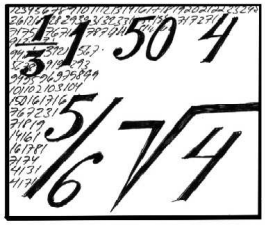

Algebran peruslause lukiolaisille

Tuomas Hytönen
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

Johdanto

Algebran peruslauseena tunnetaan seuraava tulos:

Lause 1. *Olkoon $p(z) = a_0 + a_1 z + \ldots + a_n z^n$ polynomi, jonka kertoimet ovat kompleksilukuja $a_i \in \mathbb{C}$, ja jonka aste on $n \geq 1$, siis $a_n \neq 0$. Tällöin polynomilla p on ainakin yksi kompleksinen nollakohta, eli on olemassa sellainen $z_0 \in \mathbb{C}$, että $p(z_0) = 0$.*

Nimi luo liiankin mahtipontisen kuvan lauseen asemasta algebrassa alan koko nykyisessä laajuudessa, mutta joka tapauksessa tämä on kiistatta keskeinen polynomeja koskeva tulos. Algebran peruslauseen todistuksesta annetaan usein[1] kunnia C. F. Gaussille (1799), mutta ilmeisesti[2] sille julkaisi ensimmäisen nykykriteerein täydellisen todistuksen vasta J.-R. Argand vuonna 1806, kun taas Gaussin ja useiden muiden matemaatikoiden varhaisemmat todistusyritykset vielä sisälsivät aukkoja. Oma tarmoni ei ole riittänyt näiden väitteiden tarkistamiseen alkuperäislähteistä.

Nyky-Suomessa algebran peruslause kuuluu yliopistomatematiikan perusopintoihin, ja usein se esitetään seurauksena yleisemmistä kompleksimuuttujan funktioiden teorian tuloksista. Kuitenkin tämä keskeinen lause on mahdollista todistaa selvästi kevyemmälläkin koneistolla, jonka pitäisi avautua jo lukiopohjalta, kompleksilukujen perustiedoilla täydennettynä. Esitän tässä algebran peruslauseelle tällaisen helpohkon todistuksen, jossa kompleksilukujen alkeiden (peruslaskutoimitukset, itseisarvo ja napakoordinaattiesitys) ja rajaarvojen käsittelyn lisäksi tarvitaan ainoastaan seuraava yksittäinen differentiaali- ja integraalilaskennan tulos:

Lause 2. *Olkoon $D = \{z \in \mathbb{C} : |z| \leq R\}$ kompleksitason suljettu kiekko ja $f : D \to \mathbb{R}$ jatkuva reaaliarvoinen funktio. Tällöin funktiolla f on kiekolla D minimikohta, eli on olemassa sellainen $z_0 \in D$, että $f(z_0) \leq f(z)$ kaikilla $z \in D$.*

Lukion differentiaali- ja integraalilaskennassa käsitellään ilman todistusta tämän lauseen yksiulotteinen vastine, jossa suljetun kiekon paikalla on reaaliakselin suljettu väli $[a, b]$. Samoin tässä esityksessä lause 2 otetaan käyttöön ilman todistusta.

Todistus

Esitettävä todistus jakautuu kahteen pääkohtaan:

1. Osoitetaan, että polynomin itseisarvo $|p(z)|$ saavuttaa jossakin pisteessä miniminsä koko kompleksitasossa, ts. on olemassa sellainen $z_0 \in \mathbb{C}$, että $|p(z_0)| \leq |p(z)|$ kaikilla $z \in \mathbb{C}$.

[1] Esim. suomenkielisessä Wikipediassa, ladattu 1.6.2011.

[2] Mm. englannin- ja saksankielisen Wikipedian perusteella, ladattu 1.6.2011.

2. Osoitetaan, että tällaisessa minimikohdassa polynomin arvo on välttämättä $p(z_0) = 0$.

Kumpikin kohta käyttää hyväkseen polynomien erityisominaisuuksia yleisempiin funktioihin nähden: esimerkiksi jatkuvalla funktiolla $z \mapsto (1+|z|)^{-1}$ ei ole lainkaan minimiä kompleksilukujen joukossa (se tulee mielivaltaisen lähelle nollaa, mutta ei saavuta tätä arvoa), kun taas myös jatkuva funktio $z \mapsto 1 + |z|$ kylläkin saavuttaa miniminsä pisteessä $z_0 = 0$, mutta funktion arvo tässä pisteessä on 1 eikä 0. Jatkossa polynomia p koskevat oletukset ovat aina samat kuin lauseessa 1 ilman eri mainintaa.

Minimi on olemassa

Lemma 1. *Kun $|z| \to \infty$, myös $|p(z)| \to \infty$.*

Todistus. Kirjoitetaan polynomin itseisarvo muotoon

$$|p(z)| = \Big|\sum_{k=0}^{n} a_k z^k\Big| = \Big|a_n z^n + \sum_{k=0}^{n-1} a_k z^k\Big|$$
$$= |a_n| \cdot |z|^n \cdot \Big|1 + \sum_{k=0}^{n-1} \frac{a_k}{a_n} z^{k-n}\Big|.$$

Kun $|z| \to \infty$, myös $|z|^n \to \infty$, ja toisaalta $z^{k-n} \to 0$ kaikilla $k \in \{0, 1, \ldots, n-1\}$. Tästä seuraa, että viimeinen tulontekijä oikealla lähestyy ykköstä, kun $|z| \to \infty$. Siis

$$\lim_{|z|\to\infty} |p(z)|$$
$$= |a_n| \cdot \lim_{|z|\to\infty} |z|^n \cdot \lim_{|z|\to\infty} \Big|1 + \sum_{k=0}^{n-1} \frac{a_k}{a_n} z^{k-n}\Big|$$
$$= |a_n| \cdot \infty \cdot 1 = \infty. \qquad \square$$

Lemma 2. *Polynomin itseisarvo $|p(z)|$ saavuttaa miniminsä kompleksitasossa.*

Todistus. Koska $|p(z)| \to \infty$ kun $|z| \to \infty$, pätee erityisesti, että on olemassa sellainen luku R, että $|p(z)| > |p(0)|$ aina kun $|z| > R$ (raja-arvon määritelmä!). Tarkastellaan sitten suljettua kiekkoa $D = \{z \in \mathbb{C} : |z| \leq R\}$. Koska $z \mapsto |p(z)|$ on jatkuva reaaliarvoinen funktio, se saavuttaa tässä suljetussa kiekossa miniminsä jossakin pisteessä z_0. Nyt siis $|p(z_0)| \leq |p(z)|$, kun $|z| \leq R$, ja erityisesti $|p(z_0)| \leq |p(0)|$. Toisaalta luvun R valinnan perusteella pätee $|p(z_0)| \leq |p(0)| < |p(z)|$, kun $|z| > R$. Edelliset havainnot yhdistämällä nähdään, että $|p(z_0)| \leq |p(z)|$ kaikilla $z \in \mathbb{C}$. $\square$

Minimi on nolla

Lemma 3. *Olkoon z_0 funktion $z \mapsto |p(z)|$ minimikohta kompleksitasossa. Tällöin $p(z_0) = 0$.*

Todistus. Määritellään uusi apupolynomi

$$q(z) = p(z + z_0).$$

Tällöin 0 on funktion $z \mapsto |q(z)|$ minimikohta, ja lemman väite on yhtäpitävä sille, että $q(0) = 0$. Kirjoitetaan nyt $q(z)$ auki seuraavasti:

$$q(z) = b_0 + \sum_{j=r}^{n} b_k z^k,$$

missä $r \in \{1, \ldots, n\}$ ja $b_r \neq 0$. Tässä esityksessä on otettu huomioon se, että osa polynomin alkupään kertoimista, $b_1, \ldots, b_{r-1}$ voi olla nollia, ja ne on jätetty kirjoittamatta. Toisaalta havaitaan (harjoitustehtävä!), että polynomien p ja q johtokertoimet ovat samat, eli $b_n = a_n \neq 0$. Siis ainakin yksi kertoimista $b_1, \ldots, b_n$ on nollasta poikkeava, ja merkitään ensimmäisen tällaisen kertoimen järjestyslukua kirjaimella r.

Koska $q(0) = b_0$, on siis lemman väite yhtäpitävä sille, että $b_0 = 0$. Tehdään *vastaoletus*, että $b_0 \neq 0$, ja osoitetaan, että tämä johtaa mahdottomuuteen; siis $b_0 = 0$ on ainoa mahdollisuus. Mahdottomuus syntyy siten, että etsitään toinen kompleksitason piste z, jossa $|q(z)|$ saakin vielä pienemmän arvon kuin $|q(0)|$, mikä on ristiriidassa sen kanssa, että 0 oli polynomin q minimikohta.

Tarkastellaan ensin katkaistua apupolynomia $\tilde{q}(z) = b_0 + b_r z^r$, ja havaitaan, että tälle osataan ratkaista nollakohta. Nimittäin $\tilde{q}(z) = 0$ on yhtäpitävä sille, että $z^r = -b_0/b_r$, ja esittämällä kompleksiluku $-b_0/b_r$ napakoordinaateissa $-b_0/b_r = te^{i\phi}$ nähdään, että $z_1 = \sqrt[r]{t}\, e^{i\phi/r}$ on eräs ratkaisu. (Yhteensä ratkaisuita on täsmälleen r kappaletta. Mitkä ne ovat?)

Tarkastellaan nyt koko polynomia $q(z)$ pisteessä $z = sz_1$, missä $s \in]0, 1[$ on pieni positiivinen reaaliluku. Saadaan

$$|q(sz_1)|$$
$$= \Big|b_0 + b_r s^r z_1^r + \sum_{k=r+1}^{n} b_k s^k z_1^k\Big|$$
$$= \Big|(1 - s^r)b_0 + s^r(b_0 + b_r z_1^r) + s^r \sum_{k=r+1}^{n} b_k s^{k-r} z_1^k\Big|$$
$$\leq (1 - s^r)|b_0| + 0 + s^r \sum_{k=r+1}^{n} |b_k| s^{k-r} |z_1|^k.$$

Kun $s \to 0$, myös $s^{k-r} \to 0$ kaikilla $k \in \{r+1, \ldots, n\}$, ja siis viimeinen summa lähestyy nollaa. Erityisesti voidaan valita jokin pieni positiivinen s_1 niin, että tämän

loppusumman arvo kohdassa $s = s_1$ on korkeintaan $\frac{1}{2}|b_0|$. Tällöin siis

$$|q(s_1 z_1)| \leq (1 - s_1^r)|b_0| + s_1^r \cdot \frac{1}{2}|b_0|$$
$$= (1 - \frac{1}{2}s_1^r)|b_0| < |b_0| = |q(0)|,$$

ja tämä on haettu ristiriita vastaoletukselle, että $|q(0)| = |b_0| > 0$, sillä $|q(0)|$ oli oletuksen perusteella polynomin q pienin arvo. Siis vastaoletuksen täytyy olla väärä, ja täten $q(0) = 0$, mikä oli todistettava. □

Lopuksi

Algebran peruslause nojaa oleellisesti kompleksilukujen ominaisuuksiin. Vastaava väite reaaliluvuille ei pidä paikkaansa: reaalikertoimisella polynomilla ei tarvitse olla reaalista nollakohtaa, kuten helppo esimerkki $p(x) = x^2 + 1$ osoittaa. Kompleksilukuihin päädytään luonnostaan, kun määritellään tälle polynomille kuvitteelinen nollakohta i reaalilukujen joukon ulkopuolelta ja tarkastellaan laajennettua lukukuntaa $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$. Algebran peruslause siis kertoo sen yllättävän tuloksen, että täydentämällä reaalilukuja tämän yhden polynomin nollakohdilla, saadaan samalla kaikkien muidenkin polynomien nollakohdat.

Mutta missä kohtaa todistusta sitten käytettiin kompleksilukujen erityisominaisuuksia reaalilukuihin nähden? Suurin osa yllä olevasta todistuksesta toimisi yhtä hyvin reaalilukujen joukossa. Ratkaiseva kohta oli nollakohdan hakeminen apupolynomille $\tilde{q}(z) = b_0 + b_r z^r$. Oleellista oli se, että jokaisella kompleksiluvulla on r:s juuri kompleksilukujen joukossa, mutta reaaliluvuilla tämä ominaisuus horjuu jo neliöjuuren kohdalla.

Verkko-Solmusta `http://solmu.math.helsinki.fi` löytyviä oppimateriaaleja

Jaksolliset desimaaliesitykset algebrallisesta näkökulmasta (Jaska Poranen ja Pentti Haukkanen)

Algebra (Tauno Metsänkylä ja Marjatta Näätänen)

Algebra (K. Väisälä)

Geometrian perusteita (Matti Lehtinen)

Geometria (K. Väisälä)

Matematiikan peruskäsitteiden historia (Erkki Luoma-aho)

Matematiikan historia (Matti Lehtinen)

Matemaattista fysiikkaa lukiolaiselle (Markku Halmetoja ja Jorma Merikoski)

Lukuteorian helmiä lukiolaisille (Jukka Pihko)