PERUSASIOITA ALGEBRASTA

Matti Lehtinen

Tässä luetellut lauseet ja käsitteet kattavat suunnilleen sen, mitä algebrallisissa kilpatehtävissä edellytetään. Ns. algebrallisia struktuureja, jotka ovat nykyaikaisen algebran keskeisiä tutkimuskohteita, kilpatehtävissä ei juuri käsitellä.

1 Hyödyllisiä identiteettejä

Kaavojen manipuloinnissa tavallisimmin hyödyksi käytettäviä identiteettejä ovat binomin potenssikaavojen ohessa mm.

$$a^2 - b^2 = (a-b)(a+b),$$
$$a^2 + b^2 + c^2 + 2(ab + bc + ca) = (a+b+c)^2,$$
$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$
$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2 + b^2 + c^2 - bc - ca - ab)$$
$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Seuraavat summaidentiteetit tulevat myös aika ajoin käyttöön:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6},$$
$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}, \qquad \sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3},$$
$$\sum_{k=1}^{n} k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4},$$
$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}, \qquad \sum_{k=0}^{n}(a+bk) = \frac{(n+1)(2a+bn)}{2},$$
$$\sum_{k=0}^{n} aq^k = \frac{a(1-q^{n+1})}{1-q}, \quad (q \neq 1).$$

2 Polynomit

Olkoot a_0, a_1, ..., a_n kiinteitä lukuja. Muuttujan x funktio p,

$$p(x) = a_0 + a_1x + \cdots + a_nx^n,$$

on (yhden muuttujan) polynomi. Jos $a_n \neq 0$, niin p:n *aste* on n, $n = \deg p$. Luvut a_i ovat polynomin p *kertoimet*, jos ne ovat kaikki kokonaislukuja, rationaalilukuja, reaalilukuja tai kompleksilukuja, puhutaan vastaavasti kokonaiskertoimisesta, rationaalikertoimisesta, reaalikertoimisesta tai kompleksikertoimisesta polynomista.

Kahden muuttujan polynomi on vastaavasti funktio

$$p(x,\,y) = a_0 + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \cdots + a_{n0}x^n + a_{n-1,1}x^{n-1}y + \cdots + a_{0n}y^n.$$

Kahden muuttujan polynomin aste on n, jos jokin kertoimista $a_{n-k,k} \neq 0$. Useamman kuin kahden muuttujan polynomit ja niiden aste määritellään analogisesti. Kilpatehtävissä saattaa esiintyä useamman kuin yhden muuttujan polynomeja, mutta yleensä niin, että olennaisesti tarvitaan yhden muuttujan polynomin ominaisuuksia.

Jos $p(r) = 0$, niin r on p:n *nollakohta* tai *juuri*. Jos polynomin aste on $\leq n$, mutta sen nollakohtien lukumäärä on $> n$, niin polynomi on identtisesti nolla eli *nollapolynomi*. Tästä seuraa, että jos kahdella polynomilla on sama arvo useammassa pisteessä kuin polynomeista asteluvultaan suuremman asteluku, niin molemmat polynomit ovat identtisesti samat.

Kahden muuttujan polynomi $p(x,\,y)$ voi olla $= 0$ äärettöämän monessa pisteessä $(x,\,y)$. Tällaisten pisteiden sanotaan muodostavan *algebrallisen käyrän*.

Toisen asteen reaalikertoimisella polynomilla $p(x) = ax^2 + bx + c$, $a \neq 0$, on tasan kaksi reaalista nollakohtaa, jos sen *diskriminantti* $\Delta = b^2 - 4ac$ on positiivinen. Jos $\Delta = 0$, p:llä on tasan yksi reaalinen nollakohta. Jos $\Delta < 0$, p:llä ei ole reaalisia nollakohtia, mutta kylläkin kaksi kompleksista nollakohtaa. Nollakohtien lausekkeet ovat

$$r_{1,2} = \frac{1}{2a}(-b \pm \sqrt{\Delta}).$$

Toisen asteen polynomi voidaan täydentää neliöksi:

$$ax^2 + bx + c = a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right];$$

tästä nähdään mm., että tapauksessa $\Delta < 0$ $p(x)$ on kaikilla x samanmerkkinen kuin a.

Jos u ja v ovat polynomeja ja $\deg u \geq 1$, niin on olemassa polynomit q ja r, $\deg r < \deg u$, siten, että

$$v(x) = q(x)u(x) + r(x). \tag{1}$$

Polynomit q ja r voidaan määrittää jakolaskualgoritmilla jakokulmassa. Jos u ja v ovat rationaali- tai reaalikertoimisia, niin q ja r ovat samaa lajia. Jos u ja v ovat kokonaislukukertoimisia ja u:n korkeinta astetta olevan termin kerroin on 1, niin myös q ja r ovat kokonaislukukertoimisia. Jos $r = 0$, niin v on jaollinen u:lla.

Polynomi h on polynomien u ja v *suurin yhteinen tekijä*, jos u ja v ovat molemmat jaollisia h:lla ja h on jaollinen jokaisella polynomilla, jolla u ja v ovat jaollisia. Jos h_1 ja h_2 ovat u:n ja v:n suurimpia yhteisiä tekijöitä, niin $h_2 = ch_1$, missä c on vakio. Suurin yhteinen tekijä löydetään soveltamalla *Eukleideen algoritmia*.

Kun jakoyhtälöä (1) sovelletaan polynomiin $v(x) = x - a$, saadaan

$$u(x) = (x - a)q(x) + u(a).$$

Jos a on u:n juuri, niin u on jaollinen $(x - a)$:lla.

Jos
$$p(x) = (x-a)^m q(x)$$
ja $q(a) \neq 0$, niin a on p:n m-kertainen juuri. Polynomin juurien kertalukujen summa on enintään polynomin aste.

Polynomi p on *jaoton*, jos siitä, että $p(x) = u(x)v(x)$ seuraa, että joko u tai v on vakio eli nollannen asteen polynomi. Polynomi saattaa olla esim. rationaalikertoimisena jaoton, mutta reaalikertoimisena jaollinen jne. ($p(x) = x^2 - 2$ on rationaalikertoimisena jaoton, koska $\sqrt{2}$ on irrationaaliluku, muttei reaalikertoimisena: $p(x) = (x-\sqrt{2})(x+\sqrt{2})$.)

Jokainen vähintään astetta 1 oleva reaalikertoiminen polynomi voidaan kirjoittaa jaottomien polynomien tulona; esitys on yksikäsitteinen, paitsi tekijöiden järjestystä ja sitä, että tekijät voidaan kertoa vakioilla.

Jos
$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
on kokonaiskertoiminen polynomi ja jos rationaaliluku $\dfrac{s}{q}$, missä s:n ja q:n suurin yhteinen tekijä on 1, on p:n juuri, niin s on a_0:n tekijä ja q on a_n:n tekijä.

Jos r_1 ja r_2 ovat polynomin $x^2 + ax + b$ nollakohdat, niin $r_1 + r_2 = -a$ ja $r_1 r_2 = b$. Yleisemmin, jos $r_1, r_2, \ldots, r_n$ ovat polynomin
$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
juuret (useampikertaiset juuret lueteltuna kertalukunsa osoittaman määrän kertoja) ja jos S_i on summa, jonka yhteenlaskettavina ovat kaikki mahdolliset i:stä luvuista $r_1, \ldots, r_n$ muodostetut tulot, niin $S_1 = -a_{n-1}$, $S_2 = a_{n-2}$, $\ldots$, $S_i = (-1)^i a_{n-i}$, $S_n = (-1)^n a_0$. (S_i:t ovat n:n muuttujan *symmetrisiä polynomeja*. $S_1 = r_1 + r_2 + \cdots + r_n$, $S_2 = r_1r_2 + r_1r_3 + \cdots + r_1r_n + r_2r_3 + \cdots + r_{n-1}r_n$, $S_3 = r_1r_2r_3 + r_1r_2r_4 + \cdots + r_{n-2}r_{n-1}r_n$ jne., $S_n = r_1r_2\cdots r_n$.)

Jos $x_1, x_2, \ldots, x_n$ ovat keskenään eri lukuja ja $y_1, y_2, \ldots, y_n$ mielivaltaisia lukuja, on olemassa yksikäsitteinen enintään astetta $n-1$ oleva polynomi p, jolle pätee $p(x_1) = y_1$, $p(x_2) = y_2$, $\ldots$, $p(x_n) = y_n$. p löydetään käyttämällä *Lagrangen interpolaatiokaavaa*: merkitään
$$g(x) = (x-x_1)(x-x_2)\cdots(x-x_n)$$
ja
$$g'(x_1) = (x_1-x_2)(x_1-x_3)\cdots(x_1-x_n),$$
$$g'(x_2) = (x_2-x_1)(x_2-x_3)\cdots(x_2-x_n)$$
jne. Silloin
$$p(x) = \frac{g(x)y_1}{(x-x_1)g'(x_1)} + \frac{g(x)y_2}{(x-x_2)g'(x_2)} + \cdots + \frac{g(x)y_n}{(x-x_n)g'(x_n)}.$$

3 Kompleksiluvut.

Kompleksiluvut ovat muotoa $z = x + iy$, missä $x = \Re z$ ja $y = \Im z$ ovat reaalilukuja ja $i^2 = -1$. Kertolasku:

$$zw = (x + iy)(u + iv) = xu - yv + i(xv + yu).$$

Jakolasku:

$$\frac{z}{w} = \frac{x + iy}{u + iv} = \frac{xu + yv + i(-xv + yu)}{u^2 + v^2}.$$

Kompleksiluvun $z = x + iy$ *liittoluku* eli *kompleksikonjugaatti* on kompleksiluku $\overline{z} = \overline{x + iy} = x - iy$. Pätee

$$\overline{z + w} = \overline{z} + \overline{w},$$
$$\overline{zw} = \overline{zw}$$
$$\overline{az} = a\overline{z}, \quad a \in \mathbf{R}.$$

Kompleksiluvun z reaali- ja imaginaariosat voidaan lausua z:n ja $\overline{z}$:n avulla:

$$x = \Re z = \frac{1}{2}(z + \overline{z}) \qquad y = \Im z = \frac{1}{2i}(z - \overline{z}).$$

Kompleksiluvun $z = x + iy$ *itseisarvo* $|z|$ on ei-negatiivinen luku

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}.$$

Itseisarvolle pätee $|zw| = |z||w|$, josta $|z^n| = |z|^n$, ja $|z + w| \leq |z| + |w|$.

Jos $z = x + iy$ samastetaan xy-tason pisteen $P = (x, y)$ kanssa, voidaan kirjoittaa $x = |z| \cos\phi$, $y = |z| \sin\phi$, missä ϕ on x-akselin ja suoran OP välinen kulma. Siis

$$z = |z|(\cos\phi + i\sin\phi) = |z|e^{i\phi}.$$

Tässä on käytetty *Eulerin kaavaa*

$$\cos\phi + i\sin\phi = e^{i\phi}.$$

– Kulmaa ϕ sanotaan z:n *argumentiksi*, $\phi = \arg z$.

Kompleksiluvun esitys itseisarvon ja argumentin avulla johtaa kaavoihin

$$zw = |z||w|e^{i(\arg z + \arg w)},$$
$$\frac{z}{w} = \frac{|z|}{|w|}e^{i(\arg z - \arg w)},$$
$$z^n = |z|^n e^{in\arg z}.$$

Viimeinen kaava pätee kaikilla eksponenteilla n, ja mahdollistaa siten esim. juurien ottamisen kompleksiluvuista.

Algebran peruslause. Jokaisella kompleksilukukertoimisella polynomilla p, jonka aste on ≥ 1, on ainakin yksi kompleksinen nollakohta.

Jos reaalikertoimisella polynomilla p on kompleksinen juuri z, on myös $0 = \overline{p(z)} = p(\overline{z})$. Reaalikertoimisen polynomin kompleksijuuren ohella sen liittoluku on myös juuri. Koska

$$(x - z)(x - \overline{z}) = x^2 - 2x\Re z + |z|^2,$$

nähdään, että reaalikertoiminen polynomi voidaan aina esittää ensimmäistä tai toista astetta olevien jaottomien polynomien tulona.

Yhtälön $z^n = 1$ juuret eli *n:nnet yksikköjuuret* ovat luvut 1, $e^{i2\pi/n}$, $e^{i4\pi/n}$, $\ldots$, $e^{i2(n-1)\pi/n}$.

4 Kolmannen ja neljännen asteen yhtälöt

Kolmannen asteen yhtälö $x^3 + ax^2 + bx + c = 0$ voidaan sijoituksella $x = y - \dfrac{a}{3}$ saada muotoon $y^3 + py + q = 0$. Kun tähän sijoitetaan $u + v = y$, tullaan yhtälöön

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Valitaan u ja v niin, että $3uv = -p$. Tällöin u tulee toteuttamaan yhtälön

$$u^3 - \frac{p^3}{27u^3} - q = 0.$$

Tämä on muuttujan $t = u^3$ toisen asteen yhtälö. Kun tämä yhtälö ratkaistaan ja tehdyt sijoitukset puretaan, saadaan alkuperäisen kolmannen asteen yhtälön ratkaisukaavat, *Cardanon kaavat.*

Yleisestä neljännen asteen yhtälöstä voidaan samoin hävittää kolmannen asteen termi. Tarpeen on ratkaista yhtälö

$$x^4 + ax^2 + bx + c = 0 \tag{2}$$

eli

$$\left(x^2 + \frac{a}{2}\right)^2 = -bx - c + \frac{a^2}{4}.$$

Jos x on (2):n ratkaisu ja y mielivaltainen, niin

$$\left(x^2 + \frac{a}{2} + y\right)^2 = -bx - c + \frac{a^2}{4} + 2y\left(x^2 + \frac{a}{2}\right) + y^2 \tag{3}$$

Pyritään valitsemaan y niin, että yhtälön (3) oikea puoli olisi myös täydellinen neliö. Tämä saadaan aikaan valitsemalla oikean puolen x:n toisen asteen polynomin diskriminantti on nolla. Diskriminantin nollaehto on kolmannen asteen yhtälö y:lle. Kun se ratkaistaan ja tulos sijoitetaan (3):een, saadaan kahden neliön yhtäsuuruus. Kun siitä otetaan neliöjuuri, jää jäljelle x:n toisen asteen yhtälö, josta x voidaan ratkaista.