## 13. Algebralliset laajennokset

Vanhoina aikoina algebran tutkimuksen päämääränä oli oppia ratkaisemaan polynomiyhtälöitä. Niinpä erityisen tärkeää osaa klassisessa kuntalaajennosten teoriassa näyttelevät sellaiset laajennokset, joiden kaikki alkiot ovat joidenkin lähtökunnan polynomien juuria. Esimerkiksi jokainen kompleksiluku on jonkin korkeintaan toisen asteen polynomiyhtälön ratkaisu.

### 13.1. Algebrallisuus ja minimipolynomit.

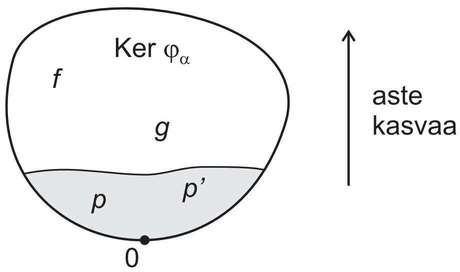
MÄÄRITELMÄ 13.1. Olkoon $L$ kunnan $K$ laajennos. Alkiota $\alpha \in L$ kutsutaan *algebralliseksi* kunnan $K$ suhteen, jos on olemassa nollasta poikkeava polynomi $f \in K[X]$, jolle pätee $f(\alpha) = 0$. Jos tällaista polynomia ei ole, sanotaan, että $\alpha$ on *transkendenttinen* $K$:n suhteen. Jos kaikki $L$:n alkiot ovat algebrallisia $K$:n suhteen, sanotaan, että $L$ on algebrallinen $K$:n suhteen, ja laajennosta $L/K$ kutsutaan *algebralliseksi laajennokseksi*.

Oletetaan, että $L$ on kunnan $K$ laajennos ja $\alpha \in L$. Jos $\alpha$ on transkendenttinen $K$:n suhteen, niin kaikilla nollasta poikkeavilla polynomeilla $f \in K[X]$ pätee $f(\alpha) \neq 0$. Tämä tarkoittaa, että alkioon $\alpha$ liittyvän sijoitushomomorfismin ydin

$$\operatorname{Ker} \varphi_\alpha = \{f \in K[X] \mid f(\alpha) = 0\}$$

on nollaideaali.

Vastaavasti $\alpha$ on algebrallinen, jos ja vain jos sijoitushomomorfismin ydin on epätriviaali. Koska $K[X]$ on pääideaalirengas, ideaali $\operatorname{Ker} \varphi_\alpha$ on jonkin yhden polynomin $p$ virittämä, eli $\operatorname{Ker} \varphi_\alpha = \langle p \rangle$. Koska jokainen ideaalin $\langle p \rangle$ polynomi on jaollinen $p$:llä, nähdään että $p$:n aste on minimaalinen joukon $\operatorname{Ker} \varphi_\alpha$ nollasta poikkeavien polynomien keskuudessa. Lisäksi myös kaikki $p$:n kanssa samanasteiset joukon $\operatorname{Ker} \varphi_\alpha$ polynomit ovat jaollisia $p$:llä, joten ne voivat erota tästä vain vakiokertoimella, ja jokainen niistä virittää saman ideaalin. Polynomin $p$ määräämiseksi yksikäsitteisesti riittää siis viritysominaisuuden lisäksi vaatia esimerkiksi, että korkeimman asteen kerroin on 1 eli että $p$ on *pääpolynomi*. Tätä polynomia nimitetään alkion $\alpha$ *minimipolynomiksi*.




KUVA 24. Sijoitushomomorfismin ytimen virittää mikä tahansa minimaalisen asteen omaava nollasta poikkeava polynomi. Nämä ovat kaikki toistensa liittoalkioita.

MÄÄRITELMÄ 13.2. Oletetaan, että $\alpha \in L$ on algebrallinen kunnan $K$ suhteen. Alkion $\alpha$ *minimipolynomi* $K$:n suhteen on sellainen nollasta poikkeava pääpolynomi $p \in K[X]$, jolle pätee $p(\alpha) = 0$ ja jonka aste on pienin mahdollinen. Alkion $\alpha$ minimipolynomia kunnan $K$ suhteen merkitään $p = \min(K, \alpha)$.

*Huom.* Koska määritelmän mukaan $p(\alpha) = 0$, niin $p \in \operatorname{Ker}\varphi_\alpha$. Määritelmää edeltävän päättelyn perusteella alkion $\alpha$ minimipolynomi voidaan karakterisoida niin, että se on *se pääpolynomi, joka virittää alkioon $\alpha$ liittyvän sijoitushomomorfismin ytimen.*

Esimerkki 13.3. Luku $\sqrt{2}$ on algebrallinen kunnan $\mathbb{Q}$ suhteen, sillä se on polynomin $X^2 - 2$ juuri. Koska $\sqrt{2}$ ei ole rationaaliluku, se ei ole minkään ensimmäisen asteen polynomin juuri. Näin ollen $\min(\mathbb{Q}, \sqrt{2}) = X^2 - 2$. Toisaalta $\min(\mathbb{R}, \sqrt{2}) = X - \sqrt{2}$.

Alkion $\alpha$ minimipolynomin hyödyllisyys piilee siinä, että sen aste kertoo laajennoksen $K(\alpha)$ asteen. Seuraavassa lauseessa tämä seikka on koottu yhteen muiden hyödyllisten ominaisuuksien kanssa.

Lause 13.4. *Olkoon $L$ kunnan $K$ laajennos, ja olkoon $\alpha \in L$ algebrallinen kunnan $K$ suhteen. Tällöin*

i) *Minimipolynomi* $\min(K, \alpha)$ *on jaoton renkaassa $K[X]$.*
ii) *Jos $f \in K[X]$, niin $f(\alpha) = 0$, jos ja vain jos* $\min(K, \alpha)$ *jakaa $f$:n.*
iii) *$K[\alpha]$ on kunta, ja $K[\alpha] = K(\alpha)$.*
iv) *Jos $n$ on polynomin* $\min(K, \alpha)$ *aste, niin alkiot $1, \alpha, \ldots, \alpha^{n-1}$ muodostavat laajennoksen $K(\alpha)/K$ kannan. Erityisesti $[K(\alpha) : K] = n < \infty$.*

Todistus. Merkitään $\min(K, \alpha) = p$. Aloitetaan kohdasta (ii). Jos $f(\alpha) = 0$ jollain $f \in K[X]$, niin $f \in \operatorname{Ker}\varphi_\alpha$. Koska $p$ virittää ideaalin $\operatorname{Ker}\varphi_\alpha$, $f$ on jaollinen $p$:llä. Toisaalta, jos $f = pg$ jollain $g \in K[X]$, niin $f(\alpha) = p(\alpha)g(\alpha) = 0$.

i) Oletetaan, että $p = fg$ joillain $f, g \in K[X]$, jolloin

$$f(\alpha)g(\alpha) = p(\alpha) = 0.$$

Lauseen 12.5 perusteella $f(\alpha)$ ja $g(\alpha)$ ovat renkaassa $K[\alpha]$. Tämä rengas on kokonaisalue, koska se on kunnan $L$ alirengas, joten $f(\alpha) = 0$ tai $g(\alpha) = 0$. Nyt $p$:n asteen minimaalisuudesta seuraa, että $\deg(f) \geq \deg(p)$ tai $\deg(g) \geq \deg(p)$. Toisaalta $p$ on jaollinen sekä $f$:llä että $g$:llä, joten joko $f$ tai $g$ on vakio. Vakiot ovat yksiköitä renkaassa $K[X]$, joten $p$ on jaoton.

iii) Lauseen 12.5 mukaan $K[\alpha] = \operatorname{Im}\varphi_\alpha$, ja toisaalta $\langle p \rangle = \operatorname{Ker}\varphi_\alpha$. Algebrojen homomorfialauseesta seuraa täten, että $K[X]/\langle p \rangle \cong K[\alpha]$. Koska $K[\alpha] \subset L$ on kokonaisalue, $\langle p \rangle$ on alkuideaali. Toisaalta $K[X]$ on pääideaalirengas, joten sen jokainen nollasta poikkeava alkuideaali on maksimaalinen. Tästä seuraa, että $K[\alpha]$ on kunta. Lisäksi $K[\alpha] = K(\alpha)$, koska $K[\alpha] \subset K(\alpha)$ ja $K(\alpha)$ on pienin kunta, joka sisältää sekä $K$:n että alkion $\alpha$.

iv) Olkoon $x \in K(\alpha)$. Kohdan (iii) nojalla $x = f(\alpha)$ jollain $f \in K[X]$. Jakoyhtälöstä nähdään, että $f = qp + r$, missä $\deg(r) < \deg(p) = n$. Nyt $f(\alpha) = r(\alpha)$, koska $p(\alpha) = 0$. Alkio $x = r(\alpha)$ voidaan siis kirjoittaa lineaarikombinaationa alkioista $1, \alpha, \ldots, \alpha^{n-1}$. Oletetaan sitten, että $\sum_{i=0}^{n-1} a_i\alpha^i = 0$ joillain $a_i \in K$. Tällöin polynomi $g = \sum_{i=0}^{n-1} a_i X_i$ on ytimessä $\operatorname{Ker}\varphi_\alpha = \langle p \rangle$, joten $p$ jakaa $f$:n. Kuitenkin $f$:n aste on pienempi kuin $n$, joten $f$:n on oltava nollapolynomi. Tämä tarkoittaa sitä, että $a_i = 0$ kaikilla $i$, ja joukko $\{1, \alpha, \ldots, \alpha^{n-1}\}$ on vapaa. Kyseinen joukko muodostaa siis laajennoksen $K(\alpha)$ kannan kerroinkunnan $K$ suhteen. $\square$

ESIMERKKI 13.5. Tarkastellaan laajennosta $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Polynomille $f = X^3 - 2$ pätee $f(\sqrt[3]{2}) = 0$, joten luvun $\sqrt[3]{2}$ minimipolynomi jakaa $f$:n. Toisaalta $f$ on jaoton Eisensteinin kriteerin perusteella, joten se on luvun $\sqrt[3]{2}$ minimipolynomi. Täten laajennoksen $\mathbb{Q}(\sqrt[3]{2})$ aste on 3. Lisäksi $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$, joten jokainen laajennoksen alkio on muotoa $a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Tämä koskee myös käänteislukuja $x^{-1}$, missä $x \in \mathbb{Q}[\sqrt[3]{2}]$.

ESIMERKKI 13.6. Kompleksiluku $\omega = e^{i\pi/3}$ on polynomin $X^3 - 1$ juuri. Tämä polynomi ei kuitenkaan ole $\omega$:n minimipolynomi, sillä se jakautuu tekijöihin seuraavasti: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. Näistä tekijöistä jälkimmäinen on jaoton rationaalijuuritestin perusteella, ja sillä on juurenaan $\omega$. Siispä alkion $\omega$ minimipolynomi on $X^2 + X + 1$, ja $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

Ei ole vaikea nähdä, että äärellinen laajennos on aina äärellisviritteinen. Aiemmin todettiin, että sama ei päde toisinpäin: äärellisviritteinen laajennos ei ole välttämättä aina äärellinen. Käsitteet ovat kuitenkin yhtäpitäviä, mikäli laajennos on algebrallinen. Lisäksi äärellinen laajennos on aina algebrallinen. Nämä ajatukset on ilmaistu seuraavissa kahdessa lauseessa.

LAUSE 13.7. *Olkoon $L$ kunnan $K$ äärellinen laajennos. Tällöin $L$ on äärellisviritteinen ja algebrallinen $K$:n suhteen.*

TODISTUS. Harjoitustehtävä. □

LAUSE 13.8. *Olkoon $L$ kunnan $K$ laajennos. Oletetaan, että $\alpha_i \in L$ on algebrallinen $K$:n suhteen kaikilla $i$. Tällöin $K[\alpha_1, \ldots, \alpha_n]$ on kunnan $K$ äärellinen laajennos, jonka asteelle pätee*

$$[K[\alpha_1, \ldots, \alpha_n] : K] \leq \prod_{i=1}^{n} [K(\alpha_i) : K].$$

TODISTUS. Käytetään induktiota $n$:n suhteen. Tapaus $n = 1$ seuraa lauseesta 13.4. Oletetaan, että väite pätee renkaalle $K_1 = K[\alpha_1, \ldots, \alpha_{n-1}]$. Tällöin $K_1$ on kunta. Koska $\alpha_n$ on algebrallinen $K$:n ja siis myös $K_1$:n suhteen, lauseesta 13.4 seuraa, että $K[\alpha_1, \ldots, \alpha_n] = K_1[\alpha_n]$ on kunta. Edelleen saman lauseen mukaan $\min(K_1, \alpha_n)$ jakaa polynomin $\min(K, \alpha_n)$, joten

$$[K_1[\alpha_n] : K_1] \leq [K(\alpha_n) : K].$$

Induktio-oletuksen ja lauseen 12.3 perusteella

$$[K_1[\alpha_n] : K] = [K_1[\alpha_n] : K_1] \cdot [K_1 : K] \leq \prod_{i=1}^{n} [K(\alpha_i) : K].$$

□

Edellisistä lauseista saadaan suoraan seuraava ehto alkion algebrallisuudelle.

KOROLLAARI 13.9. *Olkoon $L$ kunnan $K$ laajennos. Tällöin $\alpha \in L$ on algebrallinen $K$:n suhteen, jos ja vain jos $[K(\alpha) : K]$ on äärellinen. Lisäksi $L$ on algebrallinen, jos $[L : K]$ on äärellinen.*

Korollaarin jälkimmäisen väitteen implikaatiota ei voi kääntää. Esimerkiksi joukko $\{2^{1/n} \mid n \in \mathbb{N}\}$ virittää $\mathbb{Q}$:n algebrallisen laajennoksen, jonka aste on ääretön.

Nyt voidaan todistaa, että laajennoksen algebrallisuus on transitiivinen ominaisuus.

Lause 13.10. *Olkoot $K \subset L \subset M$ kuntia. Jos $L/K$ ja $M/L$ ovat algebrallisia laajennoksia, niin $M/K$ on algebrallinen.*

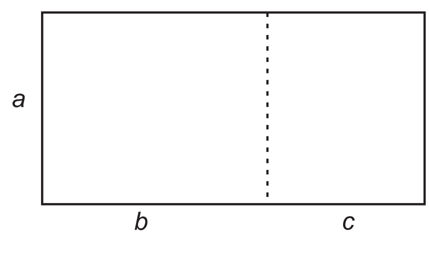
Todistus. Oletetaan, että $m \in M$. Olkoon $p = a_0 + a_1X + \cdots + a_nX^n$ alkion $m$ minimipolynomi kunnan $L$ suhteen. Merkitään $K_1 = K(a_0, \ldots, a_n)$. Koska $L$ on algebrallinen $K$:n suhteen ja $a_i \in L$ jokaisella $i$, laajennos $K_1$ on äärellinen lauseen 13.8 perusteella. Nyt $p \in K_1[X]$, joten $m$ on algebrallinen kunnan $K_1$ suhteen. Täten $[K_1(m) : K_1]$ on äärellinen, ja

$$[K_1(m) : K] = [K_1(m) : K_1] \cdot [K_1 : K] < \infty.$$

Edelleen $K(m) \subset K_1(m)$, joten $[K(m) : K] < \infty$. Lauseesta 13.7 seuraa, että $K(m)$ on algebrallinen $K$:n suhteen. Erityisesti siis $m$ on algebrallinen $K$:n suhteen, ja koska $m$ oli mielivaltainen, koko laajennos $M/K$ on algebrallinen. □

**13.2. Sovellus: Harppi–viivainkonstruktiot.** Edellä opittua teoriaa voidaan käyttää tiettyjen klassisten geometristen konstruktioiden tutkimiseen. Nämä konstruktiot, joista ehkä tunnetuin kulkee nimellä ympyrän neliöinti, ovat askarruttaneet matemaatikkojen mieltä antiikista 1800-luvulle saakka, jolloin niiden toteuttaminen saatiin viimein saatiin osoitettua mahdottomaksi algebrallisten menetelmien avulla.

Antiikin Kreikassa geometrialla oli erityisen tärkeä sija matemaattisessa kirjallisuudessa. Algebrallisten merkintöjen puuttuessa geometriaa käytettiin kaikkien matemaattisten (eli lähinnä geometristen ja lukuteoreettisten) tulosten todistamiseen. Luvut esitettiin eripituisina janoina: yhteenlasku tulkittiin kahden janan liittämiseksi peräkkäin, ja kahden luvun tulo tarkoitti sellaisen suorakulmion muodostamista, jonka sivut vastasivat kerrottavia lukuja. Näin voitiin todistaa esimerkiksi osittelulaki $a(b+c) = ab + ac$ jakamalla suorakulmio, jonka sivujen pituudet ovat $a$ ja $b + c$, kahdeksi suorakulmioksi, jotka vastasivat tuloja $ab$ ja $ac$.




Kuva 25. Geometrinen konstruktio osittelulain todistamiseksi

Perinteisen tarinan mukaan filosofi Platon[19] vaati, että geometriset konstruktiot olisi toteutettava vain harppia ja viivainta hyväksikäyttäen. Viivaimella sai

[19]Platon (428/427–348/347 eKr.), ateenalainen filosofi, Akatemian perustaja. Platon oli aikanaan huomattava vaikuttaja myös matematiikan alalla, vaikka hänen ei tiedetä itse tuottaneen omaperäisiä matemaattisia tuloksia.

piirtää rajattoman pitkän suoran kahden tunnetun pisteen kautta, ja harpilla oli sallittua piirtää ympyrä, jonka keskipiste ja säde tunnettiin. (Oikeastaan säännöt olivat vielä tiukemmat, mutta yhtäpitävät tässä esitettyjen kanssa.) Pian esiin nousi kolme ongelmaa, joita kreikkalaiset eivät pystyneet ratkaisemaan edes lukemattomien yritysten jälkeen:

1. *Ympyrän neliöinti.* On tuotettava sellaisen neliön sivu, jonka pinta-ala on sama kuin annetulla ympyrällä.
2. *Kuution kahdentaminen.* On tuotettava sellaisen kuution sivu, jonka tilavuus on kaksi kertaa annetun kuution tilavuus.
3. *Kulman kolmiajako.* On tuotettava kulma, jonka suuruus on kolmasosa annetun kulman suuruudesta.

Kreikkalaisten epäonnistuminen yllä mainittujen tehtävien ratkaisemisessa ei ollut osoitus heidän kyvyttömyydestään. Vuonna 1837 Pierre Wantzel nimittäin osoitti, että 2. ja 3. konstruktio eivät olisi mahdollisia suorittaa pelkästään harpilla ja viivaimella. Myös 1. kostruktio on mahdoton, mutta tämän todistaminen onnistui vasta, kun Ferdinand von Lindemann osoitti vuonna 1882 luvun $\pi$ transkendenttisuuden.

Selvitetään nyt, miten geometriset konstruktio-ongelmat voidaan formuloida algebran kielelle. Tarkasteltavana ovat pistejoukot $G \subset \mathbb{R}^2$, joita nimitetään *kuvioksi.* Kuvion $G$ *suora* on suora, joka kulkee $G$:n kahden pisteen kautta. Kuvion $G$ *ympyrä* taas on ympyrä, jonka keskipiste on $G$:ssä ja säde kahden $G$:n pisteen välinen etäisyys.

Olkoon annettu kuvio $G_0 \subset \mathbb{R}^2$. *Geometrinen konstruktio joukosta* $G_0$ on äärellinen jono kuvioita

$$G_0 \subset G_1 \subset \cdots \subset G_n,$$

missä $G_{i+1} = G_i \cup \{P_{i+1}\}$ ja $P_{i+1}$ on jokin kuvion $G_i$ suorien tai ympyröiden leikkauspiste. Sanotaan, että kuvio $G$ *voidaan konstruoida kuviosta* $G_0$, jos on olemassa geometrinen konstruktio $G_0 \subset \cdots \subset G_n$, missä $G_n = G$. Kuvion $G$ *kunta* $K_G$ on laajennos $\mathbb{Q}(A)$, missä $A$ sisältää kaikkien $G$:n pisteiden x- ja y-koordinaatit.

Seuraava lause antaa algebrallisen ehdon kuvion konstruoitavuudelle.

LAUSE 13.11. *Jos kuvio $G$ voidaan konstruoida kuviosta $G_0$, niin*

$$[K_G : K_{G_0}] = 2^n$$

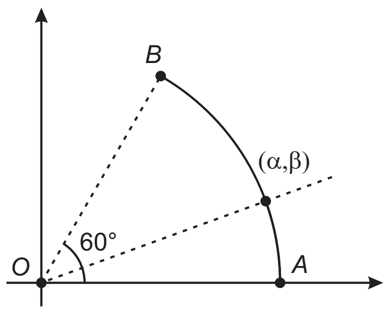
*jollain $n \in \mathbb{N}$.*

TODISTUS. Olkoon $G_0 \subset \cdots \subset G_n = G$ geometrinen konstruktio. Analyyttisen geometrian perusteista tiedetään, että jokaista kuvion $G_i$ suoraa ja ympyrää kuvaa polynomiyhtälö, jonka kertoimet ovat kunnassa $K_{G_i}$ ja joka on korkeintaan toista astetta. Edelleen tiedetään, että näiden suorien ja ympyröiden leikkauspisteiden löytämiseksi on ratkaistava korkeintaan toisen asteen yhtälöpari, jonka ratkaisut ovat muotoa $x = a_1 + b_1\sqrt{c}$ ja $y = a_2 + b_2\sqrt{c}$, missä $a_1, a_2, b_1, b_2, c \in K_{G_i}$. Täten $K_{G_{i+1}} \subset K_{G_i}(\sqrt{c})$. Koska luvun $\sqrt{c}$ minimipolynomi kunnan $K_{G_i}$ suhteen on korkeintaan toista astetta, saadaan lopulta $[K_{G_{i+1}} : K_{G_i}] \leq 2$. Väite seuraa tästä induktiolla, kun käytetään lausetta 12.3. $\square$

Yllä oleva lause pätee myös käänteisessä muodossa: jos aste $[K_G : K_{G_0}]$ on kakkosen potenssi, niin kuvio $G$ voidaan konstruoida kuviosta $G_0$. Tätä ei kuitenkaan tarvita silloin, kun konstruktioita osoitetaan mahdottomiksi, kuten seuraavassa esimerkissä tehdään.

Esimerkki 13.12. *Kulman kolmiajako.* Osoitetaan, että $60°$ kulmaa ei voi jakaa kolmeen osaan harpilla ja viivaimella. Valitaan koordinaatisto niin, että annettu 60 asteen kulma tulee suorien $OA$ ja $OB$ väliin, missä $O = (0,0)$, $A = (1,0)$ ja $B = (1/2, \sqrt{3}/2)$. Olkoon $G_0 = \{O, A, B\}$, jolloin $K_{G_0} = \mathbb{Q}(\sqrt{3})$, ja $[K_{G_0} : \mathbb{Q}] = 2$.

Oletetaan, että kulma $AOB$ voidaan jakaa kolmeen osaan. Tällöin syntyvän kulman kyljen ja origokeskisen yksikköympyrän leikkauspiste (joka siis myös voidaan konstruoida) on $(\alpha, \beta)$, missä $\alpha = \cos 20°$ ja $\beta = \sin 20°$. Oletuksen mukaan voidaan konstruoida kuvio $G$, joka sisältää pisteen $(\alpha, \beta)$.




Kuva 26. Kulman kolmiajako

Tutkitaan tarkemmin koordinaattia $\alpha$. Kolminkertaisen kulman kosinin kaavasta nähdään, että

$$\cos(3 \cdot 20°) = 4\cos^3 20° - 3\cos 20°.$$

Koska $\cos 60° = 1/2$, tästä seuraa, että $\alpha$ on polynomin $8X^3 - 6X - 1$ juuri. Koska tämä polynomi on lisäksi jaoton $\mathbb{Q}$:n suhteen esimerkiksi rationaalijuuritestin perusteella, se on minimipolynomin $\min(\mathbb{Q}, \alpha)$ liittoalkio. Siispä kyseisen minimipolynomin aste on 3, ja edelleen $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Lauseiden 13.11 ja 12.3 perusteella

$$[K_G : \mathbb{Q}] = [K_G : K_{G_0}] \cdot [K_{G_0} : \mathbb{Q}] = 2^n \cdot 2 = 2^{n+1}$$

jollain $n \in \mathbb{N}$, mutta toisaalta

$$[K_G : \mathbb{Q}] = [K_G : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K_G : \mathbb{Q}(\alpha)] \cdot 3.$$

Tämä on selvästi mahdotonta, joten kuviota $G$ ei voida konstruoida.

Tämä esimerkki osoittaa, että mielivaltaisen kulman kolmiajakamiseksi harpilla ja viivaimella ei voi olla olemassa yleistä menetelmää. Joitakin kulmia silti voidaan jakaa kolmeen osaan: esimerkiksi 30 asteen kulma voidaan konstruoida, mikä tarkoittaa sitä, että suoran kulman kolmiajako onnistuu.