Waring-Hilbertin lause

Esa Vesalainen

Syyskuu 2008
Helsingin yliopisto
Matematiikan ja tilastotieteen laitos
Kandidaatin tutkielma
Ohjaaja: Hans-Olav Tylli

Sisältö

Luku 1

Johdanto

Tavoitteemme on todistaa seuraava kuuluisa klassinen lukuteorian tulos, Waring-Hilbertin lause:

Lause 1.1 (Waring-Hilbert)**.** *Jokaista $k \in \mathbb{Z}_+$ kohti on olemassa sellainen luku $s(k) \in \mathbb{Z}_+$, että kaikki luvut $n \in \mathbb{Z}_+$ voidaan esittää muodossa*

$$n = n_1^k + n_2^k + ... + n_{s(k)}^k,$$

missä $n_1, n_2, ..., n_{s(k)} \in \mathbb{Z}_+ \cup \{0\}$.

Nykyisin on tapana katsoa, että tuloksen konjekturoi ensimmäisenä E. Waring 1700-luvulla teoksessaan *Meditationes Algebraicae*. L. Euler yritti todistaa lauseen erikoistapauksessa $k = 2$ siinä kuitenkaan täysin onnistumatta. Ensimmäinen todellinen edistysaskel kohti ongelman ratkaisua oli J. L. Lagrangen kuuluisa neljän neliön lause vuodelta 1770, jonka mukaan jokainen luonnollinen luku on enintään neljän neliöluvun summa, eli lauseen 1.1 merkinnöin voidaan valita $s(2) = 4$. Vaikka 1800-luvun kuluessa saatiin menestyksekkäästi todistettua erikoistapaukset $k \in \{3, 4, 5, 6, 7, 8, 10\}$, todisti konjektuurin kokonaan vasta D. Hilbert 1909. Hänen todistuksensa perustui varsin yleisen algebrallisen identiteetin olemassaolon todistamiseen. 1910-luvulla G. H. Hardy ja J. E. Littlewood esittivät generoiviin funktioihin perustuvan analyyttisen todistuksen. 1940-luvulla Yu. V. Linnik esitti probleemalle täysin alkeellisen todistuksen.

Esitämme Hilbertin alkuperäiseen ideaan perustuvan todistuksen, niin kuin sitä ovat parannelleet F. Hausdorff, E. Stridsberg, W. J. Ellison, H. Koch ja H. Pieper. Esityksemme perustuu pääasiassa artikkeliin [El], joka sisältää myös probleeman historiaa sekä laajat lähdeviittaukset. Kuitenkin kyseisen artikkelin esittämän todistuksen loppupuolella esiintyvien lukuisten vakavien epätarkkuuksien vuoksi nojaamme myös paljon teoksen [K&P] lukuun 5. Teknisistä syistä todistamme Waring-Hilbertin lauseesta seuraavan ekvivalentin muodon:

Lause 1.2. *Jokaista $k \in \mathbb{Z}_+$ kohti löytyvät sellaiset $A \in \mathbb{Z}_+$, $M \in \mathbb{Z}_+$ sekä $\lambda_1, \lambda_2, ..., \lambda_M \in \mathbb{Q}_+$ että kaikki luvut $n \in \mathbb{Z}_+$, joilla $n > A$, voidaan esittää muodossa $n = \sum_{\ell=1}^{M} \lambda_\ell n_\ell^k$, missä $n_1, n_2, ..., n_M \in \mathbb{Z}_+ \cup \{0\}$.*

Selvästi lause 1.2 seuraa Waring-Hilbertin lauseesta; Waring-Hilbertin lauseen vallitessahan riittää valita $A = 1$, $M = s(k)$ ja $\lambda_1 = \lambda_2 = ... = \lambda_M = 1$.

Oletetaan nyt, että lause 1.2 pitää paikkaansa ja kiinnitetään jokin $k \in \mathbb{Z}_+$. Esitetään lauseen 1.2 antamat kertoimet $\lambda_1, \lambda_2, ..., \lambda_M$ muodossa $\lambda_\ell = \frac{p_\ell}{q_\ell}$, missä $p_\ell, q_\ell \in \mathbb{Z}_+$, kaikilla $\ell \in \{1, 2, ..., M\}$. Jos nyt merkitään $\sigma = q_1 q_2 \cdots q_M$, niin kertomalla identiteetti $n = \sum_{\ell=1}^{M} \lambda_\ell n_\ell^k$ luvulla σ saadaan $\sigma n = \sum_{\ell=1}^{M} \sigma\lambda_\ell n_\ell^k$, missä siis $\sigma\lambda_\ell = p_\ell q_1 \cdots q_{\ell-1} q_{\ell+1} \cdots q_M \in \mathbb{Z}_+$. Siis kaikki lukua σA suuremmat luvulla σ jaolliset luonnolliset luvut voidaan esittää enintään $\sum_{\ell=1}^{M} \sigma\lambda_\ell$ luvun k-asteisten potenssien summina. Toisaalta, jos nyt $n \in \mathbb{Z}_+$, $n > A$, on mielivaltainen, niin tietenkin jakoyhtälön nojalla löytyvät sellaiset $m \in \mathbb{Z}_+ \cup \{0\}$ ja $r \in \{0, 1, ..., \sigma - 1\}$, että $n = \sigma m + r$. Jos nyt $\sigma m = \sum_{\ell=1}^{M} \sigma\lambda_\ell m_\ell^k$ $(m_1, m_2, ..., m_M \in \mathbb{Z}_+ \cup \{0\})$, on lauseen 1.2 mukainen esitys, niin

$$n = \sum_{\ell=1}^{M} \sigma\lambda_\ell m_\ell^k + \sum_{1}^{r} 1^k,$$

eli n on enintään $\sum_{\ell=1}^{M} \sigma\lambda_\ell + \sigma - 1$ luvun k-asteisten potenssien summa.

Toisaalta, jos $n \in \mathbb{Z}_+$ on sellainen, että $n \leqslant \sigma A$, niin tietenkin $n = \sum_{1}^{n} 1^k$. Jokainen luonnollinen luku on siis lauseen 1.2 vallitessa enintään $\max\{\sum_{\ell=1}^{M} \sigma\lambda_\ell + \sigma - 1, \sigma A\}$ luvun k-asteisten potenssien summa ja Waring-Hilbertin lause pätee.

Erityisesti huomataan, että lauseiden 1.1 ja 1.2 väitteet ovat yhtäpitäviä keskenään jokaiselle eksponentille $k \in \mathbb{Z}_+$ erikseen. Tätä havaintoa tarvitaan luvussa 5.

Todistuksen avain on neljännessä luvussa todistettava lemma 4.1, mutta sen todistuksessa tarvitaan joitakin työkaluja konveksisten joukkojen teoriasta sekä alkeellisesta lukuteoriasta. Nämä tarvittavat työkalut esitellään seuraavissa kahdessa luvussa.

Luku 2

Lagrangen neljän neliön lause

Waring-Hilbertin lauseen todistamisessa tarvitsemme seuraavaa kuuluisaa teoreemaa, jonka ensimmäisen kokonaisen todistuksen esitti J. L. Lagrange vuonna 1770.

Lause 2.1 (Lagrangen neljän neliön lause)**.** *Jokainen $n \in \mathbb{Z}_+$ on esitettävissä enintään neljän neliöluvun summana.*

Todistuksessa seuraamme klassikkoteosta [H&W]. Koska $1 = 1^2$ ja $2 = 1^2 + 1^2$, riittää aritmetiikan peruslauseen ja seuraavan Eulerin identiteetin perusteella todistaa Lagrangen lause vain parittomille alkuluvuille.

Lemma 2.2 (Eulerin identiteetti)**.** *Kaikilla $a, b, c, d, \alpha, \beta, \gamma, \delta \in \mathbb{Z}$ pätee*

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = (a\alpha + b\beta + c\gamma + d\delta)^2 + (a\beta - b\alpha + c\delta - d\gamma)^2 + (a\gamma - c\alpha + d\beta - b\delta)^2 + (a\delta - d\alpha + b\gamma - c\beta)^2$$

Todistus. Suora lasku.

Lause 2.3. *Jokainen pariton alkuluku on esitettävissä neljän neliön summana.*

Todistus. Olkoon p pariton alkuluku. Osoitetaan ensin, että löytyy luonnollinen luku $m \in \{1, 2, ..., p-1\}$ siten, että $mp = x^2 + y^2 + 1^2 + 0^2$, joillakin $x, y \in \mathbb{Z}$. $\frac{p+1}{2}$ lukua $0^2, 1^2, 2^2, ..., (\frac{p-1}{2})^2$ ovat keskenään epäkongruentteja modulo p. Niin myös $\frac{p+1}{2}$ lukua $-1-0^2, -1-1^2, -1-2^2, ..., -1-(\frac{p-1}{2})^2$. Siispä kyyhkyslakkaperiaatteen nojalla välttämättä $x^2 \equiv -1 - y^2 \pmod{p}$ joillakin $x, y \in \{0, 1, 2, ..., \frac{p-1}{2}\}$, eli $x^2 + y^2 + 1 = mp$ jollakin $m \in \mathbb{Z}$. Selvästi tässä $m > 0$. Toisaalta $mp = x^2 + y^2 + 1 \leqslant (\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1 < p^2$, joten $m < p$. Siis $1 \leqslant m \leqslant p - 1$.

Voidaan siis valita **pienin** $m_0 \in \mathbb{Z}_+$, jolle $m_0 p$ on neljän neliön summa – sanokaamme $m_0 p = a^2 + b^2 + c^2 + d^2$, missä $a, b, c, d \in \mathbb{Z}$. Edellä sanotun nojalla varmasti $m_0 < p$. Jos nyt $m_0 = 1$, niin $p = m_0 p = a^2 + b^2 + c^2 + d^2$ ja asia on selvä. Tarkastellaan siis tilannetta, missä $m_0 > 1$.

Jos m_0 on parillinen, niin välttämättä parillinen määrä luvuista a, b, c, d on parillisia. Jos täsmälleen kaksi niistä ovat parillisia niin voidaan olettaa, että nimenomaan a ja b ovat parillisia ja c ja d parittomia. Nyt joka tapauksessa luvut $a+b, a-b, c+d, c-d$ ovat kaikki varmasti parillisia ja saadaan

$$\frac{m_0}{2} p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2,$$

vastoin luvun m_0 määritelmää. Siis m_0 on välttämättä pariton, ja erityisesti $m_0 \geqslant 3$.

Seuraavaksi todetaan, että kaikki luvut a, b, c, d eivät voi olla jaollisia luvulla m_0, sillä tällöin olisi $m_0 \mid p$, mikä on mahdotonta. Kun nyt valitaan $\alpha, \beta, \gamma, \delta$ lukujen a, b, c, d (vastaavasti) itseisesti pienimmiksi jäännöksiksi modulo m_0, on

$$\alpha \equiv a, \beta \equiv b, \gamma \equiv c, \text{ja } \delta \equiv d \pmod{m_0},$$

lisäehdoin $\alpha, \beta, \gamma, \delta \in \mathbb{Z} \cap \left]-\frac{m_0}{2}, \frac{m_0}{2}\right[$ sekä $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 > 0$. Toisaalta myös

$$0 < \alpha^2 + \beta^2 + \gamma^2 + \delta^2 < 4\left(\frac{m_0}{2}\right)^2 = m_0^2,$$

ja

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m_0},$$

eli $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = m_0 m_1$ jollakin $m_1 \in \{1, 2, ..., m_0 - 1\}$.

Eulerin identiteettiä käyttämällä: $m_0^2 m_1 p = m_0 p \cdot m_0 m_1 = (a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = A^2 + B^2 + C^2 + D^2$, missä

$$\begin{cases} A = a\alpha + b\beta + c\gamma + d\delta \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m_0}, \\ B = a\beta - b\alpha + c\delta - d\gamma \equiv ab - ba + cd - dc \equiv 0 \pmod{m_0}, \\ C = a\gamma - c\alpha + d\beta - b\delta \equiv ac - ca + db - bd \equiv 0 \pmod{m_0}, \\ D = a\delta - d\alpha + b\gamma - c\beta \equiv ad - da + bc - cb \equiv 0 \pmod{m_0}. \end{cases}$$

Siis $m_1 p = \left(\frac{A}{m_0}\right)^2 + \left(\frac{B}{m_0}\right)^2 + \left(\frac{C}{m_0}\right)^2 + \left(\frac{D}{m_0}\right)^2$, vastoin luvun m_0 määritelmää. Täten $m_0 = 1$ ja $p = m_0 p = a^2 + b^2 + c^2 + d^2$ on neljän neliön summa. Q.E.D.

Luku 3

Konveksit peitteet

Olkoon $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}\}$ ja V jokin äärellisulotteinen $\mathbb{K}$-vektoriavaruus. Merkitään $N = \dim V$. Osajoukkoa $S \subseteq V$ sanotaan *konveksiksi* jos kaikilla $\alpha \in [0,1] \cap \mathbb{K}$ ja $x, y \in S$ on myös $\alpha x + (1-\alpha)y \in S$. Tietenkin V itse on konveksi joukko ja konveksien joukkojen leikkaukset ovat myös selvästi konvekseja. Siis on mielekästä määritellä joukon S *pienin konveksi peite* $h(S)$ kaikkien joukon S sisältävien konveksien joukkojen leikkauksena. Siis $h(S)$ on **konveksi** joukko, joka sisältyy jokaiseen joukon S sisältävään konveksiin joukkoon. Lainaamme kirjasta [Eg] C. Carathéodoryn nimeä kantavan lauseen.

Lemma 3.1. *Jokainen $a \in h(S)$ on esitettävissä muodossa $a = \sum_{\ell=0}^{M} \lambda_\ell s_\ell$, missä $M \in \mathbb{Z}_+$, $s_0, s_1, ..., s_M \in S$, $\lambda_0, \lambda_1, ..., \lambda_M \in [0,1] \cap \mathbb{K}$, ja $\sum_{\ell=0}^{M} \lambda_\ell = 1$.*

Todistus. Merkitään $T = \{\sum_{\ell=0}^{M} \lambda_\ell s_\ell | s_\ell \in S, \lambda_\ell \in [0,1] \cap \mathbb{K}, \sum \lambda_\ell = 1\}$. Triviaalisti $S \subseteq T$. Joukko T on joukko, sillä jos $\sum_{\ell=0}^{M} \lambda_\ell s_\ell, \sum_{\ell=0}^{P} \mu_\ell r_\ell \in T$ (missä jälleen $M, P \in \mathbb{Z}_+$, $s_\ell, r_\ell \in S$, $\lambda_\ell, \mu_\ell \in [0,1] \cap \mathbb{K}$, ja $\sum \lambda_\ell = \sum \mu_\ell = 1$), niin kaikilla $\alpha \in [0,1] \cap \mathbb{K}$

$$\alpha \sum_{\ell=0}^{M} \lambda_\ell s_\ell + (1-\alpha) \sum_{\ell=0}^{P} \mu_\ell r_\ell = \sum_{\ell=0}^{M} \alpha\lambda_\ell s_\ell + \sum_{\ell=0}^{P} (1-\alpha)\mu_\ell r_\ell \in T,$$

onhan $\alpha \sum \lambda_\ell + (1-\alpha) \sum \mu_\ell = \alpha + (1-\alpha) = 1$. Siispä $h(S) \subseteq T$.

Toisaalta, varmasti $s \in h(S)$ kaikilla $s \in S$, ja jos $h(S)$ sisältää kaikki summat $\sum_{\ell=0}^{P} \lambda_\ell s_\ell$ (missä jälleen $s_\ell \in S$ ja $\lambda_\ell \in [0,1] \cap \mathbb{K}$ s.e. $\sum \lambda_\ell = 1$) kaikilla $P \in \{1, 2, ..., M\}$, jollakin $M \in \mathbb{Z}_+$, niin joukon $h(S)$ konveksisuuden nojalla myös

$$\sum_{\ell=0}^{M+1} \lambda_\ell s_\ell = \sum_{k=0}^{M} \lambda_k \cdot \sum_{\ell=0}^{M} \frac{\lambda_\ell}{\sum_{k=0}^{M} \lambda_k} s_\ell + \lambda_{M+1} s_{M+1} \in h(S),$$

kunhan vain edelleen $\sum_{\ell=0}^{M+1} \lambda_\ell = 1$ ja $\lambda_0, ..., \lambda_{M+1} \in [0,1] \cap \mathbb{K}$. Siis induktiolla nähdään, että $T \subseteq h(S)$, ja itse asiassa $T = h(S)$. q.e.d.

Lemma 3.2. *Olkoot $x_0, x_1, ..., x_{N+1}$ avaruuden V vektoreita. Tällöin löytyvät kertoimet $\alpha_0, \alpha_1, ..., \alpha_{N+1} \in \mathbb{K}$ joille $\sum_{\ell=0}^{N+1} \alpha_\ell x_\ell = 0$, $\sum_{\ell=0}^{N+1} \alpha_\ell = 0$, ja $\alpha_\ell \neq 0$ ainakin yhdellä $\ell \in \{0, 1, ..., N+1\}$.*

Todistus. Suoraan luvun N määritelmän nojalla löytyvät sellaiset luvut $\beta_0, \beta_1, ..., \beta_N \in \mathbb{K}$, joille $\sum_{\ell=0}^{N} \beta_\ell x_\ell = 0$. Ilman yleisyyden menettämistä voidaan olettaa, että $\beta_0 \neq 0$. Samoin löytyvät luvut $\gamma_1, \gamma_2, ..., \gamma_{N+1} \in \mathbb{K}$ siten, että $\sum_{\ell=1}^{N+1} \gamma_\ell x_\ell = 0$, ja kertomalla luvut $\gamma_1, ..., \gamma_{N+1}$ sopivalla vakiolla, voidaan olettaa, että $\sum_{\ell=0}^{N} \beta_\ell = \sum_{\ell=1}^{N+1} \gamma_\ell$. Valitaan nyt

$$\begin{cases} \alpha_0 = \beta_0, \\ \alpha_\ell = \beta_\ell - \gamma_\ell, \text{jokaiselle } \ell \in \{1, 2, ..., N\}, \\ \alpha_{N+1} = -\gamma_{N+1}. \end{cases}$$

Selvästi nyt $\sum_{\ell=0}^{N+1} \alpha_\ell = \sum_{\ell=0}^{N} \beta_\ell - \sum_{\ell=1}^{N+1} \gamma_\ell = 0$, $\alpha_0 \neq 0$ ja $\sum_{\ell=0}^{N+1} \alpha_\ell x_\ell = \sum_{\ell=0}^{N} \beta_\ell x_\ell - \sum_{\ell=1}^{N+1} \gamma_\ell x_\ell = 0 - 0 = 0$, ja lemma on todistettu.

Lause 3.3 (Carathéodory)**.** *Jokainen $a \in h(S)$ on esitettävissä muodossa $a = \sum_{\ell=0}^{N} \lambda_\ell s_\ell$, missä $s_0, s_1, ..., s_N \in S$, $\lambda_0, \lambda_1, ..., \lambda_N \in [0,1] \cap \mathbb{K}$, ja $\sum_{\ell=0}^{N} \lambda_\ell = 1$.*

Todistus. Olkoon siis $a \in h(S)$ mielivaltainen. Lemman 3.1 nojalla löytyvät sellaiset $M \in \mathbb{Z}_+$, $s_0, ..., s_M \in S$, ja $\lambda_0, ..., \lambda_M \in [0,1] \cap \mathbb{K}$, että $a = \sum_{\ell=0}^{M} \lambda_\ell s_\ell$ ja $\sum_{\ell=0}^{M} \lambda_\ell = 1$. Jos $M \leqslant N$, niin asia on selvä. Oletetaan siis, että $M > N$.

Lemman 3.2 nojalla löytyvät luvut $\alpha_0, ..., \alpha_M \in \mathbb{K}$, joille $\sum_{\ell=0}^{M} \alpha_\ell s_\ell = 0$, $\sum_{\ell=0}^{M} \alpha_\ell = 0$ ja $\alpha_\ell \neq 0$ jollakin $\ell \in \{0, ..., M\}$. Määritellään

$$\tau = \max \left\{ -\frac{\lambda_\ell}{\alpha_\ell} \,\middle|\, \ell \in \{0, ..., M\}, \alpha_\ell > 0 \right\}.$$

Tässä yhtälön oikealla puolella esiintyvä joukko ei ole tyhjä, sillä $\alpha_\ell \neq 0$ ainakin yhdellä $\ell \in \{0, ..., M\}$ ja $\sum_{\ell=0}^{M} \alpha_\ell = 0$, eli varmasti $\alpha_\ell > 0$ ainakin yhdellä $\ell \in \{0, ..., M\}$. On helppo nähdä, että $\tau\alpha_\ell \geqslant -\lambda_\ell$, eli $\tau\alpha_\ell + \lambda_\ell \geqslant 0$, kaikilla $\ell \in \{0, ..., M\}$. Lisäksi $\tau\alpha_i + \lambda_i = 0$ jollakin $i \in \{0, ..., M\}$, ja $\sum_{\ell=0}^{M} (\tau\alpha_\ell + \lambda_\ell) = 1$. Ja koska

$$a = \sum_{\ell=0}^{M} (\tau\alpha_\ell + \lambda_\ell) s_\ell = \sum_{\substack{\ell=0, \\ \ell \neq i}}^{M} (\tau\alpha_\ell + \lambda_\ell) s_\ell,$$

on vektorille a saatu halutunkaltainen esitys M vektorin summana. Tätä konstruktiota toistamalla saadaan lyhyempiä ja lyhyempiä halutunkaltaisia esityksiä vektorille a, ja lopulta saavutetaan tavoiteltu $N+1$ vektorin mittainen esitys. Q.E.D.

Oletamme luvun loppuun saakka, että V on äärellisulotteinen $\mathbb{R}$-vektoriavaruus, jonka dimensio N on äärellinen, ja joka on varustettu tavanmukaisella topologialla. Lisäksi oletamme, $|\cdot|$ on avaruuden V tavallinen euklidinen normi, joka tietenkin indusoi avaruuteen V edellä mainitun topologian.

Lemma 3.4. *Kompaktin joukon $S \subseteq V$ konveksi peite $h(S)$ on myös kompakti.*

Todistus. Merkitään

$$\Delta = \left\{ \langle \alpha_0, \alpha_1, ..., \alpha_N \rangle \in \mathbb{R}^{N+1} \,\middle|\, \alpha_\ell \geqslant 0, \sum \alpha_\ell = 1 \right\}.$$

Tihonovin lauseen nojalla $\Delta \times S^{N+1}$ on kompakti joukko ja Carathéodoryn lauseen nojalla jatkuva kuvaus

$$f = \left\langle \langle \alpha_0, \alpha_1, ..., \alpha_N \rangle, s_0, s_1, ..., s_N \right\rangle \longmapsto \sum_{\ell=0}^{N} \alpha_\ell s_\ell : \Delta \times S^{N+1} \longrightarrow h(S),$$

on surjektio. Siis $h(S) = \operatorname{Im} f$ on kompakti. q.e.d.

Seuraavaksi lainaamme useita sekalaisia tuloksia teoksesta [Eg]. Luvun loppuun saakka $M \subsetneq V$ merkitsee epätyhjää konveksia joukkoa. Merkitsemme symbolilla $L(M)$ sitä pienintä avaruuden V affiinia aliavaruutta joka sisältää joukon M. Jos $M \subseteq A \subseteq V$, niin symbolit $\operatorname{int}_A M$ ja $\partial_A M$ merkitsevät tavanmukaisesti joukon $M \cap A$ sisäpisteiden ja (vastaavasti) reunapisteiden joukkoja avaruuden V topologisessa aliavaruudessa A. Lisäksi $d(x, A)$ merkitsee pisteen $x \in V$ etäisyyttä joukosta $A \subseteq V$, $A \neq \emptyset$.

Lause 3.5. *Olkoon $\delta \in \mathbb{R}_+$. Tällöin joukko $M_\delta = \left\{ x \in V \middle| d(x, M) < \delta \right\}$ on konveksi.*

Todistus. Olkoot $x, y \in M_\delta$. Tällöin löytyvät $x', y' \in M$ joille $|x - x'| < \delta$ ja $|y - y'| < \delta$. Olkoon $\lambda \in]0, 1[$ mielivaltainen. Tietenkin $\lambda x' + (1-\lambda)y' \in M$, ja koska

$$\begin{aligned} \left| \lambda x + (1-\lambda)y - \left(\lambda x' + (1-\lambda)y' \right) \right| &\leqslant \left| \lambda x - \lambda x' \right| + \left| (1-\lambda)y - (1-\lambda)y' \right| \\ &= \lambda |x - x'| + (1-\lambda)|y - y'| < \lambda\delta + (1-\lambda)\delta = \delta, \end{aligned}$$

on oltava $d\big(\lambda x+(1-\lambda)y, M\big) < \delta$. Siis myös $\lambda x+(1-\lambda)y \in M_\delta$, mistä väite suoraan seuraakin.

Huomautetaan, että tästä lauseesta seuraa suoraan, että $\overline{M} = \bigcap_{\delta>0} M_\delta$ on konveksien joukkojen leikkauksena konveksi.

Lause 3.6. *Olkoot $x \in M$ ja $y \in \operatorname{int} M$. Tällöin jokaisella $\lambda \in]0,1[$ on myös $\lambda y + (1-\lambda)x \in \operatorname{int} M$.*

Todistus. Löytyy $\delta \in \mathbb{R}_+$ jolle $y \in B(y,\delta) \subseteq M$ (missä tietenkin $B(y,\delta)$ on y-keskinen δ-säteinen avoin kuula). Olkoon $\lambda \in]0,1[$.

Olkoon nyt $z \in B(\lambda y + (1-\lambda)x, \lambda\delta)$. Tällöin

$$\big|z - \big(\lambda y + (1-\lambda)x\big)\big| < \lambda\delta,$$

ja siis

$$\left|\frac{z}{\lambda} + \frac{1-\lambda}{\lambda}x - y\right| < \delta.$$

Nyt $\frac{z}{\lambda} + \frac{\lambda-1}{\lambda}x \in B(y,\delta) \subseteq M$, ja toisaalta

$$z = \lambda\left(\frac{z}{\lambda} + \frac{\lambda-1}{\lambda}x\right) + (\lambda-1)x \in M.$$

Siispä $B\big(\lambda x + (1-\lambda)y, \lambda\delta\big) \subseteq M$, eli $\lambda y + (1-\lambda)x \in \operatorname{int} M$, ja väite on todistettu.

Tästä lauseesta seuraa triviaalisti, että $\operatorname{int} M$ on konveksi joukko. Lisäksi saamme:

Korollaari 3.7. *Olkoot $x \in \overline{M}$ ja $y \in \operatorname{int} M$. Tällöin jokaisella $\lambda \in]0,1[$ on myös $\lambda y + (1-\lambda)x \in \operatorname{int} M$.*

Todistus. On olemassa $\delta \in \mathbb{R}_+$ jolle $B(y,\delta) \subseteq M$. Valitaan jokin piste $u \in B\left(x, \frac{\delta\lambda}{1-\lambda}\right) \cap M$. Merkitään lisäksi

$$v = y - \frac{1-\lambda}{\lambda}(u-x).$$

Tällöin tietenkin

$$|v-y| < \frac{1-\lambda}{\lambda}\frac{\delta\lambda}{1-\lambda} = \delta,$$

eli $v \in B(y,\delta) \subseteq M$. Nyt lauseen 3.6 nojalla

$$\begin{aligned}\lambda y + (1-\lambda)x &= \lambda y - \lambda\frac{1-\lambda}{\lambda}(u-x) + (1-\lambda)u \\ &= \lambda v + (1-\lambda)u \in \operatorname{int} M. \qquad \text{q.e.d.}\end{aligned}$$

Lause 3.8. *Oletetaan, että* $\operatorname{int} M \neq \emptyset$. *Tällöin* $\overline{M} = \overline{\operatorname{int} M}$ *ja joukoilla* M *ja* $\overline{M}$ *on samat sisäpisteet.*

Todistus. Koska $\operatorname{int} M \subseteq M$ niin tietenkin $\overline{\operatorname{int} M} \subseteq \overline{M}$. Oletetaan nyt, että $x \in \overline{M}$ on mielivaltainen. Olkoon $y \in \operatorname{int} M$. Nyt korollaarin 3.7 nojalla jokaisella $\lambda \in]0,1[$ on $\lambda y + (1-\lambda)x \in \operatorname{int} M$. Erityisesti

$$x = \lim_{n \longrightarrow \infty} \left(\frac{1}{n} y + \left(1 - \frac{1}{n} \right) x \right) \in \overline{\operatorname{int} M}.$$

Siispä $\overline{M} \subseteq \overline{\operatorname{int} M}$, ja asia on selvä.

Samoin tosiasiasta $M \subseteq \overline{M}$ seuraa, että $\operatorname{int} M \subseteq \operatorname{int} \overline{M}$. Oletetaan siis, että $x \in V \setminus \operatorname{int} M$ on mielivaltainen. Olkoon $y \in \operatorname{int} M$. Koska nyt jokaisella $\lambda \in]0,1[$ on

$$x = \lambda \left(y - \frac{1}{\lambda}(y-x) \right) + (1-\lambda) y,$$

ei koskaan voi olla $y - \frac{1}{\lambda}(y-x) \in \overline{M}$, sillä muutenhan korollaarin 3.7 nojalla olisi $x \in \operatorname{int} M$. Toisaalta

$$x = \lim_{n \longrightarrow \infty} \left(y - \frac{1}{1-n^{-1}}(y-x) \right),$$

eli $x \notin \operatorname{int} \overline{M}$. Täten $V \setminus \operatorname{int} M \subseteq V \setminus \operatorname{int} \overline{M}$ ja siten myös $\operatorname{int} M = \operatorname{int} \overline{M}$.

Aivan erityisesti tästä lauseesta seuraa, että myös

$$\operatorname{int}_{L(M)} M = \operatorname{int}_{L(M)}(\operatorname{cl}_{L(M)} M), \text{ ja } \operatorname{cl}_{L(M)}(\operatorname{int}_{L(M)} M) = \operatorname{cl}_{L(M)} M.$$

Lause 3.9. *Joukolla* M *on sisäpisteitä avaruudessa* $L(M)$.

Todistus. Merkitään $n = \dim L(M)$. Joukon M on sisällettävä $n+1$ pistettä $v_0, v_1, ..., v_n$ siten, että vektorit $v_1 - v_0, v_2 - v_0, ..., v_n - v_0$ ovat lineaarisesti riippumattomia avaruudessa V. Nyt joukko

$$\Delta \stackrel{\text{def}}{=} \left\{ \sum_{\ell=0}^{n} \lambda_\ell v_\ell \middle| \lambda_0, ..., \lambda_n \in]0,1[\,, \sum_{\ell=0}^{n} \lambda_\ell = 1 \right\} \subseteq M,$$

on avoin simpleksi avaruudessa $L(M)$, eli jokaisella $x \in \Delta$ on $x \in \operatorname{int}_{L(M)} M$ ja tavoite on saavutettu.

Lopuksi lainaamme teoksesta [G&H] seuraavan tärkeän tuloksen:

Lause 3.10. *Olkoon* $p \in \partial M$. *Tällöin löytyy avaruuden* V *hypertaso* τ *jolle* $p \in \tau$ *ja* $\tau \cap \operatorname{int} M = \emptyset$.

Todistus. Olkoot $\langle x_n\rangle_{n=1}^{\infty}$ jono joukon M ulkopisteitä, joille $\lim_{n\to\infty} x_n = p$. Olkoon jokaisella $n \in \mathbb{Z}_+$ y_n se joukon $\overline{M}$ piste, joka on lähinnä pistettä x_n. Määritellään pisteet

$$a_n = \frac{x_n - y_n}{|x_n - y_n|}.$$

Koska $|a_n| = 1$ jokaisella $n = 1, 2, ...$, voidaan (tarvittaessa rajoittumalla jonon $\langle a_n\rangle$ osajonoon) olettaa, että $\lim_{n\to\infty} a_n = a \in V$. Merkitään

$$\tau_n = \{x \in V | a_n \cdot x = a_n \cdot x_n\}.$$

Nyt jokainen τ_n on selvästi avaruuden V hypertaso. Lisäksi millekään $n \in \mathbb{Z}_+$ ei voi olla $\tau_n \cap \operatorname{int} M \neq \emptyset$, sillä jos jollakin $n \in \mathbb{Z}_+$ löytyisi $z \in \tau_n \cap \operatorname{int} M$, niin pisteet y_n, z ja x_n olisivat suorakulmaisen kolmion kärjet. Koska lauseen 3.6 nojalla

$$w \overset{\text{def}}{=} \frac{|y_n - x_n|}{|y_n - x_n| + |z - x_n|} y_n + \frac{|z - x_n|}{|y_n - x_n| + |z - x_n|} z \in \operatorname{int} M,$$

ja koska w selvästi on pisteen x_n projektio pisteitä y_n ja z yhdistävälle suoralle, olisi $|x_n - w| < |x_n - y_n|$, vastoin pisteen y_n määritelmää.

Määritellään nyt viimein $\tau = \{x \in V | a \cdot x = a \cdot p\}$. Tietenkin $p \in \tau$. Toisaalta, jos olisi olemassa $z \in \tau \cap \operatorname{int} M$, niin voitaisiin määritellä jono $\langle z_n\rangle_{n=1}^{\infty}$:

$$z_n = x_n + (z - p) - \big(a_n \cdot (z - p)\big) a_n,$$

jolloin

$$\begin{aligned} a_n \cdot x_n &= a_n \cdot x_n + a_n \cdot (z - p) - \big(a_n \cdot (z - p)\big) a_n \cdot a_n \\ &= a_n \cdot x_n + \big(a_n \cdot (z - p)\big)(1 - |a_n|^2) = a_n \cdot x_n, \end{aligned}$$

eli $z_n \in \tau_n \subseteq V \setminus \operatorname{int} M$. Toisaalta

$$\begin{aligned} V \setminus \operatorname{int} M \ni \lim_{n\to\infty} z_n &= \lim_{n\to} \Big(x_n + (z - p) - \big(a_n \cdot (z - p)\big) a_n\Big) \\ &= p + z - p - \big(a \cdot (z - p)\big) a = z \in \operatorname{int} M, \end{aligned}$$

mikä on mahdotonta. Siis halutunkaltainen hypertaso on olemassa. q.e.d.

Erityisesti tästä viimeisestä lauseesta seuraa, että jokaista reunapistettä $p \in \partial_{L(M)} M$ kohti löytyy avaruuden $L(M)$ hypertaso τ jolle $p \in \tau$ mutta kuitenkin $\tau \cap \operatorname{int}_{L(M)} M = \emptyset$.

Luku 4

Avainlemma

Tarkasteltavan Waring-Hilbertin lauseen todistuksen ydin on pian todistettava lemma 4.2, mutta ennen sitä tarvitsemme vielä yhden teknisen lemman:

Lemma 4.1. *Olkoot V äärellisulotteinen $\mathbb{R}$-vektoriavaruus varustettuna tavanmukaisella topologialla sekä euklidisella normilla $|\cdot|$, $N = \dim V$, $B \subseteq \mathbb{R}^N$ sellainen kompakti joukko, että $\iint\cdots\int_B \mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_N$ on olemassa Riemann-integraalina ja positiivinen, x_0 joukon B sisäpiste ja $f : B \longrightarrow V$ jatkuva kuvaus. Tällöin*

$$g = \frac{\iint\cdots\int_B f(x_1, x_2, ..., x_N)\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_N}{\iint\cdots\int_B \mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_N} \in h(\mathrm{Im}\, f).$$

Todistus. Olkoon $L \in \mathbb{R}_+$ niin iso, että $B \subseteq [-L, L]^N$, ja olkoon $N_0 \in \mathbb{Z}_+$ niin iso, että $\frac{\sqrt{N}}{N_0}$-säteinen ja x_0-keskinen suljettu kuula $\overline{B^N}\left(x_0, \frac{\sqrt{N}}{N_0}\right)$ sisältyy joukkoon B. Määritellään lisäksi funktion f jatko $\widetilde{f}$ kuutioon $[-L, L]^N$

$$\widetilde{f} = x \longmapsto \begin{cases} f(x), \text{jos } x \in B \\ 0, \text{jos } x \notin B \end{cases} : [-L, L]^N \longrightarrow V,$$

ja olkoon vielä $\chi_B : \mathbb{R}^N \longrightarrow [0, 1]$ joukon B tavanmukainen karakteristinen funktio.

Määritellään kaikille $\nu = N_0, N_0 + 1, ...$

$$I_\nu = \sum_{i_1=1-\nu}^{\nu} \sum_{i_2=1-\nu}^{\nu} \cdots \sum_{i_N=1-\nu}^{\nu} \widetilde{f}\left(\frac{i_1 L}{2\nu}, \frac{i_2 L}{2\nu}, ..., \frac{i_N L}{2\nu}\right)\left(\frac{L}{\nu}\right)^N,$$

ja:

$$J_\nu = \sum_{i_1=1-\nu}^{\nu} \sum_{i_2=1-\nu}^{\nu} \cdots \sum_{i_N=1-\nu}^{\nu} \chi_B\left(\frac{i_1 L}{2\nu}, \frac{i_2 L}{2\nu}, ..., \frac{i_N L}{2\nu}\right)\left(\frac{L}{\nu}\right)^N.$$

I_ν ja J_ν ovat tietenkin Riemann-summia ja

$$\lim_{\nu\to\infty} I_\nu = \iint_B \cdots \int f(x_1, x_2, ..., x_N)\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_N,$$

sekä

$$\lim_{\nu\to\infty} J_\nu = \iint_B \cdots \int \mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_N.$$

Lisäksi luvun J_ν määrittelevän summan kaikki termit ovat ei-negatiivisia ja ainakin yksi niistä on positiivinen, sillä ainakin yksi pisteistä $\langle \frac{i_1 L}{2\nu}, ..., \frac{i_N L}{2\nu}\rangle$ kuuluu joukkoon $\overline{B^N}\left(x_0, \frac{\sqrt{N}}{N_0}\right)$. Täten luvut J_ν ovat kaikki positiivisia. Määritellään kaikille $\nu = N_0, N_0+1, ...$

$$\begin{aligned} g_\nu = \frac{I_\nu}{J_\nu} &= \frac{1}{J_\nu}\sum_{i_1=1-\nu}^{\nu}\sum_{i_2=1-\nu}^{\nu}\cdots\sum_{i_N=1-\nu}^{\nu}\widetilde{f}\left(\frac{i_1 L}{2\nu}, \frac{i_2 L}{2\nu}, ..., \frac{i_N L}{2\nu}\right)\left(\frac{L}{\nu}\right)^N \\ &= \sum_{i_1=1-\nu}^{\nu}\sum_{i_2=1-\nu}^{\nu}\cdots\sum_{i_N=1-\nu}^{\nu}\frac{\chi_B\left(\frac{i_1 L}{2\nu}, ..., \frac{i_N L}{2\nu}\right)\cdot\left(\frac{L}{\nu}\right)^N}{J_\nu}\widetilde{f}\left(\frac{i_1 L}{2\nu}, \frac{i_2 L}{2\nu}, ..., \frac{i_N L}{2\nu}\right). \end{aligned}$$

Lemman 3.1 nojalla $g_\nu \in h(\mathrm{Im}\, f)$ jokaisella $\nu \in \{1, 2, ...\}$ ja selvästi $\lim_{\nu\to\infty} g_\nu = g$. Lopuksi, koska $\mathrm{Im}\, f$ on kompakti, on $h(\mathrm{Im}\, f)$ lemman 3.4 nojalla kompakti, joten $g = \lim_{\nu\to\infty} g_\nu \in h(\mathrm{Im}\, f)$. Q.E.D.

Lemma 4.2 (Avainlemma)**.** *Olkoon $k \in \mathbb{Z}_+$ mielivaltainen ja merkitään $N = \binom{2k+4}{4}$. Tällöin löytyvät $\lambda_1, \lambda_2, ..., \lambda_N \in \mathbb{Q}_+$ sekä*

$$\alpha_{1,1}, \alpha_{2,1}, ... \alpha_{N,1}, \alpha_{1,2}, \alpha_{2,2}, ..., \alpha_{N,2}, ..., \alpha_{1,5}, \alpha_{2,5}, ..., \alpha_{N,5} \in \mathbb{Z}$$

siten, että reaalilukumuuttujille $x_1, x_2, ..., x_5$ pätee identiteetti

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2)^k = \sum_{\ell=0}^{N}\lambda_\ell(\alpha_{\ell,1}x_1 + \alpha_{\ell,2}x_2 + \alpha_{\ell,3}x_3 + \alpha_{\ell,4}x_4 + \alpha_{\ell,5}x_5)^{2k}.$$

Todistus. Olkoot $x_1, x_2, ..., x_5$ siis symbolisia muuttujia. Tällöin näiden viiden muuttujan homogeeniset $2k$-asteiset $\mathbb{R}$-kertoimiset muodot muodostavat N-ulotteisen $\mathbb{R}$-vektoriavaruuden, kuten helposti nähdään. Merkitään tätä avaruutta symbolilla V.

Tarkastellaan nyt avaruuden V osajoukkoa

$$S = \left\{(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 + \alpha_5 x_5)^{2k}\middle|\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in \mathbb{Q}\right\}.$$

Tietenkin $S \subseteq V$, koska multinomikaavan nojalla

$$(\alpha_1 x_1 + ... + \alpha_5 x_5)^{2k} = \sum_{n,m,p,q,r} \frac{(2k)!}{n!m!p!q!r!} \cdot \alpha_1^n \cdots \alpha_5^r x_1^n \cdots x_5^r \in V,$$

missä summataan niiden ei-negatiivisten kokonaislukujen 5-tuplien $\langle n, ..., r \rangle$ yli, joille $n + m + p + q + r = 2k$.

Jos nyt $h(S)$ sisältää elementin, joka on muotoa $r(x_1^2 + ... + x_5^2)^k$, missä $r \in \mathbb{Q}_+$, niin avainlemman väite seuraa suoraan Carathéodoryn lauseesta.

Siirrytään nyt tarkastelemaan avaruuden V osajoukkoa T, joka käsittää ne muodot $(\alpha_1 x_1 + ... + \alpha_5 x_5)^{2k}$, joissa $\alpha_1, ..., \alpha_5 \in \mathbb{R}$, sekä $\sqrt{\alpha_1^2 + ... + \alpha_5^2} \leqslant 1$. Olkoon $\overline{B^5}(1)$ tällaisten reaalilukuviisikoiden joukko, eli avaruuden $\mathbb{R}^5$ origokeskinen 1-säteinen suljettu kuula. Määritellään

$$g = \frac{\iiiii_{\overline{B^5}(1)} (\alpha_1 x_1 + ... + \alpha_5 x_5)^{2k} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_3 \mathrm{d}\alpha_4 \mathrm{d}\alpha_5}{\iiiii_{\overline{B^5}(1)} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_3 \mathrm{d}\alpha_4 \mathrm{d}\alpha_5}.$$

Merkitään selvyyden vuoksi $I_1 = \iiiii_{\overline{B^5}(1)} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \cdots \mathrm{d}\alpha_5$. Kun jokin $\langle \xi_1, ..., \xi_5 \rangle \in \mathbb{R}^5 \backslash \{\langle 0, ..., 0 \rangle\}$ on annettu, voidaan integraalissa $g(\xi_1, ..., \xi_5)$ tehdä muuttujanvaihto: $t_i = \sum_{j=1}^5 \beta_{ij} \alpha_j$, $(i \in \{1, ..., 5\})$, missä $\beta_{1,i} = \frac{\xi_i}{\sqrt{\xi_1^2 + ... + \xi_5^2}}$, ja loput β_{ij} valitaan siten, että $[\beta_{ij}]$ on ortogonaalimatriisi.

Tällöin

$$\begin{aligned} g(\xi_1, ..., \xi_5) &= \frac{1}{I_1} \iiiii_{\overline{B^5}(1)} (\alpha_1 \xi_1 + ... + \alpha_5 \xi_5)^{2k} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_5 \\ &= \frac{1}{I_1} (\xi_1^2 + ... + \xi_5^2)^k \iiiii_{\overline{B^5}(1)} \left(\frac{\alpha_1 \xi_1 + ... + \alpha_5 \xi_5}{\sqrt{\xi_1^2 + ... + \xi_5^2}} \right)^{2k} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_5 \\ &= \frac{1}{I_1} (\xi_1^2 + ... + \xi_5^2)^k \iiiii_{\overline{B^5}(1)} t_1^{2k} \mathrm{d}t_1 \cdots \mathrm{d}t_5. \end{aligned}$$

Kun merkitään $I_2 = \iiiii_{\overline{B^5}(1)} t_1^{2k} \mathrm{d}t_1 \cdots \mathrm{d}t_5$, niin voidaan näiden laskujen tulokset kirjoittaa muotoon

$$g = \frac{I_2}{I_1} (x_1^2 + ... + x_5^2)^k,$$

missä varmasti $\frac{I_2}{I_1} \in \mathbb{R}_+$. Lemman 4.1 nojalla $g \in h(T)$, ja koska $0 \in T \subseteq h(T)$, niin joukon $h(T)$ konveksisuuden nojalla $\frac{cI_2}{I_1} g \in h(T)$, missä $c \in]0, \frac{I_2}{I_1}[\cap \mathbb{Q}$ on mielivaltainen.

Merkitään selvyyden vuoksi $A = L(h(T))$. Haluamme osoittaa, että $g \in \operatorname{int}_A h(T)$. Oletetaan, että $g \in \partial_A h(T)$. Tällöin lauseen 3.10 nojalla löytyy avaruuden A hypertaso τ siten, että $g \in \tau$ ja $\tau \cap \operatorname{int}_A h(T) = \emptyset$. Tietenkin nyt löytyvät $a \in V$ ja $b \in \mathbb{R}$ joille $\tau = \{x \in A | a \cdot x = b\}$ ja $a \neq 0$. Edelleen voidaan ilman yleisyyden menettämistä olettaa, että jokaisella $x \in h(T)$ on $a \cdot x \geqslant b$. Nimittäin lauseen 3.9 nojalla löytyy $y \in \operatorname{int}_A h(T)$ ja ilman yleisyyden menettämistä voidaan olettaa, että $a \cdot y > b$. Jos nyt löytyisi piste $x \in h(T)$ siten, että $a \cdot x < b$, niin lauseen 3.6 nojalla olisi

$$z \stackrel{\text{def}}{=} \frac{b - a \cdot x}{a \cdot y - a \cdot x} y + \frac{a \cdot y - b}{a \cdot y - a \cdot x} x \in \operatorname{int}_A h(T),$$

ja

$$a \cdot z = b \left(\frac{a \cdot y}{a \cdot y - a \cdot x} - \frac{a \cdot x}{a \cdot y - a \cdot x} \right) - \frac{(a \cdot x)(a \cdot y)}{a \cdot y - a \cdot x} + \frac{(a \cdot y)(a \cdot x)}{a \cdot y - a \cdot x} = b,$$

eli olisi $z \in \tau \cap \operatorname{int}_A h(t)$, mikä on mahdotonta. Siis voidaan olettaa, että $a \cdot x \geqslant b$ kaikilla $x \in h(T)$.

Mutta tällöinhän skalaaritulon $g \cdot a$ määrittelevässä integraalissa

$$g \cdot a = \frac{\iiiint\!\!\int_{\overline{B^5}(1)} (\alpha_1 x_1 + ... + \alpha_5 x_5)^{2k} \cdot a \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_3 \mathrm{d}\alpha_4 \mathrm{d}\alpha_5}{\iiiint\!\!\int_{\overline{B^5}(1)} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_3 \mathrm{d}\alpha_4 \mathrm{d}\alpha_5},$$

on integrandi aina $\geqslant b$, eli $g \cdot a \geqslant b$. Koska $g \in \tau$, on kyseisen integrandin jatkuvuuden nojalla oltava identtisesti b, jolloinka siis $h(T)$ pisteen g määrittelevän integraalin integrandin kuvana sisältyisi hypertasoon τ, mikä olisi ristiriita. Täten $g \in \operatorname{int}_A h(T)$.

Olkoon $c \in]0, \min\{1, \frac{I_2}{I_1}\}[\cap \mathbb{Q} \subseteq]0, 1[$. Koska $0 \in h(T)$, on lauseen 3.6 nojalla oltava $cg \in \operatorname{int}_A h(T)$. Nyt $cg \in \operatorname{int}_A h(T) \subseteq \operatorname{int}_A \overline{h(S)} = \operatorname{int}_A \operatorname{cl}_A h(S)$, ja lauseen 3.8 nojalla myös $cg \in \operatorname{int}_A h(S)$. Lopuksi, koska $cg \in \operatorname{int}_A h(S) \subseteq h(S)$, on todistuksen alkupuolella tehdyn havainnon nojalla avainlemma todistettu. Q.E.D.

Luku 5

Loppuhuipennus

Aloitetaan muutamalla avainlemman korollaarilla.

Korollaari 5.1. *Olkoon $k \in \mathbb{Z}_+$. Tällöin löytyvät $N \in \mathbb{Z}_+$ sekä*

$$\lambda_1, \lambda_2, ..., \lambda_N, \alpha_1, \alpha_2, ..., \alpha_N \in \mathbb{Q}_+,$$

siten, että kaikilla $y \in \mathbb{Z}_+$ löytyvät $\beta_1, \beta_2, ..., \beta_N \in \mathbb{Z}_+$, joille

$$(x_1^2 + y)^k = \sum_{\ell=0}^{N} \lambda_\ell (\alpha_\ell x_1 + \beta_\ell)^{2k}.$$

Todistus. Lagrangen lauseen nojalla voidaan valita $x_2, x_3, x_4, x_5 \in \mathbb{Z}$ s.e. $y = x_2^2 + x_3^2 + x_4^2 + x_5^2$. Haluttu tulos saadaan nyt merkitsemällä avainlemman tuloksessa $\alpha_\ell = \alpha_{\ell,1} \in \mathbb{Z}$ ja $\beta_\ell = \alpha_{\ell,2} x_2 + ... + \alpha_{\ell,5} x_5 \in \mathbb{Z}$.

Korollaari 5.2. *Jos lauseen 1.2 väite pitää paikkaansa jollakin eksponentilla $k = m \in \mathbb{Z}_+$, niin se pitää paikkaansa myös eksponentilla $k = 2m$.*

Todistus. Nimittäin, jos jokaisella kokonaisluvulla $n \geqslant A \in \mathbb{Z}_+$, missä A on jokin vakio, on välttämättä esitys $n = \sum_{\ell=1}^{M} \lambda_\ell y_\ell^k$ (missä $\lambda_1, ..., \lambda_M \in \mathbb{Q}_+$, $y_1, ..., y_M \in \mathbb{Z}_+ \cup \{0\}$, ja $M \in \mathbb{Z}_+$), niin korollaarista 5.1 seuraa valitsemalla $x_1 = 0$, että jokainen y_ℓ^k on esitettävissä muodossa $y_\ell^k = \sum_{j=0}^{N} \mu_{\ell,j} \beta_{\ell,j}^{2k}$, jolloinka siis luvulle n löytyy esitys

$$n = \sum_{\ell=1}^{M} \lambda_\ell y_\ell^k = \sum_{\ell=1}^{M} \sum_{j=0}^{N} \lambda_\ell \mu_{\ell,j} \beta_{\ell,j}^{2k},$$

missä varmasti $\beta_{\ell,j} \in \mathbb{Z}$ ja $\lambda_\ell, \mu_{\ell,j} \in \mathbb{Q}_+$.

Artikkelia [El] seuraten otamme käyttöön seuraavan kätevän lyhennysmerkinnän. Olkoot $m \in \mathbb{Z}_+$ mielivaltainen. Jos $a = a(\omega_1, \omega_2, ..., \omega_N)$ ($N \in \mathbb{Z}_+$) on jokin vain ei-negatiivisia kokonaislukuarvoja saava funktio, jolle löytyy jokin $M \in \mathbb{Z}_+$ ja jotkin vakiokertoimet $\lambda_1, \lambda_2, ..., \lambda_M \in \mathbb{Q}_+$ siten, että jokaiselle funktion a saamalle arvolle $a(\omega_1, \omega_2, ..., \omega_N)$ löytyvät ei-negatiiviset kokonaisluvut $n_1, n_2, ..., n_M$ siten, että

$$a(\omega_1, \omega_2, ..., \omega_N) = \sum_{\ell=1}^{M} \lambda_\ell n_\ell^m,$$

niin merkitsemme $a = \sum(m)$.

Esimerkiksi triviaalisti aina $a = \sum(1)$, ja Lagrangen neljän neliön lauseen nojalla myös $a = \sum(2)$. Jos $a = \sum(2m)$, niin selvästi myös $a = \sum(m)$. Jos a ja b ovat samassa joukossa määriteltyjä vain ei-negatiivisia kokonaislukuarvoja saavia funktioita, niin relaatioista $a = \sum(m)$ ja $b = \sum(m)$ seuraa, että $a + b = \sum(m)$. Korollaarin 5.2 todistuksessa käytetyllä idealla nähdään, että ehdosta $a = \sum(m)$ seuraa myös $a = \sum(2m)$.

Viimeisenä esimerkkinä mainittakoon, että lauseen 1.2 väite voitaisiin lyhyesti ilmaista muodossa: jokaiselle $m \in \mathbb{Z}_+$ löytyy sellainen $A \in \mathbb{Z}_+$, että $\mathrm{id}_{\{A, A+1, A+2, ...\}} = \sum(m)$, missä id tarkoittaa tavanmukaista identiteettifunktiota. Käytännössä emme kuitenkaan eksplisiittisesti tule puhumaan funktioista vaan lausuisimme lauseen 1.2 väitteen vieläkin lyhyemmin muodossa: jos $m \in \mathbb{Z}_+$, niin $n = \sum(m)$ kaikilla tarpeeksi suurilla $n \in \mathbb{Z}_+$.

Korollaari 5.3. *Olkoon r ja m positiivisia kokonaislukuja, joille $r < m$. Tällöin löytyvät kiinteät kertoimet $B_{0,r}, B_{1,r}, ..., B_{r,r} \in \mathbb{Z}_+$ siten, että kaikille positiivisille kokonaisluvuille x ja T, joille $x^2 < T$, pätee*

$$\sum_{\nu=0}^{r} B_{\nu,r} x^{2\nu} T^{m-\nu} = \sum(m).$$

Todistus. Sijoitetaan korollaarin 5.1 antamaan yhtälöön $k = m+r$, joilloin se saa muodon

$$(x_1^2 + y)^{m+r} = \sum_{\ell=0}^{N} \lambda_\ell (\alpha_\ell x_1 + \beta_\ell)^{2m+2r}.$$

Derivoimalla tätä yhtälöä $2r$ kertaa puolittain muuttujan x_1 suhteen saadaan yhtälön vasemmalle puolelle $2m$-asteinen polynomi jonka jokainen termi on parillisasteinen. On siis helppo nähdä, että

$$\frac{\mathrm{d}^{2r}}{\mathrm{d}x_1^{2r}}(x_1^2 + y)^{m+r} = \sum_{\nu=0}^{r} B_{\nu,r} x_1^{2\nu} (x_1^2 + y)^{m-\nu},$$

joillakin $B_{\nu,r} \in \mathbb{Z}_+$ $(\nu = 0, 1, 2, ..., r)$. Toisaalta yhtälön oikea puoli saa muodon

$$\sum_{\ell=0}^{N} \lambda_\ell \cdot \frac{(2m+2r)!}{(2m)!} \cdot \alpha_\ell^{2r}(\alpha_\ell x_1 + \beta_\ell)^{2m} = \sum(2m),$$

ja väite seuraa sijoittamalla $x_1 = x$ ja $y = T - x^2$.

Lauseen 1.2 todistus. Todistamme lauseen 1.2 induktiolla eksponentin k suhteen. Tapaus $k = 1$ on tietenkin triviaali, ja tapaus $k = 2$ seuraa suoraan Lagrangen neljän neliön lauseesta. Oletetaan nyt, että olemme todistaneet lauseen 1.2 eksponentin k arvoille $1, 2, ..., m-1$, jollakin $m \in \mathbb{Z}_+$. Tavoitteemme on nyt todistaa tapaus $k = m$. Korollaarin 5.2 nojalla lause 1.2 pätee nyt myös parillisilla eksponenteilla $2, 4, ..., 2m-2$, ja ensimmäisen luvun lopussa tehdyn havainnon nojalla myös itse Waring-Hilbertin lause pätee näille eksponenteille.

Jatkossa T merkitsee aina tarpeeksi suurta positiivista kokonaislukua. Olkoot nyt $N_1, N_2, ..., N_{m-1}$ lukua T pienempiä positiivisia kokonaislukuja, jotka valitaan myöhemmin kun aika on kypsä. Induktio-oletuksen nojalla löytyvät ei-negatiiviset kokonaisluvut r ja $x_{i,j}$, $i \in \{1, ..., r\}$,$j \in \{1, ..., m-1\}$, joille $N_j = \sum_{i=1}^{r} x_{i,j}^{2j}$ kun $j = 1, 2, ..., m-1$. Tässä voidaan luvun 1 merkinnöin valita esimerkiksi $r = \max\{s(2), s(4), ..., s(2m-2)\}$.

Kiinnitetään nyt $j \in \{1, 2, ..., m-1\}$. Sijoittamalla korollaarin 5.3 antamaan kaavaan muuttujan x paikalle yksi kerrallaan luvut $x_{1,j}, x_{2,j}, ..., x_{r,j}$ saadaan

$$\sum_{\nu=0}^{j} B_{\nu,j} x_{i,j}^{2\nu} T^{m-\nu} = \sum(m), \text{kun } i \in \{1, 2, ..., r\}.$$

Laskemalla nämä yhteen indeksin i suhteen saadaan

$$\sum_{i=1}^{r} \sum_{\nu=0}^{j} B_{\nu,j} x_{i,j}^{2\nu} T^{m-\nu} = \sum(m),$$

eli

$$rB_{0,j}T^m + \sum_{\nu=1}^{j-1} B_{\nu,j} \sum_{i=1}^{r} x_{i,j}^{2\nu} T^{m-\nu} + B_{j,j}N_j T^{m-j} = \sum(m).$$

Merkitään $c_{\nu,j} = B_{\nu,j} \sum_{i=1}^{r} x_{i,j}^{2\nu}$, kun $\nu = 0, 1, 2, ..., j-1$, jolloin tämä kaava sievenee muotoon

$$\sum_{\nu=0}^{j-1} c_{\nu,j} T^{m-\nu} + B_{j,j} N_j T^{m-j} = \sum(m). \tag{A}$$

Tässä vaiheessa siirrymme lopullisesti seuraamaan kirjan [K&P] luvun 5 esitystä, joka voittaa artikkelin [El] sekä rakenteessa että tarkkuudessa.

Havainto 1. Olkoon $a \in \mathbb{Z}_+$ ja $a > 1$. Tällöin kaikilla kokonaisluvuilla T, joilla

$$T \geqslant (r+1)\frac{a^{2j}}{a-1},$$

pätee myös

$$a\left(1+\sum_{i=1}^{r} x_{i,j}^{2(j-1)}\right) < T.$$

Todistus. Riippumatta siitä, ovatko jotkin yksittäiset luvut $x_{i,j}$ lukua a suurempia vai pienempiä, voidaan arvioida seuraavasti:

$$\begin{aligned} a\left(1+\sum_{i=1}^{r} x_{i,j}^{2(j-1)}\right) &= a + a\sum_{i=1}^{r} x_{i,j}^{2(j-1)} \leqslant a^{2j-1} + a\sum_{i=1}^{r}\left(a^{2(j-1)} + \frac{1}{a^2}x_{i,j}^{2j}\right) \\ &= (1+r)a^{2j-1} + \frac{1}{a}\sum_{i=1}^{r} x_{i,j}^{2j} < \frac{a-1}{a}\cdot\frac{(1+r)a^{2j}}{a-1} + \frac{1}{a}T \\ &\leqslant \frac{a-1}{a}T + \frac{1}{a}T = T. \qquad \text{q.e.d.} \end{aligned}$$

Koska $\sum_{i=1}^{r} x_{i,j}^{2j} = N_j < T$, on tämän havainnon 1 nojalla kaikilla tarpeeksi isoilla kokonaisluvuilla T ja jokaisella $\nu \in \{0, 1, ..., j-1\}$

$$c_{\nu,j} = B_{\nu,j}\sum_{i=1}^{r} x_{i,j}^{2\nu} \leqslant B_{\nu,j}\sum_{i=1}^{r} x_{i,j}^{2(j-1)} < T.$$

Nyt yhtälön (A) voi kirjoittaa muodossa

$$\sum_{\nu=0}^{j-2} c_{\nu,j}T^{m-\nu} + (c_{j-1,j} + B_{j,j})T^{m-j+1} - B_{j,j}(T-N_j)T^{m-j}, \qquad \text{(B)}$$

missä tietenkin aina $0 < T - N_j < T$ ja havainnon 1 nojalla tarpeeksi suurilla T ja jokaisella $\nu \in \{0, 1, ..., j-1\}$ myös

$$c_{\nu,j} + B_{j,j} = B_{\nu,j}\sum_{i=1}^{r} x_{i,j}^{2\nu} + B_{j,j} \leqslant \left(\max\{B_{\nu,j}, B_{j,j}\}\right)\left(1+\sum_{i=1}^{r} x_{i,j}^{2\nu}\right) < T.$$

Havainto 2. Olkoon $q \in \{0, 1, ..., m-1\}$. Tällöin löytyy sellainen $A_q \in \mathbb{Z}_+$, että tarpeeksi suurilla $T \in \mathbb{Z}_+$ ja mielivaltaisilla $b_1, b_2, ..., b_q \in \mathbb{Z} \cap [-T, T[$ on

$$A_qT^m + b_1T^{m-1} + ... + b_qT^{m-q} = \sum(m).$$

Todistus. Käytämme (äärellistä) induktiota muuttujan q suhteen. Tapauksessa $q = 0$ väitteen kaava saa muodon $A_0T^m = \sum(m)$, eikä mitään todistettavaa ole. Oletetaan nyt, että olemme todistaneet väitteen kaikilla jotakin lukua $j \in \{1, 2, ..., m-1\}$ pienemmillä muuttujan q arvoilla, ja oletetaan, että jotkin $b_1, ..., b_j \in \mathbb{Z} \cap [-T, T[$ ovat annetut.

Riippumatta siitä, onko b_j positiivinen vai negatiivinen, saadaan (tarpeeksi suurilla T) joko kaavasta (A) tai kaavasta (B) luvut $a_0, a_1, ..., a_{j-1} \in \{0, 1, ..., T-1\}$, joille

$$\sum_{\nu=0}^{j-1} a_\nu T^{m-\nu} + B_{j,j} b_j T^{m-j} = \sum(m). \tag{1}$$

Koska varmasti $a_0T^m = \sum(m)$, on suoraan induktio-oletuksen nojalla

$$(A_{j-1} + a_0)T^m + \sum_{\nu=1}^{j-1}(-a_\nu)T^{m-\nu} = \sum(m).$$

Jos λ on sellainen positiivinen kokonaisluku, että $\lambda B_{j,j} \geqslant A_{j-1} + a_0$, niin

$$\lambda B_{j,j} T^m - \sum_{\nu=1}^{j-1} a_\nu T^{m-\nu} = \sum(m). \tag{2}$$

Laskemalla yhteen kaavat (1) ja (2) saadaan

$$B_{j,j}\left(\lambda T^m + b_j T^{m-j}\right) = \sum(m),$$

josta tietenkin saadaan jakamalla puolittain luvulla $B_{j,j} > 0$, että

$$\lambda T^m + b_j T^{m-j} = \sum(m).$$

Tämän kaavan ja induktio-oletuksen nojalla on nyt

$$(A_{j-1} + \lambda)T^m + \sum_{\nu=1}^{j} b_\nu T^{m-\nu} = \sum(m).$$

Täten väite pätee myös tapauksessa $q = j$. q.e.d.

Esittämällä mielivaltainen luku $c \in \mathbb{Z} \cap]-T^{m-1}, T^{m-1}[$ T-kantaisena saamme havainnosta 2 korollaarina tuloksen:

Havainto 3. On olemassa (eksponentista m riippuvat) $A, T_0 \in \mathbb{Z}_+$, jolle jokaisella $T \in \mathbb{Z}_+, T > T_0$ ja jokaisella $c \in \mathbb{Z} \cap]-T^{m-1}, T^{m-1}[$ on

$$AT^m \pm cT = \sum(m).$$

Merkitään seuraavaksi

$$\widetilde{T}_0 \stackrel{\text{def}}{=} \max\left\{T_0, \frac{2}{\sqrt[m]{1+\frac{1}{A}}-1}\right\},$$

missä A ja T_0 ovat havainnon 3 antamat kokonaislukuvakiot, ja olkoon nyt $n \geqslant A\left((\widetilde{T}_0+1)^m + \widetilde{T}_0^m\right)$ mielivaltainen kokonaisluku. Olkoon edelleen T se suurin kokonaisluku, jolle

$$n \geqslant A\big((T+1)^m + T^m\big).$$

Tällöin tietenkin $n < A\big((T+2)^m + (T+1)^m\big)$ ja $T \geqslant \widetilde{T}_0$. Määritellään

$$\widetilde{n} = n - A\big((T+1)^m + T^m\big).$$

Voidaan arvioida:

$$\begin{aligned}
0 \leqslant \widetilde{n} &= n - A\big((T+1)^m + T^m\big) \\
&< A\big((T+2)^m + (T+1)^m\big) - A\big((T+1)^m + T^m\big) \\
&= A\big((T+2)^m - T^m\big) = T^m A\left(\frac{(T+2)^m}{T^m} - 1\right) \\
&= T^m A\left(\left(1+\frac{2}{T}\right)^m - 1\right) \leqslant T^m A\left(\left(1+\frac{2}{\widetilde{T}_0}\right)^m - 1\right) \\
&\leqslant T^m A\left(\left(1+2\left(\frac{2}{\sqrt[m]{1+\frac{1}{A}}-1}\right)^{-1}\right)^m - 1\right) = T^m.
\end{aligned}$$

Valitaan nyt $\eta \in \{0,1,...,T\}$ siten, että $\eta \equiv \widetilde{n} \pmod{T+1}$. Tällöin tietenkin $\eta T + \widetilde{n} \equiv \widetilde{n}(T+1) \equiv 0 \pmod{T+1}$, eli voidaan valita $\vartheta = \frac{\eta T+\widetilde{n}}{T+1} \in \mathbb{Z}$, jolloin

$$-T^{m-1} < 0 \leqslant \eta \leqslant T < T^{m-1},$$

ja

$$-(T+1)^{m-1} < 0 \leqslant \vartheta = \frac{\eta T + \widetilde{n}}{T+1} < \frac{T^2+T^m}{T+1} < \frac{(T+1)^m}{T+1} = (T+1)^{m-1},$$

sekä erityisesti

$$\widetilde{n} = \vartheta(T+1) - \eta T.$$

Havainnon 3 nojalla

$$AT^m - \eta T = \sum(m),$$

ja

$$A(T+1)^m + \vartheta(T+1) = \sum(m).$$

Laskemalla nämä yhteen saadaan, että

$$\begin{aligned} n &= A\big((T+1)^m + T^m\big) + \widetilde{n} \\ &= A(T+1)^m + \vartheta(T+1) + AT^m - \eta T = \sum(m). \end{aligned}$$

Eli $n = \sum(m)$, kun $n \geqslant A\big((\widetilde{T}_0+1)^m + \widetilde{T}_0^m\big)$, ja lause 1.2 pätee myös eksponentilla $k = m$. Q.E.D.

Lähteet

[Eg] Eggleston, H. G.: *Convexity*, Cambridge Tracts in Mathematics and Mathematical Physics, **47**, Cambridge University Press, Cambdrige, 1958.

[El] Ellison, W. J.: *Waring's problem*, Amer. Math. Monthly, **78** (1971), 10–36.

[G&H] Giaquinta, M., ja S. Hildebrandt: *Calculus of Variations II*, Grundlehren der mathematischen Wissenschaften, **311**, Springer-Verlag, Berlin, 1996.

[H&W] Hardy, G. H., ja E. M. Wright: *An Introduction to the Theory of Numbers*, 5th edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

[K&P] Koch, H., ja H. Pieper: *Zahlentheorie: Ausgewählte Methoden und Ergebnisse*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1976.