $K[x]$ on A:n aliavaruutena myäös äärellisulotteinen. Väite seuraa nyt b)-kohdasta.

d) Harjoitustehtävä. □