POLYNOM OCH EKVATIONER

Torbjörn Tambour

Matematiska institutionen

Stockholms universitet

Experimentupplaga 2003

Postadress

Matematiska institutionen
Stockholms universitet
106 91 Stockholm

Besöksadress

Kräftriket hus 5 och 6, Stockholm

Internet

www.math.su.se

Till lärare och läsare

Föreliggande kompendium är tänkt att användas i undervisningen i algebra för blivande lärare och en grundkurs kan lämpligen omfatta avsnitten 1.1, 1.2, 1.3, 1.4.1, 2.1, 2.2, 2.3 (valda delar), 2.5, 2.7 och 2.8. Anledningen till att kompendiet innehåller mer stoff än så är att jag tror att en lärare i sin verksamhet i skolan kan ha glädje av att kunna ta reda på mer avancerade saker, som Cardanos formler, när någon elev frågar. Dessutom vet jag att det finns studenter som är intresserade av sådant också. De flesta övningarna har jag tagit från skrivningar som givits vid institutionen.

Jag tar tacksamt emot synpunkter och påpekanden om fel.

Stockholm på Kyndelsmässodagen 2003

Torbjörn Tambour

torbjorn@math.su.se

Innehåll

Kapitel 1

Polynom

1.1 Inledning

Sedan skolan känner Du säkert till funktioner av typen

$$f(x) = 2x - 3 \quad \text{och} \quad g(x) = -x^2 + x - 5.$$

Sådana funktioner är väldigt viktiga i hela matematiken och vi skall på de här sidorna diskutera deras grundläggande egenskaper. Som Du också känner till kallas sådana funktioner med ett gemensamt namn för *polynom* eller *polynomfunktioner*. Ordet polynom är sammansatt av grekiskans *polys*, som betyder många och latinets *nomen*, namn eller term.

Allmänt är ett polynom ett uttryck av formen

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

där $a_0, a_1, \ldots, a_n$ är några tal, som kallas polynomets *koefficienter*.[1] Koefficienterna kan vara heltal, rationella tal, reella tal eller till och med komplexa tal. Polynom betecknas ofta med $p(x)$ eller $q(x)$ (eller $f(x)$ och $g(x)$ som ovan). I vilken ordning man skriver termerna i ett polynom är oväsentligt, men man brukar skriva antingen $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ eller i omvänd ordning, dvs $p(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$. Vilket sätt man väljer beror på vad man sysslar med och man måste helt enkelt vänja sig vid båda

[1] Ordet kommer från latinet och är sammansatt av *ko-*, sam- eller med-, och *efficio*, verka eller utgöra.

sätten. Här är några fler exempel på polynom:

$$\begin{aligned} p_1(x) &= x - 1 && (1.1)\\ p_2(x) &= x^2 + 1 && (1.2)\\ p_3(x) &= 6x^4 - \frac{1}{5}x^3 - \frac{50}{37}x^2 + 1001x - \frac{2}{99} && (1.3)\\ p_4(x) &= x^{1000042} && (1.4)\\ p_5(x) &= -3 && (1.5)\\ p_6(x) &= 0,12x^3 + 3,14x^2 - 100,57x + 1,49 && (1.6)\\ p_7(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 && (1.7) \end{aligned}$$

(Som Du ser har jag här valt att inte ge polynomen olika bokstäver som namn, utan istället numrerat dem från 1 till 7.) Exponenten i den högsta potens av x som förekommer i ett polynom $p(x)$ kallas polynomets *grad* och betecknas $\deg p$ efter det engelska ordet för grad, degree. För polynomen vi skrev ner nyss har vi sålunda

$$\begin{aligned} \deg p_1 &= 1\\ \deg p_2 &= 2\\ \deg p_3 &= 4\\ \deg p_4 &= 1000042\\ \deg p_5 &= 0\\ \deg p_6 &= 3\\ \deg p_7 &= 10 \end{aligned}$$

Det här förtjänar ett par kommentarer. Med uttrycket ”att en potens av x förekommer” i ett polynom menar vi förstås att den har en koefficient som inte är 0. Man skulle mycket väl kunna skriva t ex

$$p_2(x) = 0x^4 + 0x^3 + x^2 + 0x + 1,$$

men de termer som har koefficienter 0 är inte intressanta. De potenser av x som förekommer i p_2 är x^2 och x^0. Lägg således märke till att $x^0 = 1$! Ett polynom i vilket alla koefficienter utom möjligen a_0 är 0 kallas ett *konstant* polynom. Det polynom i vilket *alla* koefficienter (inklusive a_0) är 0, kallas *nollpolynomet*. Man tilldelar inte nollpolynomet någon grad (av skäl som strax skall framgå).

Det x som förekommer i alla polynomen ovan kallas *variabel* eller emellanåt *obestämd*. Det är inte alls nödvändigt att använda bokstaven x för variabeln; ibland kanske x redan är upptaget (och man skall undvika att använda samma bokstav i flera olika betydelser) och då måste man helt enkelt ta till någon annan bostav, t ex y, z eller t. Vi har exempelvis $p_4(t) = t^{1000042}$. Det är inte alls nödvändigt att använda en bokstav för variabeln, man kan ta vilken symbol som helst om man känner för det, så här:

$$p_6(\spadesuit) = 0,12\spadesuit^3 + 3,14\spadesuit^2 - 100,57\spadesuit + 1,49$$

men om man ofta använder exotiska symboler så blir man betraktad som en excentriker. En sak som däremot är viktig att behärska är att kunna ersätta variabeln med något annat uttryck, så här:

$$p_2(1+t) = (1+t)^2 + 1 = 1 + 2t + t^2 + 1 = t^2 + 2t + 2$$

eller

$$\begin{aligned} p_6(2-y) &= 0,12(2-y)^3 + 3,14(2-y)^2 - 100,57(2-y) + 1,49 \\ &= 0,12(2^3 - 3\cdot 2^2 \cdot y + 3\cdot 2\cdot y^2 - y^3) + 3,14(2^2 - 2\cdot 2\cdot y + y^2) \\ &\quad -100,57(2-y) + 1,49 \\ &= -0,12y^3 + 3,86y^2 + 89,57y - 187,13 \end{aligned}$$

som den ambitiöse (ganska) lätt kontrollerar.

1.1.1 Övningar

1. Skriv följande polynom på vanlig form: $p_1(1-x)$, $p_3(2t-1)$, $p_5(55x+32)$.

1.2 Aritmetik med polynom

Aritmetik med polynom låter ju tjusigt, men det handlar inte om något annat än konsten att räkna med dem. Man adderar, subtraherar och multiplicerar dem på samma sätt som man gör med vilka algebraiska uttryck som helst. Exempelvis har vi

$$\begin{aligned} 3p_2(x) - p_6(x) &= 3(x^2+1) - (0,12x^3 + 3,14x^2 - 100,57x + 1,49) \\ &= -0,12x^3 + (3 - 3,14)x^2 + 100,57x + 3 - 1,49 \\ &= -0,12x^3 - 0,14x^2 + 100,57x + 1,51. \end{aligned}$$

Här har det faktiskt insmugit sig en operation till, nämligen multiplikation av ett polynom med ett tal (i termen $3p_2(x)$), men den är naturligtvis också helt

oproblematisk. Ett exempel till:

$$\begin{aligned}
p_2(x)\cdot p_3(x) &= (x^2+1)(6x^4-\frac{1}{5}x^3-\frac{50}{37}x^2+1001x-\frac{2}{99})\\
&= x^2\cdot 6x^4 - x^2\cdot\frac{1}{5}x^3 - x^2\cdot\frac{50}{37}x^2 + x^2\cdot 1001x - x^2\cdot\frac{2}{99}\\
&\quad +6x^4-\frac{1}{5}x^3-\frac{50}{37}x^2+1001x-\frac{2}{99}\\
&= 6x^6-\frac{1}{5}x^5-\frac{50}{37}x^4+1001x^3-\frac{2}{99}x^2\\
&\quad +6x^4-\frac{1}{5}x^3-\frac{50}{37}x^2+1001x-\frac{2}{99}\\
&= 6x^6-\frac{1}{5}x^5+(6-\frac{50}{37})x^4+(1001-\frac{1}{5})x^3\\
&\quad +(-\frac{2}{99}-\frac{50}{37})x^2+1001x-\frac{2}{99}\\
&= 6x^6-\frac{1}{5}x^5+\frac{172}{37}x^4+\frac{5004}{5}x^3-\frac{5024}{3663}x^2+1001x-\frac{2}{99}.
\end{aligned}$$

Läsaren har kanske redan observerat vad som händer med graden när man multiplicerar polynom. Låt $p(x)$ och $q(x)$ vara polynom av grad n respektive m. Om termerna av högst grad är a_nx^n respektive b_mx^m (där alltså koefficienterna a_n och b_m är skilda från 0), så är termen av högst grad i produkten $p(x)\cdot q(x)$ lika med

$$a_nx^n\cdot b_mx^m = a_nb_mx^n\cdot x^m = a_nb_mx^{n+m},$$

vilket visar att graderna *adderas*. Vi har bevisat vår första viktiga sats.

Sats 1 *Om varken $p(x)$ eller $q(x)$ är nollpolynomet, så gäller*

$$\deg(pq) = \deg p + \deg q.$$

Sats 1 är förklaringen till att man inte tilldelar nollpolynomet någon grad. För om man bestämde sig för att låta det ha grad N och insisterade på att Sats 1 skall gälla för alla polynom inklusive nollpolynomet, så skulle man få

$$\deg(0\cdot q) = \deg 0 + \deg q$$

för alla polynom $q(x)$. Eftersom $0\cdot q = 0$, så ger detta $N = N + \deg q$, dvs $\deg q = 0$ för alla $q(x)$, vilket ju ser illa ut. Man kan tilldela nollpolynomet vilken grad man vill, men hur man än gör, så måste man alltid utesluta det från Sats 1.

Det finns ingen motsvarighet till Sats 1 för addition av polynom. Vad man kan säga är att graden av en summa $p(x)+q(x)$ är högst lika med det största av talen $\deg p$ och $\deg q$, men frånsett det kan nästan vad som helst hända.[2] Om $p(x) = x^3-2x^2+5x+4$ och $q(x) = -x^3+2x^2-5x-1$ så är $p(x)+q(x) = 3$ och alltså $\deg(p+q) = 0$.

[2]För att det överhuvudtaget skall vara meningsfullt att tala om graden av summan måste den naturligtvis vara skild från nollpolynomet.

1.2.1 Övningar

1. Beräkna $-p_1(x) + p_2(x)p_5(x)$ och $p_4(x) - x^{1000040}p_2(x)$.

2. Beräkna produkten $p_1(x) \cdot p_7(x)$. Förvånad? Räkna även ut produkterna $(x-1)(x^2+x+1)$ och $(x-1)(x^5+x^4+x^3+x^2+x+1)$. Kan du räkna ut produkten

$$(x-1)(x^m + x^{m-1} + \ldots + x^2 + x + 1)$$

i allmänhet? [3] Prickarna betyder att alla potenser av x mellan x^2 och x^{m-1} finns med.

1.3 Polynom som funktioner

1.3.1 Faktorsatsen.

Hittills har vi behandlat polynom bara som algebraiska uttryck, men Du är förmodligen van att betrakta dem som *funktioner* också. Om $p(x) = a_n x^n + \ldots + a_1 x + a_0$ så blir $p(x)$ en funktion genom att man sätter in tal på x:s plats. Värdet av p för $x = \alpha$ (eller i punkten α, som man ofta säger) är alltså[4]

$$p(\alpha) = a_n\alpha^n + \ldots + a_1\alpha + a_0.$$

Om exempelvis $p(x) = x^3 - x^2 + x - 1$, så är

$$\begin{aligned} p(3) &= 3^3 - 3^2 + 3 - 1 = 27 - 9 + 3 - 1 = 20 \\ p\left(-\frac{2}{5}\right) &= \left(-\frac{2}{5}\right)^3 - \left(-\frac{2}{5}\right)^2 + \left(-\frac{2}{5}\right) - 1 = -\frac{203}{125} \\ p(1) &= 1^3 - 1^2 + 1 - 1 = 0. \end{aligned}$$

De tal man sätter in behöver inte vara reella, det går alldeles utmärkt att låta x anta komplexa värden också:

$$\begin{aligned} p(1-i) &= (1-i)^3 - (1-i)^2 + (1-i) - 1 \\ &= 1 - 3i + 3i^2 - i^3 - (1 - 2i + i^2) + 1 - i - 1 \\ &= 1 - 3i - 3 + i - (1 - 2i - 1) + 1 - i - 1 = -2 - i. \end{aligned}$$

Ett tal α sådant att $p(\alpha) = 0$ kallar man ett *nollställe* till p. Tydligen är 1 ett nollställe till polynomet $x^3 - x^2 + x - 1$ och i är ett nollställe till $x^2 + 1$ eftersom $i^2 + 1 = -1 + 1 = 0$. En trivial men viktig observation är att om α är ett nollställe till p, så är det ett nollställe till alla produkter $p(x)q(x)$ eftersom

[3] Att räkna ut produkten "i allmänhet" betyder att du skall räkna ut den för alla värden på m, dvs hitta en allmän formel. Ibland är det matematiska språket lite annorlunda än vardagens.

[4] α är den grekiska bokstaven alfa, och motsvarar vårt a. Det är den första bokstaven i det grekiska alfabetet.

$p(\alpha)q(\alpha) = 0 \cdot q(\alpha) = 0$. Exempelvis är α nollställe till alla polynom av formen $(x-\alpha)q(x)$. Faktum är att α är nollställe *bara* till polynom av formen $(x-\alpha)q(x)$, vilket är innebörden av nästa sats:

Sats 2 (Faktorsatsen) *Låt $p(x)$ vara ett polynom. Ett tal α är ett nollställe till p om och endast om det finns ett polynom $q(x)$ sådant att*

$$p(x) = (x - \alpha) \cdot q(x).$$

Här bör Du stanna upp och tänka igenom vad satsen betyder! Det finns två påståenden i den. Det ena är att *om* $p(x) = (x - \alpha)q(x)$, så är $p(\alpha) = 0$. Det andra är att α är ett nollställe till $p(x)$ *endast om* $p(x) = (x - \alpha)q(x)$ för något polynom q. Betydelsen av uttrycket "endast om" är att om $p(\alpha) = 0$, så måste $p(x)$ ha formen $(x - \alpha)q(x)$. Det är viktigt att Du förstår detta, liksom att Du tänker igenom skillnaden mellan de två påståendena i satsen. Lägg särskilt märke till att de så att säga går åt olika håll. Matematiken (och matematikern!) använder inte bara formler och siffror när den (eller hon/han) uttrycker sig, det vanliga språket används naturligtvis också. Men matematikens sätt att använda det skiljer sig ibland i nyanserna från vad man är van vid i vardagslag och det är synnerligen viktigt att man är medveten om detta och självklart att man lär sig den korrekta innebörden i uttryck som "om och endast om".

Faktorsatsen är ett av de viktigaste resultaten[5] i den grundläggande polynomteorin och det är viktigt att Du förstår innebörden i den. För att den skall bli riktigt klar så skall vi ge inte mindre än tre bevis för satsen.

Första beviset för faktorsatsen: När man skall bevisa ett "om och endast om"-påstående, så delar man ofta upp i en "om"-del och en "endast om"-del. Det skall vi göra här också och börjar med "om", dvs vi skall bevisa att om $p(x) = (x - \alpha)q(x)$ för något polynom q, så är α ett nollställe till p. Men det var ju precis vad vi gjorde ovan, så den här riktningen är redan klar. Den intressanta riktningen är således "endast om", dvs att om $p(\alpha) = 0$, så är p av formen $p(x) = (x - \alpha)q(x)$ för något polynom q.

Vi börjar med ett särskilt enkelt specialfall, nämligen fallet $\alpha = 0$. Sedan skall vi använda specialfallet för att bevisa påståendet i allmänhet. Alltså: Vad händer om $\alpha = 0$ och således $p(0) = 0$? Om vi skriver

$$p(x) = a_n x^n + \ldots + a_1 x + a_0$$

och sätter $x = 0$ så får vi

$$p(0) = a_0.$$

Om $p(0) = 0$ så är tydligen $a_0 = 0$. Vi får då

$$p(x) = a_n x^n + \ldots + a_1 x = x(a_n x^{n-1} + \ldots + a_1) = xq(x),$$

[5] "Resultat" är ytterligare ett exempel på uttryck som finns i matematikens vokabulär, men som har en lite annan betydelse än i vardagsspråket. Det betyder helt enkelt "bevisat påstående".

där $q(x)$ är polynomet $a_n x^{n-1} + \ldots + a_1$. Detta visar att påståendet är sant åtminstone då $\alpha = 0$. Vi har med andra ord bevisat specialfallet och nu skall vi bevisa påståendet allmänt. Vi inför ett ögonblick ett nytt polynom $p_1(x)$ som $p_1(x) = p(x + \alpha)$ (i uttrycket för p ersätter vi således variabeln x med $x + \alpha$). Då är

$$p_1(0) = p(0 + \alpha) = p(\alpha).$$

Men enligt förutsättningen är $p(\alpha) = 0$, så vi får $p_1(0) = 0$. Enligt specialfallet vi nyss bevisade har vi $p_1(x) = xq_1(x)$ för något polynom q_1. Eftersom $p_1(x) = p(x + \alpha)$, så är $p(x) = p_1(x - \alpha)$ och alltså

$$p(x) = p_1(x - \alpha) = (x - \alpha)q_1(x - \alpha) = (x - \alpha)q(x),$$

där $q(x) = q_1(x - \alpha)$. Beviset är klart!

Andra beviset för faktorsatsen: Här skall vi använda en viktig och intressant likhet, nämligen

$$x^k - y^k = (x - y)(x^{k-1} + yx^{k-2} + y^2x^{k-3} + \ldots + y^{k-2}x + y^{k-1}),$$

som gäller för alla tal y.[6] För $k = 2$, 3 och 4 lyder den

$$\begin{aligned} x^2 - y^2 &= (x - y)(x + y) \quad \text{(konjugatregeln)} \\ x^3 - y^3 &= (x - y)(x^2 + xy + y^2) \\ x^4 - y^4 &= (x - y)(x^3 + x^2y + xy^2 + y^3) \end{aligned}$$

vilka man lätt verifierar genom att multiplicera ihop faktorerna i högerleden. Beviset för ett allmänt k går till på precis samma sätt, det gäller bara att vara omsorgsfull i bokföringen av alla termer:

$$\begin{aligned} & (x - y)(x^{k-1} + x^{k-2}y + x^{k-3}y^2 + \ldots + y^{k-1}) \\ = \quad & x^k + x^{k-1}y + x^{k-2}y^2 + \ldots + xy^{k-1} \\ & \quad - x^{k-1}y - x^{k-2}y^2 - \ldots - xy^{k-1} - y^k \\ = \quad & x^k - y^k \end{aligned}$$

Lägg märke till hur elegant termerna parvis tar ut varandra! Om vi sätter $q_k(x) = x^{k-1} + x^{k-2}y + x^{k-3}y^2 + \ldots + xy^{k-2} + y^{k-1}$, så gäller med andra ord

$$x^k - y^k = (x - y)q_k(x).$$

Som vanligt skriver vi vårt polynom p som $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Vi får nu

$$\begin{aligned} p(x) - p(y) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \\ &- (a_n y^n + a_{n-1}y^{n-1} + \ldots + a_1 y + a_0) \\ &= a_n(x^n - y^n) + a_{n-1}(x^{n-1} - y^{n-1}) + \ldots + a_1(x - y). \end{aligned}$$

[6] Man kan betrakta även y som en variabel om man vill. I så fall har vi här ett exempel på räkning med polynom i *två* variabler x och y. Det går alldeles utmärkt att räkna med och studera polynom i två och flera variabler också.

Termerna här har formen $a_k(x^k - y^k)$. Men $x^k - y^k = (x-y)q_k(x)$ och sätter vi in det så får vi

$$\begin{aligned} p(x) - p(y) &= a_n(x-y)q_n(x) + a_{n-1}(x-y)q_{n-1}(x) + \ldots + a_1(x-y) \\ &= (x-y)(a_n q_n(x) + a_{n-1}q_{n-1}(x) + \ldots + a_1) \\ &= (x-y)q(x), \end{aligned}$$

där $q(x) = a_n q_n(x) + a_{n-1}q_{n-1}(x) + \ldots + a_1$ är polynomet inom parentesen. De räkningar vi hittills har genomfört i det här beviset är giltiga för vilket polynom p som helst, men nu skall vi använda förutsättningen att $p(\alpha) = 0$. Sätt därför $y = \alpha$; vi har $p(x) - p(\alpha) = p(x) - 0 = p(x)$, varav $p(x) = (x-\alpha)q(x)$, vilket är exakt vad vi ville bevisa.

En intressant konsekvens av likheten $p(x) - p(y) = (x-y)q(x)$ är att *för alla tal a gäller*

$$p(x) = (x-a)q(x) + p(a)$$

för något polynom $q(x)$. (Koefficienterna i q beror på a.) Man kan faktiskt bevisa detta direkt från faktorsatsen också. För vilket a som helst så har ju polynomet $p_1(x) = p(x) - p(a)$ nollstället a (ty $p_1(a) = p(a) - p(a) = 0$). Enligt faktorsatsen är således $p(x) - p(a) = p_1(x) = (x-a)q(x)$ för något polynom q, dvs $p(x) = (x-a)q(x) + p(a)$.

1.3.2 Hur många nollställen kan ett polynom ha?

Med hjälp av faktorsatsen skall vi nu bevisa att *ett polynom av grad n kan ha högst n nollställen*. Vi skall börja med att diskutera så kallade *multipla nollställen*. Låt $p(x)$ vara ett polynom och α ett nollställe. Enligt faktorsatsen finns det ett polynom $q(x)$ sådant att $p(x) = (x-\alpha)q(x)$. Det kan mycket väl hända att α är nollställe även till q, dvs $q(\alpha) = 0$. Ett exempel är $p(x) = x^3 - 3x^2 - 9x + 27$. Det är lätt att kontrollera att 3 är ett nollställe till p och att $p(x) = (x-3)q(x)$, där $q(x) = x^2 - 9$. Nu är det ju faktiskt så att 3 är ett nollställe även till q och $q(x) = (x-3)(x+3)$. Alltså är $p(x) = (x-3)^2(x+3)$. Här säger man att 3 är ett nollställe av *multiplicitet* 2 till p eller att 3 är ett *dubbelt* nollställe till p. Multipliciteten anger alltså det antal gånger som ett tal är nollställe till ett polynom. Vårt polynom $p(x) = x^3 - 3x^2 - 9x + 27$ har ju ytterligare ett nollställe, nämligen -3 och det har multiplicitet 1. Man kan också formulera detta så här: Vi säger att talet α är ett nollställe av multiplicitet k till p om

$$p(x) = (x-\alpha)^k q(x)$$

där q är ett polynom sådant att $q(\alpha) \neq 0$, dvs som inte har nollstället α.

Om nu β är ett annat nollställe till p (dvs $\beta \neq \alpha$), så har vi $(\beta-\alpha)^k q(\beta) = 0$. Eftersom $\beta - \alpha \neq 0$, så är $(\beta-\alpha)^k \neq 0$, varför $q(\beta) = 0$. Om β har multiplicitet l som nollställe till q så får vi $q(x) = (x-\beta)^l r(x)$ för något polynom r sådant att $r(\beta) \neq 0$. Detta ger i sin tur

$$p(x) = (x-\alpha)^k q(x) = (x-\alpha)^k (x-\beta)^l r(x),$$

och vi ser att β har multiplicitet l även som nollställe till p. Så här kan vi förstås fortsätta och till slut får vi följande: Låt $\alpha_1, \alpha_2, \ldots, \alpha_m$ vara *alla olika* nollställen till p och beteckna deras multipliciteter med $k_1, k_2, \ldots, k_m$. Då har vi tydligen

$$p(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\ldots(x-\alpha_m)^{k_m}q(x),$$

där q är ett polynom som *saknar nollställen*. Tar vi graden av båda leden så får vi

$$\begin{aligned}\deg p &= \deg(x-\alpha_1)^{k_1} + \deg(x-\alpha_2)^{k_2} + \ldots + \deg(x-\alpha_m)^{k_m} + \deg q \\ &= k_1 + k_2 + \ldots + k_m + \deg q\end{aligned}$$

och eftersom $\deg q$ alltid är ≥ 0, så måste

$$k_1 + k_2 + \ldots + k_m \leq \deg p. \tag{1.8}$$

Men summan $k_1 + k_2 + \ldots + k_m$ är det totala antalet nollställen till p, om vi räknar dem med multiplicitet. Vi sammanfattar:.

Sats 3 *Ett polynom av grad n har högst n nollställen om dessa räknas med multiplicitet.*

Av satsen följer förstås att p kan ha högst n *olika* nollställen.

Lägg märke till att vi i formuleringen av Sats 3 inte sade något om vilken typ av nollställen det är fråga om, dvs om de är rationella tal, reella eller komplexa. Satsen är sann vilka nollställen vi än studerar; med andra ord kan vi också säga att ett polynom av grad n har högst n reella nollställen, om de räknas med sin multiplicitet. Men vi kan också säga att ett polynom av grad n har högst n *komplexa* nollställen (inklusive de som råkar vara reella), vilket ju är ett starkare påstående. Om man bara tittar på reella nollställen kan nästan vad som helst hända. Polynomet $x^3 + x^2 - x - 1$ är lika med $(x-1)(x+1)^2$ och har tydligen två olika nollställen, 1 och -1, där det senare har multiplicitet 2. Det har alltså precis lika många reella nollställen som sin grad. Polynomet $x^4 - x^3 + 2x^2 - x + 1$ å andra sidan är lika med $(x^2+1)(x^2-x+1)$ och har inga reella nollställen alls. Men det har *komplexa* nollställen så att det förslår. Den första faktorn $x^2 + 1$ har nollställena i och $-i$ och med en liten räkning (gör den!) kan man verifiera att den andra faktorn $x^2 - x + 1$ också har två nollställen, nämligen $(1+i\sqrt{3})/2$ och $(1-i\sqrt{3})/2$. Alltså har $x^4 - x^3 + 2x^2 - x + 1$ lika många komplexa nollställen som sin grad, nämligen 4. Den här lilla undersökningen antyder att man kanska kan förbättra Sats 3 i det fall då man är intresserad av komplexa nollställen. Så är det verkligen:

Sats 4 (Algebrans fundamentalsats) *Ett polynom av grad n har exakt n komplexa nollställen om de räknas med multiplicitet.*

Observera att även t ex 1, -7 och $-5\sqrt{3}/8$ är komplexa tal, eftersom de reella talen finns med bland de komplexa! Satsen är som vi såg inte sann om man

byter ut "komplexa" mot "reella". Sitt namn – algebrans fundamentalsats – har satsen naturligtvis för att den betraktas som väldigt viktig. Satsen har en lång och intressant historia och det första beviset gavs i Carl Friedrich Gauss (1777-1855) doktorsavhandling 1799. Gauss var verksam i Göttingen i Tyskland och är en av historiens absolut största matematiker.

Låt $p(x) = a_n x^n + \ldots + a_1 x + a_0$ vara ett polynom av grad n och $\alpha_1, \ldots, \alpha_m$ av multipliciteter $k_1, \ldots, k_m$ samtliga nollställen (så att $k_1 + \ldots + k_m = n$). Då kan vi tydligen faktorisera p enligt

$$p(x) = (x - \alpha_1)^{k_1} \ldots (x - \alpha_m)^{k_m} q(x),$$

för något polynom q. Men graden av p är n och graden av produkten $(x - \alpha_1)^{k_1} \ldots (x - \alpha_m)^{k_m}$ är också n, så q måste ha grad 0 och är alltså en konstant. Om man tittar på x^n-termen i båda leden så ser man att $q(x) = a_n$, dvs högstagradskoefficienten i p, således

$$p(x) = a_n (x - \alpha_1)^{k_1} \ldots (x - \alpha_m)^{k_m}.$$

Kom ihåg att nollställena α_i i allmänhet är komplexa och att det här påståendet inte är sant om man begränsar sig till t ex reella nollställen.

Ett viktigt specialfall är då p har den enkla formen $p(x) = x^n - a$ för någon exponent n. Ett nollställe till detta kallas en n:te rot ur a. Man kan bevisa att om $a \neq 0$, så är alla nollställen enkla, varför det finns precis n stycken n:te rötter ur a. Om a är reellt och ≥ 0, så kan man vidare bevisa att exakt en av dessa är reell och positiv och den betecknas $\sqrt[n]{a}$. Men kom ihåg att den här beteckningen är begränsad till det fall då a är reellt och ≥ 0! (Visserligen bryter emellanåt även matematiker mot denna begränsningsregel, men det som är tillåtet för Jupiter är ju som bekant inte tillåtet för oxen ...) De två nollställena till $x^2 - a$ kallas kvadraträtter ur a och om $a \geq 0$ så betecknas den som är ≥ 0 med $\sqrt{a}$. Lägg alltså på minnet att varje (komplext) tal har exakt två kvadraträtter (utom 0, som bara ha en enda).

1.3.3 När är två polynom lika?

En fråga som kan verka trivial, men som har ett visst djup, är den här: När är två polynom lika? Ett lite bättre sätt att formulera den är så här: Vad skall man mena med likhet mellan polynom? Vi måste börja med att säga några ord om skillnaden mellan polynom och polynomfunktioner. Ett *polynom* är ett "algebraiskt uttryck" av typen $p(x) = x^2 + x + 1$ och det ger upphov till en *polynomfunktion* när vi ersätter x med tal. Skillnaden mellan polynom och motsvarande polynomfunktioner är subtil, men inte därmed oviktig. Låt

$$\begin{aligned} p(x) &= a_n x^n + \ldots + a_1 x + a_0 \quad \text{och} \\ q(x) &= b_m x^m + \ldots + b_1 x + b_0 \end{aligned}$$

vara två polynom. Läsaren håller säkert med om att en rimlig definition av likhet mellan dessa är att de har *samma koefficienter*, dvs $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$

osv (vilket speciellt medför att de har *samma grad*; tänk igenom det!). Vi skriver likhet mellan polynom som $p = q$. Polynomen $p(x) = x^2 + x + 1$ och $q(x) = x^2 - x + 1$ är således inte lika, $p \neq q$.

Likhet mellan funktioner (inte bara polynomfunktioner) definieras på följande sätt: två funktioner $f(x)$ och $g(x)$ är lika om de antar samma värden överallt, dvs om $f(a) = g(a)$ för alla tal a. Det är självklart att om p och q är lika som *polynom*, så är de lika även som *polynomfunktioner*, men den springande punkten är den här frågan:

> *Antag att polynomen p och q ger upphov till samma polynomfunktion, dvs att $p(a) = q(a)$ för alla tal a. Är då p och q lika som polynom, dvs har de samma koefficienter?*

Som läsaren säkert gissar så är svaret på frågan "ja". För låt oss betrakta polynomet $r(x) = p(x) - q(x)$. Då har vi ju $r(a) = p(a) - q(a) = 0$ för alla tal a, så r har *oändligt många nollställen*. Men det enda polynom som har oändligt många nollställen är nollpolynomet, så p och q är lika som polynom också.

1.3.4 Övningar

1. Visa det finns ett polynom $q(x)$ sådant att $x^9 + x^7 + x^5 + x^3 + x + 5 = (x + 1)q(x)$.

2. Bestäm ett tredjegradspolynom med heltalskoefficienter som har nollställena $1/2, 1/3$ och $1/4$.

3. Bestäm ett andragradspolyom med heltalskoefficienter som har nollställena $-5/6$ och $1/7$.

4. Ange ett polynom som har nollställena $1/2$ av multiplicitet 3, -2 av multiplicitet 2 samt $\sqrt{2}$ av multiplicitet 1.

1.4 Polynomdivision och delbarhetsteori

1.4.1 Polynomdivision

Teorin för division av polynom har stora likheter med division av heltal. (Med division vi här menar *division med rest*). När man dividerar två tal så går för det mesta inte divisionen jämnt upp, utan man får en rest. Om talen t ex är 104 och 11 så får man $104 = 9 \cdot 11 + 5$. *Kvoten* är här 9 och *resten* är 5. Om resten när man dividerar a med b blir 0, så säger man som Du vet sedan tidigare i kursen att b delar a eller att a är delbart med b och man skriver denna relation $b \mid a$. Definitionen av delbarhet mellan polynom är precis densamma som för heltal:

Definition: Låt $p_1(x)$ och $p_2(x)$ vara två polynom. Vi säger att p_2 *delar* p_1 om det finns ett polynom $q(x)$ sådant att $p_1(x) = q(x) \cdot p_2(x)$. Istället för "$p_2$ delar

p_1" säger man även "p_1 är *delbart* med p_2". Det är bekvämt att ha en symbol för detta och vi skriver $p_2(x) \mid p_1(x)$ för att beteckna att p_2 delar p_1.

Vi använder alltså samma symbol för delbarhet mellan polynom som vi använder i heltalsfallet och det är lika viktigt här att fundera igenom vad $p_2 \mid p_1$ betyder. Lägg således märke till att detta är ett *påstående* och inte en räkneoperation; det betyder alltså *inte* p_2 delat med p_1 eller något liknande.

Exempel: Polynomet $x^5 - 32$ är delbart med $x - 2$, dvs $x - 2 \mid x^5 - 32$, eftersom $x^5 - 32 = (x^4 + 2x^3 + 4x^2 + 8x^3 + 16)(x - 2)$.

Exempel: Polynomet $2x^3 + 3x^2 - 1$ är delbart med $x^2 + 2x + 1$ eftersom $2x^3 + 3x^2 - 1 = (2x - 1)(x^2 + 2x + 1)$.

Exempel: Polynomet $2x^3 + 3x^2 - 1$ är delbart med $3x^2 + 6x + 3$ eftersom $2x^3 + 3x^2 - 1 = (\frac{2}{3}x - \frac{1}{3})(3x^2 + 6x + 3)$.

Exempel: Att $x^5 - 33$ inte är delbart med $x - 2$ kan man bevisa så här: Antag att $x^5 - 33$ vore delbart med $x - 2$, dvs $x^5 - 33 = q(x)(x - 2)$ för något polynom q. Sätter vi här $x = 2$ så får vi $2^5 - 33 = -1 = q(2)(2 - 2) = 0$, vilket ju är en motsägelse.

Det sista exemplet ovan kan förstås generaliseras: för att $p(x)$ skall vara delbart med $x - a$ så krävs att $p(a) = 0$, dvs att a är ett nollställe till p. Ty om $p(x) = q(x)(x - a)$, så får vi $p(a) = q(a)(a - a) = 0$. Att $p(a) = 0$ är alltså ett *nödvändigt* villkor för att $x - a \mid p(x)$. Men enligt faktorsatsen är det även *tillräckligt*, för om $p(a) = 0$, så finns enligt satsen ett polynom $q(x)$ sådant att $p(x) = q(x)(x - a)$. Vi kan alltså formulera satsen så här också:

Sats 5 (Faktorsatsen) *Ett polynom $p(x)$ är delbart med $x - a$ om och endast om $p(a) = 0$.*

Vi lämnar delbarhetsbegreppet en stund och går över till polynomdivision i praktiken. Om Du inte känner Dig helt säker på heltalsdivison, så rekommenderar jag att Du repeterar det nu. Man kan sammanfatta heltalsdivisionen så här: låt a och b vara två heltal, $b \neq 0$. Då finns tal q och r sådana att

$$a = q \cdot b + r \quad \text{och} \quad 0 \leq r < b.$$

Talet q kallas *kvot* och r kallas *rest*. Man kan komplettera detta med att talen q och r är entydigt bestämda, dvs det finns bara ett q och ett r som duger. För polynom gäller istället det här: låt $f(x)$ och $g(x)$ vara två polynom, där g inte är nollpolynomet. Då finns polynom $q(x)$ och $r(x)$ sådana att

$$f(x) = q(x) \cdot g(x) + r(x)$$

och där $r(x)$ antingen är nollpolynomet (i vilket fall $g(x)$ delar $f(x)$) eller $\deg r < \deg g$. Självklart kallar vi q kvot och r rest. För att finna kvoten och resten använder man samma algoritm som för heltal. Eftersom räkningarna kan organiseras på olika sätt (trappa, liggande stol eller enligt någon annan artikel

i IKEA-katalogen) och jag inte vet vilken modell Du föredrar, så skall jag bara beskriva principen, Du måste sedan själv räkna övningar för att lära Dig hur man gör! Din lärare kommer säkert att räkna några exempel. Låt oss illustrera metoden – *divisionsalgoritmen* – med $f(x) = 3x^4 + 2x^3 - 5x^2 + x + 7$ och $g(x) = x^2 - 3x - 1$. Polynomet $3x^2 g(x)$ har samma grad som f, nämligen 4, och samma högstagradskoefficient, och vi har

$$\begin{aligned} f(x) - 3x^2 g(x) &= (3x^4 + 2x^3 - 5x^2 + x + 7) - 3x^2(x^2 - 3x - 1) \\ &= 11x^3 - 2x^2 + x + 7 \end{aligned}$$

eller

$$f(x) = 3x^2 g(x) + (11x^3 - 2x^2 + x + 7).$$

Vi upprepar nu detta med f ersatt av $11x^3 - 2x^2 + x + 7$:

$$\begin{aligned} 11x^3 - 2x^2 + x + 7 - 11x g(x) &= (11x^3 - 2x^2 + x + 7) - 11x(x^2 - 3x - 1) \\ &= 31x^2 + 12x + 7 \end{aligned}$$

eller

$$11x^3 - 2x^2 + x + 7 = 11x g(x) + (31x^2 + 12x + 7).$$

Vi upprepar ytterligare en gång, nu med $31x^2 + 12x + 7$ och $g(x)$:

$$\begin{aligned} 31x^2 + 12x + 7 - 31 g(x) &= (31x^2 + 12x + 7) - 31(x^2 - 3x - 1) \\ &= 105x + 38 \end{aligned}$$

eller

$$31x^2 + 12x + 7 = 31 g(x) + (105x + 38).$$

Här måste vi sluta, eftersom $105x + 31$ har lägre grad (nämligen 1) än $g(x)$ (som har grad 2). Sammanfattar vi detta så får vi

$$\begin{aligned} f(x) &= 3x^2 g(x) + (11x^3 - 2x^2 + x + 7) \\ &= 3x^2 g(x) + 11x g(x) + (31x^2 + 12x + 7) \\ &= 3x^2 g(x) + 11x g(x) + 31 g(x) + (105x + 38) \\ &= (3x^2 + 11x + 31) g(x) + (105x + 38). \end{aligned}$$

Såg Du mönstret? I varje led subtraherar vi med något av typen $ax^k g(x)$ där a och k är valda så att högstagradstermen försvinner. I första steget har vi således valt $a = 3$ och $k = 2$ för att $f(x)$ och $ax^k g(x)$ skall få samma högstagradsterm (nämligen $3x^4$). Resultatet av subtraktionen $f(x) - 3x^2 g(x)$ har då lägre grad än $f(x)$ och i varje steg i algoritmen sänks graden. Det bästa sättet att lära sig polynomdivision är förstås genom att räkna exempel!

Vi vet nu att det alltid finns en kvot $q(x)$ och en rest $r(x)$, som antingen är nollpolynomet (i det fall då divisionen går jämnt upp) eller är ett polynom med lägre grad än $g(x)$. Det finns som sagt flera olika sätt att organisera sina räkningar och man kan ju möjligen fråga sig om man alltid får samma kvot och

rest eller om de beror på vilken metod man använt. Det är faktiskt så att det finns bara en enda kvot och en enda rest. För antag att $q_1(x)$, $r_1(x)$ respektive $q_2(x)$, $r_2(x)$ är två kvoter och rester. I så fall har vi

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

vilket ger

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x).$$

Tydligen är skillnaden $r_2(x) - r_1(x)$ delbar med $g(x)$, men vi vet ju att den har lägre grad än g. Alltså måste den vara nollpolynomet, så att $r_1 = r_2$. Då följer även att $q_1 = q_2$. Hur man går tillväga för att genomföra divisionen spelar således ingen roll för resultatet.

En annan observation som kan verka trivial, men som är viktig, är att om polynomen man börjar med har rationella koefficienter, så kommer även kvoten och resten att ha det, för vi använder inga andra operationer än de vanliga räknesätten när vi dividerar polynom. Motsvarande påstående när man byter ut "rationella koefficienter" mot "reella koefficienter" (eller för den delen "komplexa koefficienter") är förstås också sant. Däremot är det inte säkert att man får heltalskoefficienter i kvot och rest, om man börjar med två polynom som har det; exempelvis är

$$x^2 + 2 = (\frac{1}{2}x - \frac{1}{4})(2x + 1) + \frac{9}{4}$$

resultatet av division av $f(x) = x^2 + 2$ med $g(x) = 2x + 1$. Emellertid gäller att om f och g har heltalskoefficienter och dessutom högstagradskoefficienten i g är 1, så har både kvoten och resten heltalskoefficienter när man dividerar f med g. Tänk igenom varför själv!

En polynomdivision som har ett visst intresse är när $\deg g = 1$. Då är resten antingen 0 eller så har den lägre grad än g. Men i det senare fallet måste graden vara 0, vilket betyder att resten är en konstant. Eftersom nollpolynomet också är konstant, så är resten i vilket fall som helst ett konstant polynom. Låt oss beteckna den med C. Om $g(x) = x-a$, så har vi tydligen $f(x) = (x-a)q(x)+C$. Vi kan faktiskt bestämma värdet på C: sätter vi nämligen $x = a$ så får vi $f(a) = (a - a)q(a) + C = C$. Sammanfattningsvis har vi

$$f(x) = (x - a)q(x) + f(a),$$

resten är med andra ord f:s värde för $x = a$. Om $f(a)$ skulle råka vara 0, så får vi $f(x) = (x - a)q(x)$. Här har vi vårt utlovade *tredje bevis för faktorsatsen.*

1.4.2 Euklides algoritm och största gemensam delare

Du kommer säkert ihåg från avsnittet om heltal att divisionsalgoritmen är början till en stor teori om största gemensam delare, Euklides algoritm, faktorisering i primtal osv och det borde inte komma som någon överraskning att divisionsalgoritmen för polynom leder till en motsvarande teori för dem. En liten skillnad

är att det inte är helt självklart vad man skall mena med största gemensam delare av två polynom, men vi skjuter upp definitionen av detta begrepp lite grand. Vi börjar istället med Euklides algoritm, vilket inte är något annat än en upprepad användning av divisionsalgoritmen, och gör det i form av ett exempel. Vad detta så småningom skall utmynna i är en diskussion av *gemensamma delare* till två polynom f och g, dvs polynom som delar både f och g. [7] Låt

$$\begin{aligned} f(x) &= x^7 + 2x^6 - 5x^5 - 3x^4 + 5x^3 - 3x^2 + 2x + 2 \\ g(x) &= x^6 - x^5 - 2x^4 + 2x^3. \end{aligned}$$

Dividerar vi f med g så får vi

$$f(x) = (x+3)g(x) + (x^4 - x^3 - 3x^2 + 2x + 2) = q_1(x)g(x) + r_1(x),$$

där alltså $q_1(x) = x + 3$ och $r_1(x) = x^4 - x^3 - 3x^2 + 2x + 2$. Vi skall fortsätta och nu dividera $g(x)$ med resten $r_1(x)$:

$$g(x) = (x^2+1)r_1(x) + (x^3 + x^2 - 2x - 2) = q_2(x)r_1(x) + r_2(x).$$

I nästa steg dividerar vi $r_1(x)$ med $r_2(x)$:

$$r_1(x) = (x-2)r_2(x) + (x^2 - 2) = q_3(x)r_2(x) + r_3(x).$$

Vi fortsätter och dividerar $r_2(x)$ med $r_3(x)$:

$$r_2(x) = (x+1)r_3(x) = q_4(x)r_3(x).$$

Här gick tydligen divisionen jämnt upp och vi kan inte fortsätta längre. Vi kan sammanfatta de här divisionerna så här:

$$f = q_1 g + r_1 \tag{1.9}$$
$$g = q_2 r_1 + r_2 \tag{1.10}$$
$$r_1 = q_3 r_2 + r_3 \tag{1.11}$$
$$r_2 = q_4 r_3 \tag{1.12}$$

Det här schemat kallas *Euklides algoritm* (för polynomen f och g). Vad kan man nu dra för slutsatser av schemat? Tja, den första frågan man bör ställa sig är om det alltid är så att de successiva divisionerna förr eller senare tar slut, dvs att man så småningom får en rest som är 0 (mao att någon division går jämnt upp)? Jo, det kunde vi faktiskt ha resonerat oss fram till på förhand. Ty så länge som resten inte är nollpolynomet (och motsvarande division således inte går jämnt upp), så sjunker resternas gradtal:

$$\deg g > \deg r_1 > \deg r_2 > \deg r_3 > \dots$$

[7] En didaktisk princip som jag för det mesta omfattar säger att man inte skall införa ett nytt begrepp eller en ny metod innan man har visat att det finns ett behov av det. Emellanåt måste man dock bryta mot den här principen och låta motivationen komma senare och här har vi alltså ett exempel på en sådan situation.

Men så kan det ju inte hålla på hur länge som helst, för graden av ett polynom är ju alltid ≥ 0! Härav följer att resten förr eller senare faktiskt måste bli 0 (nollpolynomet) och motsvarande division går då jämnt upp. *Euklides algoritm slutar alltså alltid efter ett ändligt antal steg.*[8]

Så till frågan vad vi kan dra för slutsatser av de successiva divisionerna i Euklides algoritm. Låt oss fundera lite över den första divisionen $f(x) = q_1(x)g(x)+r_1(x)$ och i synnerhet vad den kan säga oss om gemensamma delare till f och g. Låt $h(x)$ vara ett polynom som delar både f och g, säg

$$f(x) = f_1(x)h(x) \quad \text{och} \quad g(x) = g_1(x)h(x).$$

Sätter vi in detta i $f = q_1 g + r_1$ så får vi

$$f_1 h = q_1 g_1 h + r_1, \quad \text{dvs} \quad r_1 = f_1 h - q_1 g_1 h = (f_1 - q_1 g_1)h.$$

Den sista likheten betyder att h är en delare även till resten r_1. *En gemensam delare till f och g är därför en gemensam delare även till g och r_1.* På precis samma sätt bevisar man att en gemensam delare till g och r_1 är en delare även till f. Sammanfattningsvis ser vi alltså att *de gemensamma delarna till f och g är precis desamma som de gemensamma delarna till g och r_1.* På exakt samma sätt ser man att de gemensamma delarna till g och r_1 är desamma som de gemensamma delarna till r_1 och r_2, vilka i sin tur är desamma som de gemensamma delarna till r_2 och r_3 (och så vidare om Euklides algoritm hade haft fler steg). Men eftersom $r_2 = q_4 r_3$ så är en gemensam delare till r_2 och r_3 helt enkelt en delare till polynomet r_3. *De gemensamma delarna till f och g är således precis de polynom som delar r_3.* Det här är ju faktiskt ganska sensationellt: istället för att leta efter polynom som delar de *två* polynomen f och g, så kan vi nöja oss med att leta efter polynom som delar r_3. För att sammanfatta:

- Den sista resten i Euklides algoritm (r_3 i vårt exempel) är en delare till både f och g.
- Varje polynom som delar både f och g delar även r_3.

Definition: En *största gemensam delare* till f och g är ett polynom h sådant att (i) h delar både f och g (ii) varje polynom som delar både f och g delar även h.

Enligt vår analys av Euklides algortim finns det verkligen (minst) en största gemensam delare, nämligen den sista resten (r_3 hos oss). Lägg märke till att det inte är självklart att det finns en största gemensam delare; det följer inte direkt av definitionen. Hur många största gemensamma delare kan det finnas? Låt h_1

[8] En *algoritm* är en process eller en metod att räkna ut något, t ex största gemensamma delaren till två heltal, som bara kräver ett ändligt antal steg. Vad vi har resonerat oss fram till är därför att Euklides algoritm för polynom gör skäl för namnet ”algoritm”!

och h_2 vara två stycken. Då har vi både $h_1|h_2$ och $h_2|h_1$ enligt definitionen. Alltså finns det polynom k_1 och k_2 sådana att

$$h_2 = k_1 h_1 \quad \text{och} \quad h_1 = k_2 h_2.$$

Detta ger

$$h_2 = k_1 h_1 = k_1 k_2 h_2, \quad \text{varav} \quad k_1 k_2 = 1.$$

Men vad måste k_1 och k_2 vara för polynom om deras produkt är 1? Jo, de måste vara konstanter.[9] Två största gemensamma delare skiljer sig tydligen bara på en konstant. Man talar ofta om *den* största gemensamma delaren till två polynom, trots att den inte är riktigt entydigt bestämd. I vårt inledande exempel kan varje största gemensam delare till $f(x) = x^7 + 2x^6 - 5x^5 - 3x^4 + 5x^3 - 3x^2 + 2x + 2$ och $g(x) = x^6 - x^5 - 2x^4 + 2x^3$ skrivas $C(x^2 - 2)$ där C är ett tal $\neq 0$.

Vi skall fortsätta analysen av Euklides algoritm. Enligt ekvation (1.11) ovan har vi $r_1 = q_3 r_2 + r_3$, vilket kan skrivas $r_3 = r_1 - q_3 r_2$. Enligt (1.10) är vidare $r_2 = g - q_2 r_1$ och sätter vi in det så får vi

$$r_3 = r_1 - q_3(g - q_2 r_1) = (q_2 q_3 + 1) r_1 - q_3 g.$$

Ekvation (1.9) ger $r_1 = f - q_1 g$ så att

$$r_3 = (q_2 q_3 + 1)(f - q_1 g) - q_3 g = (q_2 q_3 + 1) f + (-q_3 - q_1(q_2 q_3 + 1)) g. \quad (1.13)$$

Om vi sätter $h_1 = (q_2 q_3 + 1)$ och $h_2 = (-q_3 - q_1(q_2 q_3 + 1))$ så har vi alltså

$$r_3 = h_1 f + h_2 g.$$

Det här kan naturligtvis generaliseras till vilka polynom f och h som helst, så vi har bevisat

Sats 6 *Låt p vara den största gemensamma delaren till polynomen f och g. Då finns polynom h_1 och h_2 sådana att $p = h_1 f + h_2 g$.*

Man skall självklart inte försöka memorera alla formler i det här avsnittet (som t ex (1.13)), utan det viktiga är att förstå och lära sig *metoderna* att få fram dem. *Formlerna* är komplicerade och i sig inte intressanta, medan *metoderna* är enkla och synnerligen intressanta.

Vi har tidigare pratat om nollställen till polynom och en fråga vi nu kan svara på är den här: Givet två polynom $f(x)$ och $g(x)$, kan man avgöra om de har några gemensamma nollställen, dvs om det finns något tal α sådant att $f(\alpha) = g(\alpha) = 0$? Svaret är ja: *Polynomen har (minst) ett gemensamt nollställe om och endast om deras största gemensamma delare inte är ett konstant polynom.* För antag först att det finns ett gemensamt nollställe och låt $p(x)$ vara deras största

[9] Om man inte tror på det direkt, så kan man titta på graderna: $\deg k_1 + \deg k_2 = \deg 1 = 0$. Eftersom graden av ett polynom är ≥ 0, så måste $\deg k_1 = \deg k_2 = 0$.

gemensamma delare. Enligt ovan har vi $p(x) = h_1(x)f(x) + h_2(x)g(x)$ för några polynom $h_1(x)$ ochn $h_2(x)$. Sätter vi $x = \alpha$ så får vi

$$p(\alpha) = h_1(\alpha)f(\alpha) + h_2(\alpha)g(\alpha) = 0$$

eftersom $f(\alpha) = g(\alpha) = 0$. Tydligen är α ett nollställe även till p, som då inte kan vara ett konstant polynom. Om å andra sidan största gemensamma delaren inte är konstant, så har den (minst) ett nollställe (enligt algebrans fundamentalsats) och eftersom p delar både f och g, så måste detta vara ett nollställe även till f och g. Största gemensamma delaren till polynomen f och g som vi började med visade sig vara $p(x) = r_3(x) = x^2 - 2$. Nollställena till p är $\pm\sqrt{2}$, vilka alltså är samtliga gemensamma nollställen till f och g. Den intressanta slutsatsen av det här resonemanget är att *det går att avgöra huruvida två polynom har gemensamma nollställen utan att bestämma deras nollställen.*

Vi avslutar det här avsnittet med två viktiga satser:

Sats 7 *Låt $f(x)$, $g(x)$ och $p(x)$ vara tre polynom sådana att $p|fg$. Om största gemensamma delaren till f och p är 1 (ett konstant polynom), så måste $p|g$.*

Bevis: Enligt Euklides algoritm finns polynom h och k sådana att $hf + kp = 1$. Multiplicera denna likhet med g: $hfg + kpg = 1 \cdot g = g$. Enligt förutsättningen i satsen är termen hfg delbar med p och det är självklart att den andra termen kpg är delbar med p, så g måste också vara delbart med p.

Sats 8 *Låt p och q vara två polynom med största gemensam delare 1 och antag att de båda delar ett polynom f. Då är f delbart även med produkten pq, dvs $pq|f$.*

Bevis: Det finns som i det förra beviset polynom h och k sådana att $hp+kq = 1$. Multiplicera detta med f: $fhp + fkq = f$. Eftersom $q|f$ så är den första termen i vänsterledet delbar med pq. Eftersom f är delbart med p så är den andra termen delbar med pq. Alltså är deras summa f delbar med pq.

1.4.3 Primpolynom och faktorisering

Nästa steg i teorin är definitionen av motsvarigheten till primtal:

Definition: Ett *primpolynom* är ett polynom $p(x)$ av grad ≥ 1 som bara är delbart med polynom av formen $Cp(x)$ (där C är en konstant (ett tal) $\neq 0$) samt med konstanta polynom. Ett annat sätt att uttrycka detta är att ett polynom $p(x)$ är primt om det inte kan skrivas som en produkt av polynom av grad $< \deg p$.

Definitionen är lite mer komplicerad än definitionen av primtal, vilket beror på att om p är delbart med q, så är det delbart även med alla multipler Cq av q (där C återigen är ett tal $\neq 0$).[10]

[10] I mer avancerade framställningar av den här teorin använder man ordet ”primpolynom” i en annan betydelse än ovanstående och ”våra” primpolynom kallas då irreducibla polynom.

Exempel: Alla polynom av grad 1 är primpolynom. Polynomet $p_1(x) = x^2 - 4$ är inte primt, eftersom det är delbart med $x+2$ och $x-2$. Polynomet $p_2(x) = x^2 - 2$ är inte primt om man tillåter vilka reella koefficienter som helst eftersom det kan skrivas $p_2(x) = (x+\sqrt{2})(x-\sqrt{2})$. Men hur är det om man bara tillåter polynom med rationella koefficienter? Är $x^2 - 2$ primt eller ej då? Kan det med andra ord skrivas som en produkt av polynom med rationella koefficienter? Nej, för om vi hade en faktorisering, så måste faktorerna ha grad 1, $x^2 - 2 = (x-a)(x-b)$, och då är både a och b nollställen till $x^2 - 2$. Alltså är de lika med $\pm\sqrt{2}$. Polynomet $p_3(x) = x^2 + 1$ är inte primt om man tillåter komplexa koefficienter eftersom $x^2 + 1 = (x + i)(x - i)$. Men om man bara tillåter reella koefficienter, så är det primt.

Huruvida ett polynom är primt eller ej beror alltså väldigt mycket på vad man tillåter för slags faktorer i en faktorisering. Låt oss fundera ett ögonblick över hur situationen ser ut om vi tillåter alla komplexa tal som koefficienter. Enligt algebrans fundamentalsats har varje polynom $p(x)$ av grad ≥ 1 (minst) ett komplext nollställe α, vilket enligt faktorsatsen betyder att det är delbart med $x - \alpha$. *Om* $\deg p > 1$*, så kan det därför inte vara ett primpolynom.* De komplexa primpolynomen är alltså alla polynom av grad 1 och inga andra. Lite senare skall vi bestämma alla reella primpolynom (dvs reella polynom som inte kan skrivas som produkter av polynom med reella koefficienter). Att bestämma alla rationella primpolynom är emellertid ett betydligt svårare och olöst problem. Man bör lägga märke till att egenskapen "att kunna faktoriseras" (dvs att inte vara primpolynom) *inte* är detsamma som att ha nollställen:

Exempel: Polynomet $p_4(x) = x^4 + 4$ är inte primt som polynom med rationella koefficienter, eftersom det kan skrivas $(x^2 + 2x + 2)(x^2 - 2x + 2)$. Däremot har det inga rationella nollställen.

Den viktigaste egenskapen hos primpolynom är den här:

Sats 9 *Låt p vara ett primpolynom som delar en produkt $f \cdot g$. Då måste p dela f eller g (eller båda).*

Bevis: Antag att p inte delar f; då måste vi bevisa att $p|g$. Om vi kan bevisa att största gemensamma delaren till p och f är 1 så följer detta ur Sats 7. Den största gemensamma delaren delar p och är då lika med antingen 1 eller p eftersom p är ett primpolynom. Men den kan inte vara p eftersom den delar f också och vi har ju antagit att p inte delar f. Alltså är största gemensamma delaren till f och p lika med 1. Satsen följer nu som sagt av Sats 7.

Sats 9 har en omedelbar generalisering: Om $p(x)$ är primt och delar en produkt $f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_m(x)$, så måste $p(x)$ dela minst en av faktorerna.

Beviset börjar med frasen "antag att p inte delar $f\ldots$", som kan förtjäna en liten kommentar. I vardagsspråket kan ju "jag antar det" betyda ungefär detsamma som "jag tror det". (På frågan "Skall du gå på föreläsningen imorgon? kan man få svaret "Jag antar det.", eventuellt kompletterad med en lätt uppgiven axelryckning.) Men i matematiken betyder inte "anta" detsamma som

”tro”, utan meningen är att det som antas är en förutsättning i resonemanget som kommer efter. Beviset ovan skulle vi kunna omformulera så här: Det finns två möjligheter: antingen är f delbart med p eller så är det inte det. I det förra fallet är vi ju klara (vi skulle ju bevisa att p delar f eller g) och om det senare fallet handlar resten av beviset. Man måste vänja sig vid matematikens sätt att använda orden, men det kan naturligtvis ta lite tid. I matematiken används således ordet ”anta” på samma sätt som i uttrycket ”anta en lag”; vi antar (anammar) som en förutsättning ett visst påstående. Strindberg – som hade åsikter om både det ena och det andra – lär ha varit upprörd över matematikernas sätt att resonera och undrade irriterat hur de kan anta så mycket utan att vara säkra.

Huvudnumret i det här avsnittet är en motsvarighet till *aritmetikens fundamentalsats*, som säger att ett heltal på ett och endast ett sätt kan skrivas som en produkt av primtal (så när som på ordningen mellan faktorerna):

Sats 10 *Varje polynom kan på ett och endast ett sätt skrivas som en produkt av primpolynom.*

Satsen kräver några kommentarer:

- Man kan förstås kasta om ordningen på faktorerna, t ex
$$x^2 - 4 = (x - 2)(x + 2) = (x + 2)(x - 2).$$
- Vi kan ju exempelvis skriva
$$x^2 - 4 = (x + 2)(x - 2) = (2x + 4)(\frac{1}{2}x - 1),$$
så det verkar ju som om man skulle kunna skriva $x^2 - 4$ som en produkt på åtminstone två olika sätt. Förklaringen till den här skenbara motsägelsen är naturligtvis att $2x + 4 = 2(x + 2)$ och $\frac{1}{2}x - 1 = \frac{1}{2}(x - 2)$, dvs de olika faktorerna skiljer sig bara på konstanter. På det här sättet kan man naturligtvis alltid ”flytta” konstanter mellan faktorerna.
- Faktoriseringen av ett polynom i primpolynom beror i högsta grad på vad man tillåter för koefficienter. Om man bara tillåter rationella tal, så är
$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$
en fullständig faktorisering i primpolynom. Detta är också den fullständiga faktoriseringen om man tillåter alla reella tal som koefficienter, men om man tillåter komplexa tal så har vi
$$x^4 + 4 = (x - (1 + i))(x - (1 - i))(x - (-1 + i))(x - (-1 - i)).$$
- En produkt kan mycket väl ha bara en enda faktor. Polynomet $x^2 + 2$ är exempelvis primt som reellt polynom, så $x^2+2 = x^2+2$ är den fullständiga faktoriseringen i primpolynom. Analogt är $5 = 5$ den fullständiga faktoriseringen av talet 5 i primtal.

Bevis för satsen: Satsen består av två delar; dels att man alltid kan skriva ett polynom som en produkt av primpolynom, dels att det går bara på ett enda sätt (om man tar hänsyn till ovanstående modifikationer). Vi bevisar dessa i tur och ordning. Beteckna polynomet med $p(x)$. Om p har grad 1, så är vi klara, eftersom p då är ett primpolynom. Antag att $\deg p = 2$. Om p är primt, så är vi klara. Annars kan vi skriva p som en produkt av två polynom av grad 1 och dessa är primpolynom. Antag så att p har grad 3. Om p är primt, så är vi återigen klara. Annars kan vi skriva p som en produkt av polynom av lägre grad. Ett har grad 1 och det andra grad 2 och båda dessa kan vi skriva som produkter av primpolynom. På det här sättet kan vi fortsätta. Om vi exempelvis har klarat av polynom av grad ≤ 10, så antag att $\deg p = 11$. Om p är primt, så är vi klara. Annars kan vi skriva p som en produkt av polynom av grad högst 10. Men dem kan vi skriva som produkter av primpolynom (eftersom vi var klara med polynom av grad ≤ 10), och då har vi skrivit även p som en produkt av primpolynom.

Vi kommer nu till *entydigheten*. Vad skulle hända om vi hade två faktoriseringar

$$p(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_m(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_n(x)?$$

Här är alltså alla faktorer p_i och q_j primpolynom. Tydligen är p delbart med p_1, vilket medför att produkten $q_1 q_2 \ldots q_n$ är delbar med p_1. Enligt Sats 9 (eller snarare dess generalisering,som vi nämnde ovan) måste minst en av faktorerna q_j vara delbar med p_1. Vi kan numrera om q:na och anta att $p_1 | q_1$. Men p_1 och q_1 är ju primpolynom, så vi måste ha $q_1(x) = C_1 p_1(x)$ för någon konstant C_1. Nu kan vi förkorta likheten ovan och får

$$C_1 p_2 \ldots p_m = q_2 \ldots q_n.$$

Vi ser att $q_2 \ldots q_n$ är delbart med p_2, så något q_j är delbart med p_2. Vi kan anta $p_2 | q_2$ och får att $q_2 = C_2 p_2$ för någon konstant C_2. Alltså

$$C_1 C_2 p_3 \ldots p_m = q_3 \ldots q_n.$$

Så här kan vi fortsätta och får (eventuellt efter att ha numrerat om faktorerna) $q_3 = C_3 p_3, q_4 = C_4 p_4$ osv. Om t ex n vore större än m, så finge vi till slut

$$C_1 \ldots C_m = q_{m+1} \ldots q_n,$$

vilket är omöjligt eftersom graden av vänsterledet är 0 (det är ju ett konstant polynom). Alltså är $n = m$ och beviset är klart.

Det kanske är en bra idé att sammanfatta allt det här.

- Ett primpolynom är ett polynom som bara är delbart med konstanta polynom och konstanta multipler av sig själv. Alternativt kan man säga att det är primt om det inte kan skrivas som en produkt av två polynom av lägre grad. Huruvida ett polynom är primt eller ej beror på vad man tillåter för koefficienter. Exempelvis är $x^2 - 5$ primt om man bara tillåter rationella koefficienter, men tillåter man reella, så faktoriseras det som $(x + \sqrt{5})(x - \sqrt{5})$.

- Varje (rationellt, reellt, komplext) polynom kan skrivas som en produkt av (rationella, reella, komplexa) primpolynom. Faktoriseringen i primpolynom är entydig så när som ordningen mellan faktorerna och flyttande av konstanter mellan faktorerna.

1.4.4 Hur känner man igen ett primpolynom?

Låt oss börja med det som är det enklaste fallet, nämligen då vi tillåter komplexa tal som koefficienter. Låt p vara ett polynom som är primt betraktat som komplext polynom. Enligt algebrans fundamentalsats har p (minst) ett nollställe α och enligt faktorsatsen gäller $p(x) = (x - \alpha)q(x)$ för något polynom q. Men p var ju primt, så q måste vara en konstant. Slutsatsen är att de komplexa primpolynomen är alla polynom av grad 1 och inga andra (t ex x, $x - 1,89$ och $x - 1 + 3i$).

Redan om vi går över till reella koefficienter så blir det betydligt mer komplicerat. Alla polynom av grad 1 är förstås prima, men nu finns det fler. Polynomet $p(x) = x^2 + 8$ är exempelvis primt som reellt polynom (för annars skulle vi kunna skriva det som en produkt av två förstagradspolynom, och då skulle det ha ett reellt nollställe, vilket det inte har). Men det är naturligtvis inte så att alla andragradspolynom är prima, vilket t ex $x^2 - 8 = (x + 2\sqrt{2})(x - 2\sqrt{2})$ visar. Vi skall visa nedan att primpolynomen med reella koefficienter är dels alla polynom av grad 1, dels alla andragradspolynom utan reella nollställen.

Primpolynom med rationella koefficienter är en betydligt mer komplicerad historia. Det finns ingen "klassifikation" av dem, som i de reella och komplexa fallen och det är oftast utomordetligt svårt att avgöra huruvida ett givet polynom är primt eller inte. Det finns några kriterier som man ibland kan använda, t ex följande:

Sats 11 (Eisensteins kriterium) *Låt $f(x) = a_0 + a_1x + \ldots + a_nx^n$ vara ett polynom med heltalskoefficienter. Om det finns ett primtal p sådant att p inte delar a_n, men alla andra koefficienter och dessutom sådant att p^2 inte delar a_0, så är f primt.*

Av Eisensteins[11] kriterium följer t ex att polynomet $f(x) = x^n - 2$ är primt (som rationellt polynom; man tar $p = 2$) för alla $n \geq 1$, vilket visar att det finns rationella primpolynom av hur hög grad som helst. Att hitta faktoriseringen av ett polynom i primpolynom är också svårt i allmänhet. I fallet med komplexa koefficienter är detta detsamma som att hitta polynomets nollställen, vilket oftast även det är utomordentligt besvärligt.

1.4.5 Övningar

1. Bestäm kvoten och resten då $x^5 + 2x^4 + 3x^3 - x^2 + x - 2$ divideras med $x^2 + x + 1$.

[11] Gotthold Eisenstein, tysk matematiker, 1823-52

2. Bestäm kvoten och resten då $2x^6 + x^5 - 4x^4 - 6x^3 + x^2 - 8x + 1$ divideras med $2x^2 + 1$.

3. Bestäm resten då polynomet $p(x) = (3x^2 - 7x + 4)^2$ divideras med $x - 2$.

4. Bestäm resten då $f(x) = 2x^{100} - 7x^{59} + 6x^{11} - 12x^2 - 2$ divideras med $x + 1$.

5. Vad blir resten då polynomet $3x^{45} - x^{42} + x^{40} + 2x^{35} - 4x^{32} + x^{20} + x^{15} + x^4 - 5x^3 - 2$ divideras med $x - 1$?

6. Visa att polynomet $2x^{98} + x^{40} + 1$ är delbart med $x^2 + 1$.

7. Vad blir resten då $x^{201} + x^{101} + 1$ delas med $x^2 - 1$?

8. Vad blir resten då polynomet $x^{60} - x^{40} + 1$ divideras med $x + 1$?

9. Bestäm resten då $x^{12} + x^5$ divideras med $x^2 + 1$.

10. Ett polynom $p(x)$ ger resten -2 då det divideras med $x-1$ och resten 3 då det divideras med $x+1$. Vad blir resten då p divideras med $(x-1)(x+1)$?

11. Bestäm alla värden på a sådana att polynomen $p(x) = x^3 + 2x^2 - x - 2$ och $q(x) = x^3 + 2x + a$ får en icke-trivial största gemensam delare, och ange dessa.

12. Bestäm största gemensamma delaren till de två polynomen

$$x^6 + x^5 + 3x^4 + 3x^3 + 2x^2 - 1 \quad \text{och} \quad x^4 + x^2 + 1.$$

13. Skriv

$$\frac{2}{x^4 - 5x^2 + 6x - 5} - \frac{1}{x^4 + x^3 - 7x^2 - 2x + 10}$$

på formen $\frac{f(x)}{g(x)}$, där polynomen $f(x)$ och $g(x)$ saknar gemensamma icke-triviala (äkta) faktorer.

1.5 Reella polynom

Vi skall säga några ord om polynom med reella koefficienter och hur de reella primpolynomen ser ut. I diskussionen kommer vi att behöva ett par egenskaper hos komplexkonjugering av komplexa tal:

$$\begin{aligned} \overline{z + w} &= \bar{z} + \bar{w} \\ \overline{zw} &= \bar{z} \cdot \bar{w} \end{aligned}$$

Kom också ihåg att $\bar{z} = z$ om och endast om z är reellt.

Sats 12 *Låt $p(x)$ vara ett polynom med reella koefficienter och z_0 ett nollställe. Då är även det konjugerade talet $\bar{z}_0$ ett nollställe och det har samma multiplicitet som z_0.*

Bevis: Antag att $p(x) = a_0 + a_1x + \ldots + a_nx^n$, där alltså alla a_i är reella. Enligt egenskaperna hos konjugering är då

$$\begin{aligned} 0 &= \bar{0} = \overline{p(z_0)} = \overline{a_0 + a_1z_0 + \ldots + a_nz_0^n} \\ &= \bar{a}_0 + \bar{a}_1\bar{z}_0 + \ldots + \bar{a}_n\bar{z}_0^n \\ &= a_0 + a_1\bar{z}_0 + \ldots + a_n\bar{z}_0^n \\ &= p(\bar{z}_0). \end{aligned}$$

Alltså är $\bar{z}_0$ också ett nollställe. Antag nu att z_0 verkligen är icke-reellt, så att $z_0 \neq \bar{z}_0$. Polynomet p är då delbart med $x - z_0$ och $x - \bar{z}_0$. Om z_0 har multiplicitet ≥ 2 så har $q(x) = p(x)/(x - z_0)(x - \bar{z}_0)$ också nollstället z_0. Samma räkning som vi gjorde nyss visar att $\bar{z}_0$ också är ett nollställe till q. Så kan vi fortsätta och det följer till sist att z_0 och $\bar{z}_0$ har samma multiplicitet.

Sätt $z_0 = a + bi$, där $b \neq 0$. Då är

$$(x - z_0)(x - \bar{z}_0) = x^2 - (z_0 + \bar{z}_0)x + z_0\bar{z}_0 = x^2 - 2ax + a^2 + b^2$$

ett reellt primpolynom. För vore det inte primt, så skulle det faktoriseras i två reella faktorer av grad 1. Men nollställena är ju $z_0, \bar{z}_0$, vilka vi har antagit är icke-reella. Alltså är det primt. Alla polynom av grad 1 är ju prima, men finns det fler reella primpolynom? Nej, det gör det inte: Låt $x_1, \ldots, x_m$ vara alla *reella* nollställen till $p(x) = a_0 + \ldots + a_nx^n$ (eventuellt är en del av dem lika) och räkna upp de icke-reella nollställena i par så här:

$$z_1, \bar{z}_1, z_2, \bar{z}_2, \ldots, z_l, \bar{z}_l$$

(även här kan en del vara lika). (Det finns förstås ett samband mellan graden av p och antalet x_i respektive z_j, nämligen $\deg p = m + 2l$.) Då har p faktoriseringen

$$p(x) = a_n(x - x_1)\ldots(x - x_m)(x - z_1)(x - \bar{z}_1)\ldots(x - z_l)(x - \bar{z}_l),$$

där a_n är p:s högstagradskoefficient. Om vi sätter $z_j = a_j + ib_j$ för $j = 1, \ldots, l$, så är

$$p(x) = a_n(x - x_1)\ldots(x - x_m)(x^2 - 2a_1x + a_1^2 + b_1^2)\ldots(x^2 - 2a_lx + a_l^2 + b_l^2)$$

en faktorisering av p i primpolynom, varav följer att det inte finns några andra reella primpolynom än förstagradspolynomen och andragradspolynom av formen $(x - z_0)(x - \bar{z}_0)$, dvs reella andragradspolynom som saknar reella nollställen.

1.5.1 Övningar

1. Kvadratkomplettera polynomet $p(x) = (x - z_0)(x - \bar{z}_0)$, där $z_0 = a + bi$, $b \neq 0$. (Kvadratkomplettering skall vi diskutera nedan, så Du kan kanske spara den här övningen till senare.)

2. Bevisa att om $f(x)$ är ett reellt polynom sådant att $f(x) \geq 0$ för alla reella tal x, så kan f inte ha några reella nollställen av udda multiplicitet.

3. Låt $f(x)$ vara ett polynom med reella koeficienter sådant att $f(x) > 0$ för alla reella tal x. Bevisa att det finns reella polynom $p(x)$ och $q(x)$ sådana att
$$f(x) = p(x)^2 + q(x)^2.$$

1.6 Användning av derivata

I skolan lärde Du Dig kanske vad *derivatan* av en funktion är för något och hur man kan använda den t ex för att undersöka var en funktion har maxima och minima. Här skall vi använda derivatan på ett annat sätt för att studera polynom. Om Du inte har hört talas om derivata tidigare, så gör det inget; vi skall börja från början. Och även om Du har läst om derivata i skolan, så kommer det här avsnittet att visa på nya sätt att använda begreppet.

Definition: Låt
$$p(x) = a_0 + a_1x + \ldots + a_kx^k + \ldots + a_nx^n$$
vara ett polynom. Derivatan av p definieras då som polynomet
$$p'(x) = a_1 + 2a_2x + 3a_3x^2 + \ldots + ka_kx^{k-1} + \ldots + na_nx^{n-1}.$$

Derivering sänker alltså graden ett steg. Den som har sett derivata tidigare känner förmodligen igen formeln i definitionen (att derivatan av x^k är kx^{k-1} är en av de saker man brukar komma ihåg bäst från gymnasiekursen!), men är säkert inte van vid det här sättet att definiera derivata; i skolböckerna och andra läroböcker för universitetsbruk definieras istället derivatan med hjälp av differenskvoter och som ett visst gränsvärde och man brukar exemplifiera med tangentens lutning. Här behöver vi dock inte hela detta maskineri, utan det räcker med det som står i definitionen ovan (men det gör naturligtvis inget om man har sett den vanliga definitionen också). En sak som är viktig att ha i bakhuvudet nu är att det enda vi vet om derivatan av ett polynom just nu är det som utsägs i definitionen. Nu skall vi härleda några egenskaper.

Sats 13 *Derivatan av ett polynom har följande egenskaper:*

1. $(p+q)'(x) = p'(x) + q'(x)$
2. $(pq)'(x) = p'(x)q(x) + p(x)q'(x)$
3. *om* $p(x) = (x+a)^n$*, där* a *är en konstant, så är* $p'(x) = n(x+a)^{n-1}$.

Den som har sett derivata tidigare känner igen de här egenskaperna, men vi måste nu bevisa att de följer ur definitionen. Observera att $(p+q)(x)$ och $(pq)(x)$ betyder summan respektive produkten av polynomen p och q.

Bevis: Skriv
$$\begin{aligned} p(x) &= a_0 + a_1x + \ldots + a_nx^n \\ q(x) &= b_0 + b_1x + \ldots + b_nx^n. \end{aligned}$$

Här ser det ju ut som om p och q har samma grad, men så behöver det inte vara; eventuellt är några koefficienter 0. Summan av p och q är

$$(p+q)(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n,$$

där $c_k = a_k + b_k$ för $k = 0, 1, \ldots, n$. Enligt definitionen är

$$\begin{aligned}(p+q)'(x) &= c_1 + 2c_2x + \ldots + kc_kx^{k-1} + \ldots + nc_nx^{n-1} \\ &= (a_1+b_1) + 2(a_2+b_2)x + \ldots + n(a_n+b_n)x^{n-1} \\ &= (a_1 + 2a_2x + \ldots + na_nx^{n-1}) + (b_1 + 2b_2x + \ldots + nb_nx^{n-1}) \\ &= p'(x) + q'(x).\end{aligned}$$

Alltså är beviset för 1 klart. Ett annat sätt att formulera beviset är så här: Det räcker att kontrollera att termerna av samma grad i $(p+q)'$ och $p'+q'$ har samma koefficient, eftersom två polynom är lika om och endast om termerna av samma grad har samma koefficient. Men koefficienten för x^{k-1} i $(p+q)'$ är $k(a_k+b_k)$ och i $p'+q'$ är den $ka_k + kb_k$ och dessa två tal är lika.

Vi skall använda metoden att jämföra koefficienter för att bevisa egenskap 2. Vi har inte tidigare härlett någon allmän formel för koefficienten för en viss potens av x i en produkt av polynom, men nu behöver vi det. Om vi utför multiplikationen $p(x)q(x) = (a_0 + \ldots + a_nx^n)(b_0 + \ldots + b_nx^n)$ så får vi termer av typen $a_ix^i \cdot b_jx^j = a_ib_jx^{i+j}$. För att få potensen x^k av x måste $i+j = k$, så koefficienten för x^k är lika med summan

$$a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots + a_kb_0.$$

Vi får att koefficienten för x^{k-1} i derivatan $(pq)'(x)$ är lika med

$$k(a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots + a_kb_0).$$

Det är lite delikatare att skriva ner koefficienten för x^{k-1} i $p'(x)q(x)$ och $p(x)q'(x)$. Låt oss skriva $p'(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$, där $c_0 = a_1, c_1 = 2a_2, \ldots, c_{n-1} = na_n$. Koefficienten för x^{k-1} i $p'(x)q(x)$ blir då

$$c_0b_{k-1} + c_1b_{k-2} + \ldots + c_{k-1}b_0 = a_1b_{k-1} + 2a_2b_{k-2} + \ldots + ka_kb_0.$$

Om vi här byter a och b så får vi koefficienten

$$b_1a_{k-1} + 2b_2a_{k-2} + \ldots + kb_ka_0$$

för x^{k-1} i $p(x)q'(x)$. Det här är lika med

$$ka_0b_k + \ldots + 2a_{k-2}b_2 + a_{k-1}b_1$$

som vi ser om vi kastar om ordningen mellan termerna. Adderar vi de två uttrycken så får vi att koefficienten för x^{k-1} i $p'(x)q(x) + p(x)q'(x)$ är

$$ka_0b_k + ka_1b_{k-1} + \ldots + ka_kb_0$$

vilket är vad vi ville bevisa.

Formel 3 är sann för $n = 1$ för då är den inget annat än definitionen av derivatan av $x+a$. För $n = 2$ kan vi bevisa den genom att använda 2, eftersom $(x+a)^2 = (x+a)\cdot(x+a)$. Derivatan av detta är

$$1 \cdot (x+a) + (x+a) \cdot 1 = 2(x+a).$$

För $n = 3$ skriver vi $(x+a)^3 = (x+a)\cdot(x+a)^2$ och får derivatan

$$1 \cdot (x+a)^2 + (x+a) \cdot 2(x+a) = 3(x+a)^2,$$

där vi använde att vi kände derivatan av $(x+a)^2$. På exakt samma sätt får vi derivatan av $(x+a)^4 = (x+a)\cdot(x+a)^3$. Den blir

$$1 \cdot (x+a)^3 + (x+a) \cdot 3(x+a)^2 = 4(x+a)^3.$$

Om vi vet att formlen är sann för ett visst n, dvs om vi vet att derivatan av $(x+a)^n$ är $n(x+a)^{n-1}$, så kan vi bevisa att den är sann även för exponenten $n+1$ genom att använda 2, ty $(x+a)^{n+1} = (x+a)\cdot(x+a)^n$, så derivatan blir

$$1 \cdot (x+a)^n + (x+a) \cdot n(x+a)^{n-1} = (n+1)(x+a)^n$$

och detta är ju 3 för exponenten $n+1$. Bevismetoden "att gå från n till $n+1$" kallas *(matematisk) induktion.*

1.6.1 Multipla nollställen

Derivatan är ett kraftfullt hjälpmedel för att undersöka polynom:

Sats 14 *Om α är ett nollställe till $p(x)$ av multiplicitet m, så är det ett nollställe till p' av multiplicitet $m-1$. De multipla nollställena till p är precis nollställena till den största gemensamma delaren till p och p'.*

Bevis: Att α har multiplicitet m betyder definitionsvis att $p(x) = (x-a)^m q(x)$ för något polynom q sådant att $q(\alpha) \neq 0$. Deriverar vi detta så får vi

$$\begin{aligned} p'(x) &= m(x-\alpha)^{m-1}q(x) + (x-\alpha)^m q'(x) \\ &= (x-\alpha)^{m-1}(mq(x) + (x-\alpha)q'(x)) = (x-\alpha)^{m-1}q_1(x), \end{aligned}$$

där $q_1(x) = mq(x) + (x-\alpha)q'(x)$. Här syns det att α har mutiplicitet *minst* $m-1$ som nollställe till p'. Men multipliciteten kan å andra sidan inte vara större än $m-1$ eftersom

$$q_1(\alpha) = mq(\alpha) + (\alpha-\alpha)q'(\alpha) = mq(\alpha) \neq 0.$$

Om vi vet att α är ett nollställe till p och har multiplicitet k som nollställe till p', så måste det ha multiplicitet $k+1$ som nollställe till p.[12] Låt nu α vara ett

[12] Det är dock inte sant att ett nollställe till p' måste vara ett nollställe till p. Ett motexempel är $p(x) = x^2 + x$.

nollställe till största gemensamma delaren f till p och p'. Då har det multiplicitet minst 1 som nollställe till p' och alltså är det åtminstone ett dubbelt nollställe till p. Om å andra sidan α är ett multipelt nollställe till p, så är det ett nollställe även till p' enligt första delen av satsen. Låt f vara den största gemensamma delaren till p och p'. Då finns polynom g och h sådana att $f = gp + hp'$ och vi får

$$f(\alpha) = g(\alpha)p(\alpha) + h(\alpha)p'(\alpha) = 0$$

eftersom $p(\alpha) = p'(\alpha) = 0$. Beviset är klart.

Innan vi ser på ett exempel så kan vi observera att en konsekvens av satsen är att *ett primpolynom har bara enkla nollställen.* För om p vore ett primpolynom med ett nollställe α av multiplicitet ≥ 2, så vore α ett nollställe till största gemensamma delaren f till p och p'. Alltså kan f inte vara konstant och det följer att $f = p$ eftersom f delar p, som är primt. Men vi har ju också att $f|p'$, vilket är omöjligt då ju $\deg p' = \deg p - 1 = \deg f - 1$.

Exempel: Polynomet $p(x) = x^n - 1$ har bara enkla nollställen. Ty derivatan är $p'(x) = nx^{n-1}$, som bara har ett enda nollställe, nämligen 0, och det är inte nollställe till p.

Exempel: Bestäm eventuella multipla nollställen till $p(x) = x^4 - 3x^3 + 2x^2 + x - 1$. Derivatan är $p'(x) = 4x^3 - 9x^2 + 4x + 1$ och Euklides algoritm ser ut så här:

$$\begin{aligned} p(x) &= \left(\frac{1}{4}x - \frac{3}{16}\right)p'(x) - \frac{1}{16}(11x^2 - 24x + 13) \\ p'(x) &= \left(\frac{4}{11}x - \frac{3}{121}\right)(11x^2 - 24x + 13) - \frac{160}{121}(x - 1) \\ 11x^2 - 24x + 13 &= (11x - 13)(x - 1) \end{aligned}$$

Största gemensamma delaren är tydligen $f(x) = x - 1$, vilket betyder att det enda multipla nollstället till p är $x = 1$. Man visar lätt (antingen genom division eller genom att gå baklänges i Euklides algoritm) att $p'(x) = (x-1)(4x^2-5x-1)$, där den andra faktorn inte har nollstället 1. Således har 1 multiplicitet 1 som nollställe till p' och det följer att det är ett dubbelt nollställe till p.

1.6.2 Binomialsatsen

I skolan brukar man lära sig att

$$(a + b)^2 = a^2 + 2ab + b^2 \quad \text{(kvadreringsregeln)}$$

och eventuellt att

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

men har man händelsevis inte det så är det lätt att bevisa dessa samband. Binomialsatsen handlar om hur $(a + b)^n$ ser ut när man multiplicerar ihop parenteserna, närmare bestämt i följande mening. När man multiplicerar ihop parenteserna i $(a + b)^n$ kommer man att få en summa av termer som innehåller

varierande potenser av a och b. Den sammanlagda graden i a och b måste vara n i varje term, dvs termerna har utseendet $a^k b^{n-k}$, där $k = 0, 1, 2, \ldots, n$ (jfr fallen $n = 2$ och $n = 3$ ovan). Men frågan är vad koefficienterna för de olika termerna är och det är den frågan som binomialsatsen svarar på. "Binom" betyder ett uttryck med två termer, som t ex $a + b$. Det finns mängder av mer eller mindre olika bevis och vi skall ge ett som använder derivata. Vi behöver ytterligare en beteckning: Med beteckningen $p^{(k)}(x)$ menar vi den k:te derivatan av p, dvs det polynom vi får genom att derivera $p(x)$ k gånger. Den första derivatan av x^n är ju nx^{n-1} och den andra är tydligen $n(n-1)x^{n-2}$. Deriverar vi en gång till så får vi $n(n-1)(n-2)x^{n-3}$ och det är lätt att se att den k:te derivatan är $n(n-1)\ldots(n-k+1)x^{n-k}$. Om vi deriverar x^n sammanlagt n gånger så får vi tydligen en konstant, nämligen

$$n(n-1)(n-2)\ldots 3 \cdot 2 \cdot 1.$$

Den här produkten betecknas med symbolen $n!$, som utläses *n-fakultet*. Vi har således

$$\begin{aligned} 1! &= 1 \\ 2! &= 2 \cdot 1 = 2 \\ 3! &= 3 \cdot 2 \cdot 1 = 6 \\ 4! &= 4 \cdot 3 \cdot 2 \cdot 1 = 24 \quad \text{osv.} \end{aligned}$$

Vi kan uttrycka produkten $n(n-1)\ldots(n-k+1)$ med hjälp av fakulteter genom att förlänga med $(n-k)(n-k-1)\ldots 2 \cdot 1$:

$$\begin{aligned} & n(n-1)\ldots(n-k+1) \\ = & \tfrac{n(n-1)\ldots(n-k+1)\cdot(n-k)(n-k-1)\ldots 2\cdot 1}{(n-k)(n-k-1)\ldots 2\cdot 1} \\ = & \tfrac{n!}{(n-k)!} \end{aligned}$$

Den k:te derivatan av x^n är således

$$\frac{n!}{(n-k)!}x^{n-k}.$$

Man brukar definiera $0! = 1$ och då stämmer den här formeln även för $k = n$.

Låt nu $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ vara vårt gamla vanliga polynom. Om vi deriverar det k gånger så försvinner alla termer av grad $< k$ och vi har

$$p^{(k)}(x) = a_k \cdot k! + a_{k+1}\frac{(k+1)!}{1!}x + \ldots + a_n \frac{n!}{(n-k)!}x^{n-k}.$$

Om vi sätter $x = 0$ så är det bara den konstanta termen som "överlever", dvs

$$p^{(k)}(0) = k! a_k \quad \text{eller} \quad a_k = \frac{p^{(k)}(0)}{k!}.$$

Man kan alltså uttrycka koefficienterna i p med hjälp av p:s derivator i 0.

Nu skall vi använda det här på ett speciellt polynom, nämligen $p(x) = (1+x)^n$. Enligt formel 3 i Sats 13 är den k:te derivatan av p lika med

$$n(n-1)\dots(n-k+1)(1+x)^{n-k} = \frac{n!}{(n-k)!}(1+x)^{n-k},$$

så

$$p^{(k)}(0) = \frac{n!}{(n-k)!}.$$

Det följer att koefficienten för x^k i $(1+x)^n$ är lika med

$$\frac{p^{(k)}(0)}{k!} = \frac{n!}{(n-k)!k!}.$$

Talet i högerledet - den s k *binomialkoefficenten* - förekommer ofta inom alla matematikens grenar och man har därför infört en speciell beteckning för det, nämligen

$$\frac{n!}{(n-k)!k!} = \binom{n}{k},$$

vilket utläses "n över k". Vi har bevisat

Sats 15 (Binomialsatsen)

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots + \binom{n}{k}x^k + \ldots + \binom{n}{n}x^n$$

För att få fram utvecklingen av $(a+b)^n$ gör man omskrivningen

$$(a+b)^n = a^n \cdot \left(1 + \frac{b}{a}\right)^n$$

och sätter $x = b/a$. Genomför detaljerna själv! Binomialkoefficienterna $\binom{n}{k}$ har mängder av intressanta egenskaper:

Exempel: Vi skall beräkna koefficienten för x^k i $(1+x)^{n+1}$ på två olika sätt. Å ena sidan är den enligt binomialsatsen lika med $\binom{n+1}{k}$. Å andra sidan kan vi skriva $(1+x)^{n+1} = (1+x)(1+x)^n$ och i den här produkten får vi en term x^k dels genom att ta 1 ur den första parentesen och x^k ur den andra, dels genom att ta x ur den första parentesen och x^{k-1} ur den andra. Koefficienten är tydligen även lika med $\binom{n}{k} + \binom{n}{k-1}$, så att

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Exempel: Summan av alla $\binom{n}{k}$ för $k = 0, 1, 2, \ldots, n$ är lika med 2^n, vilket man får genom att sätta $x = 1$ i binomialsatsen. Om man istället sätter $x = -1$ så får man att summan

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n\binom{n}{n} = 0.$$

Den mest häpnadsväckande egenskapen hos binomialkoefficienterna, fast kanske inte den man lägger märke till först, är att *de överhuvudtaget är heltal*. För säg att vi börjar i en annan ända än ovan och *definierar* en uppsättning tal $\binom{n}{k}$ genom

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 2\cdot 1}.$$

Det intressanta är det inte finns något uppenbart skäl till varför det skulle gå att förkorta bort faktorerna i nämnaren! Men nu vet vi ju enligt binomialsatsen att $\binom{n}{k}$ är koefficienten för x^k i $(1+x)^n$, som är ett heltal.

1.6.3 Övningar

En del av nedanstående övningar passar bättre att göra efter att Du har läst avsnittet om ekvationer, men eftersom de handlar om multipla nollställen är de placerade här.

1. Finn alla gemensamma rötter till ekvationerna $x^4+x^3-2x^2+3x-1=0$ och $x^4-x^2+2x-1=0$.

2. Har ekvationen $x^4+2x^3-10x-25$ någon dubbelrot?

3. Bestäm eventuella gemensamma rötter till ekvationerna $z^5-6z^3-3z^2+2z=0$ och $z^4+4z^3+6z^2+5z+2=0$.

4. Lös ekvationen $x^4+2x^3+3x^2+2x+1=0$, om vilken man vet att den har dubbelrötter.

5. Undersök om ekvationen $x^4-8x^3+18x^2-8x+1=0$ har någon dubbelrot och bestäm samtliga rötter.

6. Ekvationen $x^4+4x^3-4x^2-16x+16=0$ har (minst) en multipelrot. Lös ekvationen.

7. Ekvationen $x^4+4x^3+2x^2-4x+1=0$ har en multipelrot. Bestäm samtliga rötter.

8. Bestäm koefficienten för x^{79} i utvecklingen av $(2+2x^2)^{158}$.

9. Bestäm koefficienten för x^2 i utvecklingen av $(\frac{x}{3}-\frac{1}{x^3})^{10}$.

10. Bevisa att $\binom{n}{k} = \binom{n}{n-k}$ för alla n och k.

11. Beräkna summan

$$\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \dots + 2^n\binom{n}{n}.$$

12. Bevisa att

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}.$$

Ledning: $(1+x)^{2n} = (1+x)^n \cdot (1+x)^n$

13. Använd $e^{i\pi/4} = (1+i)/\sqrt{2}$ för att bevisa att

$$\begin{aligned}\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \ldots &= 2^{n/2} \cos\frac{n\pi}{4} \\ \binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \ldots &= 2^{n/2} \sin\frac{n\pi}{4}.\end{aligned}$$

Kapitel 2

Ekvationer

2.1 Inledning

En *ekvation* är egentligen ett problem, nämligen det här:

> Bestäm alla x för vilka $f(x) = 0$, där f är någon given funktion.

Funktionen f kan vara nästan vilken som helst, vilket innebär att det finns myriader olika (typer av) ekvationer. Den typ som vi skall studera här kallas *algebraiska ekvationer* och har utseendet $p(x) = 0$, där p är ett *polynom* (ibland kallas de därför också polynomekvationer). I viss mening är de algebraiska ekvationerna den enklaste typen av ekvationer eftersom de inte innehåller något annat än de aritmetiska operationerna addition, subtraktion och multiplikation. Att de är den enklaste typen av ekvationer betyder emellertid inte att de är enkla att lösa,[1] det är i allmänhet ett mycket svårt problem. Här är förresten några exempel på algebraiska ekvationer:

$$5x + 2 = 0 \tag{2.1}$$

$$3x^2 - x - 4 = 0 \tag{2.2}$$

$$x^{11} - 1 = 0 \tag{2.3}$$

$$45,36x^{98} + 0,51x^{86} - 2548x^{13} - 0,0078x^5 + 4711 = 0 \tag{2.4}$$

$$ix^3 + (-2 + i)x^2 - x + 4 - 5i = 0 \tag{2.5}$$

De tal x som uppfyller $p(x) = 0$ kallas ekvationens *rötter* och är alltså nollställena till polynomet p. Om $\deg p = n$ så säger man också att ekvationen $p(x) = 0$ har grad n eller att den är en n:tegradsekvation. Vi skall grundligt diskutera andragradsekvationer nedan. Eftersom ett polynom av grad n har n nollställen (om man räknar dem med multiplicitet, dvs dubbla nollställen två gånger osv), så har en n:tegradsekvation n rötter. Ur matematisk synpunkt är ekvationer av grad 1 inte särskilt intressanta, så vi går direkt på ekvationer av grad 2.

[1] Att lösa en ekvation $f(x) = 0$ betyder förstås att bestämma de tal x som uppfyller $f(x) = 0$.

2.2 Andragradsekvationer

En allmän andragradsekvation har utseendet

$$Ax^2 + Bx + C = 0, \tag{2.6}$$

där koefficienterna A, B och C kan vara vilka tal som helst, rationella, reella eller komplexa. I fortsättningen kan de ofta vara godtyckliga komplexa tal, men då och då måste vi begränsa oss till reella och rationella koefficienter. Vi skall analysera (2.6) på några olika sätt.

För att (2.6) verkligen skall vara en andragradsekvation måste $A \neq 0$ och då kan vi dividera hela ekvationen med A och får

$$x^2 + \frac{B}{A}x + \frac{C}{A} = 0.$$

Vi sätter $p = B/A$, $q = C/A$ och får då ekvationen

$$x^2 + px + q = 0.$$

Läsaren känner förmodligen till en formel för rötterna till den här ekvationen, som ibland går under namnet p, q-formeln. Författaren till de här raderna tycker inte att man skall lära sig formler som den utantill, utan istället förstå och lära sig en *metod* att lösa ekvationen. Lär man sig matematiken som en samling formler utan något egentligt samband med varandra blir hela verksamheten mystisk, obegriplig, omöjlig att förstå och totalt ointressant.

2.2.1 Kvadratkomplettering

I skolan brukar man lära sig *kvadreringsregeln*

$$(\alpha + \beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2$$

och vi skall börja med att använda den för att analysera $x^2 + px + q = 0$. Idén är att vi vill försöka skriva uttrycket $x^2 + px + q$ som en kvadrat, dvs ett uttryck av typen $(x + \alpha)^2$, plus en konstant, alltså

$$x^2 + px + q = (x + \alpha)^2 + \beta.$$

Om vi utvecklar kvadraten i högerledet så får vi

$$x^2 + px + q = x^2 + 2\alpha x + \alpha^2 + \beta$$

så x^2-termerna stämmer i alla fall. För att antalet x-termer skall stämma måste som vi ser $p = 2\alpha$, dvs $\alpha = p/2$ och vi får till sist

$$\beta = q - \alpha^2 = q - \left(\frac{p}{2}\right)^2.$$

Således gäller

$$x^2 + px + q = x^2 + 2 \cdot \frac{p}{2}x + \left(\frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q = \left(x + \frac{p}{2}\right)^2 + q - \left(\frac{p}{2}\right)^2;$$

det är inskjutandet av termen $(p/2)^2$ som kallas *kvadratkomplettering* och tekniken att komplettera kvadraten skall man lära sig (men man skall inte memorera de inblandade formlerna utantill, utan bara själva tekniken!). Ekvationen $x^2 + px + q = 0$ kan nu skrivas

$$\left(x + \frac{p}{2}\right)^2 = \left(\frac{p}{2}\right)^2 - q. \tag{2.7}$$

Låt oss införa beteckningen

$$\Delta = \left(\frac{p}{2}\right)^2 - q$$

(Δ är den grekiska bokstaven delta, som motsvarar vårt D). Om Δ skulle råka vara 0, så har ekvationen utseendet

$$\left(x + \frac{p}{2}\right)^2 = 0$$

och den har då bara en enda rot, nämligen

$$x = -\frac{p}{2}.$$

Denna rot är tydligen en *dubbelrot* och $-p/2$ ett nollställe av multiplicitet 2 till polynomet $x^2 + px + q$. Det är tydligen möjligt att avgöra huruvida ekvationen $x^2 + px + q = 0$ har en dubbelrot utan att lösa den.

Exempel: I ekvationen $x^2 - 4x + 4 = 0$ är $p = -4$ och $q = 4$. Alltså är $\Delta = (-4/2)^2 - 4 = 0$ och ekvationen har en dubbelrot (nämligen $-4/2 = -2$).

Exempel: För att avgöra om $3x^2 + x - 1 = 0$ har en dubbelrot måste vi först dividera med koefficienten för x^2, dvs 3, och får $x^2 + \frac{1}{3}x - \frac{1}{3} = 0$, där $p = \frac{1}{3}$, $q = -\frac{1}{3}$. Således är

$$\Delta = \left(\frac{1}{2 \cdot 3}\right)^2 - \left(-\frac{1}{3}\right) = \frac{13}{36} \neq 0.$$

Ekvationen har tydligen ingen dubbelrot.

För att lösa $x^2 + px + q = 0$ kvadratkompletterar vi först enligt ovan och får efter en stund ekvationen $(x + p/2)^2 = \Delta$. Nästa steg är att vi låter δ (litet delta) vara ett tal sådant att $\delta^2 = \Delta$. Ekvationen övergår nu i $(x + p/2)^2 = \delta^2$ och vi får två möjligheter,

$$x + \frac{p}{2} = \delta \quad \text{eller} \quad x + \frac{p}{2} = -\delta$$

så rötterna blir till slut

$$x_1 = -\frac{p}{2} + \delta \quad \text{och} \quad x_2 = -\frac{p}{2} - \delta.$$

Det här kräver några kommentarer:

- En möjlighet i $(x+p/2)^2 = \delta^2$ är förstås $x + p/2 = \delta$. Men eftersom $(-\delta)^2 = \delta^2$, så är $x + p/2 = -\delta$ en annan (och det finns inte fler).
- Man kan även analysera $(x+p/2)^2 = \delta^2$ på följande vis: Enligt konjugatregeln[2] är

  $$(x+p/2)^2 - \delta^2 = (x+p/2+\delta)(x+p/2-\delta)$$

  och här kan man direkt avläsa rötterna.
- Oavsett vad Δ är så finns det minst ett tal δ sådant att $\delta^2 = \Delta$ (om $\Delta \neq 0$, så finns det två sådana δ). Om Δ är reellt och ≥ 0, så finns det ett positivt δ, vilket man ju betecknar med $\sqrt{\Delta}$. I det fall då p och q är reella tal, så skriver man därför rötterna som

  $$x_1 = -\frac{p}{2} + \sqrt{\Delta} = -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q} \tag{2.8}$$

  $$x_2 = -\frac{p}{2} - \sqrt{\Delta} = -\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q} \tag{2.9}$$

  vilket är den bekanta "p,q-formeln".

Det är dags för ytterligare exempel.

Exempel: Lös ekvationen $5x^2 - x - 3 = 0$. Vi börjar med att dividera med 5 och får $x^2 - \frac{1}{5}x - \frac{3}{5} = 0$. Kvadratkomplettera:

$$\begin{aligned} x^2 - \frac{1}{5}x - \frac{3}{5} &= x^2 - 2\cdot\frac{1}{10}x + \left(\frac{1}{10}\right)^2 - \left(\frac{1}{10}\right)^2 - \frac{3}{5} \\ &= \left(x - \frac{1}{10}\right)^2 - \frac{61}{100} \end{aligned}$$

och vi får ekvationen

$$\left(x - \frac{1}{10}\right)^2 = \frac{61}{100}$$

varav

$$x = \frac{1}{10} \pm \sqrt{\frac{61}{100}} = \frac{1 \pm \sqrt{61}}{10}.$$

Exempel: Lös ekvationen $-2x^2 + 3x + 1 = 0$. Vi dividerar med -2 och får $x^2 - \frac{3}{2}x - \frac{1}{2} = 0$. Kvadratkompletteringen ser i det här fallet ut så här:

$$\begin{aligned} x^2 - \frac{3}{2}x - \frac{1}{2} &= x^2 - 2\cdot\frac{3}{4}x + \left(\frac{3}{4}\right)^2 - \left(\frac{3}{4}\right)^2 - \frac{1}{2} \\ &= \left(x - \frac{3}{4}\right)^2 - \frac{17}{16}. \end{aligned}$$

[2]Trots vad vi tidigare sagt så kan det vara bra att lägga en och annan "regel" på minnet, t ex konjugatregeln. Men innan man lär sig en sådan regel utantill så skall man ha förstått den.

Vi får alltså ekvationen

$$\left(x - \frac{3}{4}\right)^2 = \frac{17}{16}$$

som ger rötterna

$$x = \frac{3}{4} \pm \sqrt{\frac{17}{16}} = \frac{3 \pm \sqrt{17}}{4}.$$

Exempel: Lös ekvationen $x^4 - 10x^2 + 1 = 0$. Det här är ju en ekvation av grad 4 och sådana har vi ännu inte metoder för att lösa allmänt. Dock övergår den i en andragradsekvation i en ny obekant t som vi inför genom $t = x^2$:

$$x^4 - 10x^2 + 1 = (x^2)^2 - 10x^2 + 1 = t^2 - 10t + 1$$

Vi har

$$t^2 - 10t + 1 = t^2 - 2 \cdot 5t + 5^2 - 5^2 + 1 = (t-5)^2 - 24$$

och får $(t-5)^2 = 24$, varav $t = 5 \pm \sqrt{24}$. Vi noterar att eftersom $24 < 25 = 5^2$, så är $\sqrt{24} < 5$ och båda rötterna $5 \pm \sqrt{24}$ är positiva. Eftersom $t = x^2$ så får vi rötterna till den ursprungliga ekvationen genom att dra kvadratrötterna:

$$x = \pm\sqrt{5 \pm \sqrt{24}}.$$

Här skall man kombinera tecknen på alla möjliga sätt, så det blir faktiskt $2 \cdot 2 = 4$ rötter sammanlagt, vilket det skall vara enligt algebrans fundamentalsats. Utskrivna blir de

$$\sqrt{5+\sqrt{24}},\ \sqrt{5-\sqrt{24}},\ -\sqrt{5+\sqrt{24}},\ -\sqrt{5-\sqrt{24}}.$$

Det går att skriva rötterna på en annan lite enklare form. Lägg först märke till att

$$\sqrt{24} = \sqrt{4 \cdot 6} = \sqrt{4} \cdot \sqrt{6} = 2\sqrt{6}.$$

Alltså är

$$\begin{aligned} 5 + \sqrt{24} &= 5 + 2\sqrt{6} = 2 + 2 \cdot \sqrt{2 \cdot 3} + 3 = (\sqrt{2})^2 + 2 \cdot \sqrt{2} \cdot \sqrt{3} + (\sqrt{3})^2 \\ &= (\sqrt{2} + \sqrt{3})^2 \end{aligned}$$

och $\sqrt{5+\sqrt{24}} = \pm(\sqrt{2}+\sqrt{3})$. Men både $\sqrt{5+\sqrt{24}}$ och $\sqrt{2}+\sqrt{3}$ är positiva, så vi har faktiskt $\sqrt{5+\sqrt{24}} = \sqrt{2}+\sqrt{3}$. De andra rötterna visar sig kunna skrivas

$$-\sqrt{2}+\sqrt{3},\ -\sqrt{2}-\sqrt{3},\ \sqrt{2}-\sqrt{3}.$$

Exempel: Lös ekvationen $x^2 - 2x + 2 = 0$. Kvadratkomplettera:

$$x^2 - 2x + 2 = x^2 - 2 \cdot 1 \cdot x + 1^2 - 1^2 + 2 = (x-1)^2 + 1.$$

Vi får ekvationen $(x-1)^2 + 1 = 0$ eller $(x-1)^2 = -1$. Här ser vi omedelbart att ekvationen inte har några reella rötter. Ty om x vore reellt, så vore även

$x-1$ reellt och då vore $(x-1)^2 \geq 0$. Men det finns ju komplexa tal som har kvadraten -1, nämligen $\pm i$. Alltså får vi $x-1 = \pm i$ och rötterna är $x = 1 \pm i$.

Vi skall nu diskutera ekvationer $x^2+px+q = 0$ med reella koefficienter. Kvadratkompletteringen såg vi ovan:

$$x^2 + px + q = \left(x + \frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q$$

och sätter vi som ovan $\Delta = (p/2)^2 - q$ så får vi

$$\left(x + \frac{p}{2}\right)^2 = \Delta.$$

Det finns nu tre möjligheter, $\Delta > 0$, $\Delta = 0$ och $\Delta < 0$. Det andra fallet nämnde vi ovan, det betyder att ekvationen har en dubbelrot. I det första fallet $\Delta > 0$ finns det ett reellt tal δ sådan att $\delta^2 = \Delta$ och vi får två reella rötter $x = -p/2 \pm \delta$. I det tredje fallet $\Delta < 0$ kan det inte finnas några reella rötter (se det sista exemplet ovan). Eftersom $-\Delta > 0$ så finns det ett reellt tal δ sådant att $\delta^2 = -\Delta$. Ekvationen blir $(x+p/2)^2 = -\delta^2 = (-1)\cdot\delta^2 = i^2\cdot\delta^2$, ty $i^2 = -1$. Alltså blir rötterna

$$x = -\frac{p}{2} \pm i\delta.$$

Notera att de två rötterna är *konjugerade komplexa tal*. För en ekvation med reella koefficienter finns således tre möjligheter:

- Den har två olika reella rötter (om $\Delta > 0$).
- Den har en reell dubbelrot (om $\Delta = 0$).
- Den har två icke-reella rötter, som är konjugerade komplexa tal (om $\Delta < 0$).

Tydligen kan man avgöra vilket av dessa tre fall som är för handen utan att lösa ekvationen. Det andra fallet $\Delta = 0$ är speciellt intressant eftersom i så fall $x^2 + px + q = (x - x_1)(x - x_1) = (x - x_1)^2$ är en *kvadrat* (här är förstås x_1 dubbelroten, dvs $x_1 = -p/2$). Om å andra sidan $x^2 + px + q$ är en kvadrat, säg $x^2 + px + q = (x - a)^2$, så är $p = -2a$ och $q = a^2$, så att

$$\Delta = \left(\frac{p}{2}\right)^2 - q = a^2 - a^2 = 0.$$

Tydligen har vi

Sats 16 *Polynomet $x^2 + px + q$ är en kvadrat om och endast om $\Delta = 0$.*

Som avslutning på det här avsnittet skall vi helt kort titta på ett något annorlunda sätt att kvadratkomplettera. Låt oss återigen titta på $p(x) = x^2 + px + q$. Vi skall införa en ny variabel, som vi kallar t, genom $x = t + \alpha$, där α är ett *tal* som vi om en liten stund skall välja så att p får en enkel form. Insättning ger

$$x^2 + px + q = (t + \alpha)^2 + p(t + \alpha) + q = t^2 + (2\alpha + p)t + \alpha^2 + p\alpha + q.$$

Vi ser här att om vi väljer α så att $2\alpha + p = 0$, så försvinner t-termen. Vi väljer således $\alpha = -p/2$ och då blir

$$x^2 + px + q = t^2 + q - \left(\frac{p}{2}\right)^2 (= t^2 - \Delta).$$

Sätter vi tillbaka $t = x - p/2$ i högerledet så får vi

$$x^2 + px + q = \left(x + \frac{p}{2}\right)^2 + q - \left(\frac{p}{2}\right)^2.$$

Det här är ju inget nytt, utan bara en variant av det vi gjorde tidigare.

2.2.2 Övningar

1. Kvadratkomplettera följande andragradspolynom och lös motsvarande ekvationer:
   a) $x^2 + x - 1$
   b) $2x^2 + 2x - 5$
   c) $-3x^2 + x + 1$
   d) $x^2 - 3x + 2$
   e) $5x^2 - 10x + 4$
   f) $x^2 - x\sqrt{2} + 1$
   g) $x^2\sqrt{5} - x(\sqrt{2} + \sqrt{5}) - \sqrt{2}$
2. Lös ekvationen $2x^2 - 10x + 12 = 0$ medelst kvadratkomplettering.
3. Kvadratkomplettera $3x^2 + 18x + 7$.
4. Kvadratkomplettera $3x^2+18x+5$ och lös sedan olikheten $3x^2+18x+5 < 2$.
5. En *gyllene rektangel* är en rektangel i vilken sidorna har ett sådant förhållande att om man tar bort kvadraten på den kortare sidan, så är rektangeln som återstår likformig med den man började med. Bestäm förhållandet mellan sidorna i en gyllene rektangel. (Redan grekerna ansåg att en gyllene rektangel är mycket harmonisk och vacker för ögat. Den svenska flaggan och en vanlig tändsticksask, liksom många tavelramar, är sådana rektanglar (i alla fall nära).)

2.3 Sambanden mellan rötter och koefficienter

Vi använder samma beteckningar som ovan. De två rötterna till $x^2 + px + q = 0$ är sålunda $x_1 = -\frac{p}{2} + \delta$ och $x_2 = -\frac{p}{2} - \delta$. Härav följer omedelbart

$$x_1 + x_2 = \left(-\frac{p}{2} + \delta\right) + \left(-\frac{p}{2} - \delta\right) = -p$$

och

$$\begin{aligned} x_1x_2 &= \left(-\frac{p}{2}+\delta\right)\left(-\frac{p}{2}-\delta\right) \\ &= \left(-\frac{p}{2}\right)^2-\delta^2=\left(\frac{p}{2}\right)^2-\Delta \\ &= \left(\frac{p}{2}\right)^2-\left(\left(\frac{p}{2}\right)^2-q\right)=q. \end{aligned}$$

De här två formlerna kallas *sambanden mellan rötter och koefficienter* (för en andragradsekvation; det finns analoga formler för ekvationer av högre grad). Vår härledning av dem är lite av fusk, i den meningen att vi har använt lösningsformeln; i själva verket är det "rätta" sättet att härleda dem det här: Enligt faktorsatsen är x^2+px+q delbart med $x-x_1$ och $x-x_2$, dvs

$$x^2+px+q=q(x)(x-x_1)(x-x_2)$$

för något polynom q. Om man betraktar graden på båda sidor så ser man genast att q är en konstant. Om man sedan tittar på högstagradskoefficienten (koefficienten för x^2), så ser man att $q(x)=1$ (jämför med avsnitt 1.3); alltså

$$x^2+px+q=(x-x_1)(x-x_2)=x^2-(x_1+x_2)x+x_1x_2.$$

Här kan man direkt avläsa sambanden genom att jämföra koefficienterna för x respektive de konstanta termerna. Den här härledningen kan lätt generaliseras til ekvationer av högre grad. Låt $p(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n$ vara ett polynom av grad n och $x_1,x_2,\ldots,x_n$ dess nollställen (eventuellt är en del av dem lika). Som nyss får vi

$$x^n+a_1x^{n-1}+\ldots+a_n=(x-x_1)(x-x_2)\ldots(x-x_n)$$

och multiplicerar vi ihop faktorerna i högerledet så ser vi att koefficienten för x^{n-1} är lika med $-(x_1+x_2+\ldots+x_n)$, så att

$$x_1+x_2+\ldots x_n=-a_1.$$

Genom att titta på koefficienterna för x^{n-2} på båda sidorna så får vi också

$$x_1x_2+x_1x_3+\ldots+x_{n-1}x_n=a_2$$

(vänsterledet är summan av alla dubbla produkter x_ix_j för $1\le i<j\le n$). Jämför vi de konstanta termerna så får vi

$$x_1x_2\ldots x_n=(-1)^na_n.$$

Det finns förstås analoga formler för summan av alla produkter av tre rötter $x_ix_jx_k$ osv, men de som man möjligen kan lägga på minnet är formlerna för rötternas summa och produkt. Lägg märke till att vi har härlett sambanden mellan rötter och koefficienter utan att bestämma rötterna x_i, dvs utan att lösa

ekvationen $p(x) = 0$. Sambanden kallas emellanåt även Viètes formler.[3] För tredjegradsekvationen $x^3 + a_1x^2 + a_2x + a_3 = 0$ ser sambanden utskrivna ut så här:

$$x_1 + x_2 + x_3 = -a_1 \tag{2.10}$$
$$x_1x_2 + x_1x_3 + x_2x_3 = a_2 \tag{2.11}$$
$$x_1x_2x_3 = -a_3. \tag{2.12}$$

Man kan leka med sambanden mellan rötter och koefficienter och göra en del häpnadsväckande akrobatiknummer.

Exempel: Låt $x_1, \ldots, x_4$ vara rötterna till ekvationen $x^4 - x^3 + 2x^2 + 5 = 0$. Bestäm summan av rötternas kvadrater, dvs $x_1^2 + x_2^2 + x_3^2 + x_4^2$. Här gäller det att ha lite fantasi och våga experimentera. Om vi utvecklar $(x_1 + x_2 + x_3 + x_4)^2$ så bör vi ju få summan av alla kvadrater plus en del "skräp":

$$(x_1 + x_2 + x_3 + x_4)^2 =$$
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4).$$

Enligt ovan är $x_1 + \ldots + x_4 = -(-1) = 1$ och $x_1x_2 + \ldots x_3x_4 = 2$, så resultatet är

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1^2 - 2 \cdot 2 = -3.$$

Av svaret kan vi för övrigt dra slutsatsen att inte alla rötter kan vara reella, för i så fall hade summan av deras kvadrater varit ≥ 0.

Exempel: Om rötterna till $x^n + a_1x^{n-1} + \ldots + a_n = 0$ är $x_1, \ldots, x_n$, så gäller att

$$x_1^2 + \ldots + x_n^2 = a_1^2 - 2a_2.$$

Beviset är detsamma som i det förra exemplet.

Exempel: Beräkna $\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$, där x_1, x_2, x_3 är rötterna till $x^3 - x - 1 = 0$. Vi kan ju först notera att ingen av rötterna är 0, så summan är definierad. Om vi gör liknämnigt så får vi

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{x_1x_2 + x_1x_3 + x_2x_3}{x_1x_2x_3} = \frac{-1}{-(-1)} = -1.$$

Exempel: Låt x_1, x_2, x_3 vara rötterna till $x^3 + 2x^2 - 6x + 3 = 0$. Bestäm den ekvation som har rötterna $x_1 + x_2, x_1 + x_3, x_2 + x_3$. På sätt och vis är det enkelt att lösa problemet, eftersom ekvationen är

$$(x - (x_1 + x_2))(x - (x_1 + x_3))(x - (x_2 + x_3)) = 0.$$

[3] François Viète (eller Vieta), spansk-fransk matematiker, 1540-1603.

Men utmaningen består i att explicit räkna ut koefficienterna i vänsterledet. Man får inte vara rädd att kasta sig ut i beräkningar, utan börja med att multiplicera ihop:

$$\begin{aligned} x^3 &- (x_1+x_2+x_1+x_3+x_2+x_3)x^2 \\ &+ ((x_1+x_2)(x_1+x_3))+(x_1+x_2)(x_2+x_3)+(x_1+x_3)(x_2+x_3))x \\ &- (x_1+x_2)(x_1+x_3)(x_2+x_3) \\ = x^3 &- 2(x_1+x_2+x_3)x^2 \\ &+ (x_1^2+x_2^2+x_3^2+3(x_1x_2+x_1x_3+x_2x_3))x \\ &- (x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2+2x_1x_2x_3) \end{aligned}$$

och det återstår nu att beräkna uttrycken inom parenteserna. Koefficienten för x^2 är $-2(-2)=4$ och koefficienten för x är

$$\begin{aligned} & x_1^2+x_2^2+x_3^2+2(x_1x_2+x_1x_3+x_2x_3)+(x_1x_2+x_1x_3+x_2x_3) \\ = \quad & (x_1+x_2+x_3)^2+(x_1x_2+x_1x_3+x_2x_3) = (-2)^2-6=-2. \end{aligned}$$

För att till sist räkna ut den konstanta termen provar vi med att multiplicera ihop $x_1+x_2+x_3$ och $x_1x_2+x_1x_3+x_2x_3$. Vi får produkten

$$x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2+3x_1x_2x_3$$

varför

$$\begin{aligned} & x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2+2x_1x_2x_3 \\ & = (x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)-x_1x_2x_3 \\ & = (-2)(-6)-(-3)=15. \end{aligned}$$

Den sökta ekvationen är således

$$x^3-4x^2-2x-15=0.$$

Att vi kunde bestämma ekvationen i det sista exemplet ser verkligen ut som en lycklig slump, men det är det inte riktigt. Det beror på att uttrycket

$$(x-(x_1+x_2))(x-(x_1+x_3))(x-(x_2+x_3))$$

är *symmetriskt* i x_1, x_2, x_3 (dvs man får samma sak om man permuterar dem). Ett polynom $f(x_1, x_2, \ldots, x_n)$ i n stycken variabler kallas *symmetriskt* om det inte ändras när man permuterar (kastar om) variablerna, dvs

$$f(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) = f(x_1, x_2, \ldots, x_n)$$

för alla permutationer $i_1, i_2, \ldots, i_n$ av $1, 2, \ldots, n$. Exempel på symmetriska polynom är summan $x_1+x_2+\ldots+x_n$ och produkten $x_1x_2\ldots x_n$. Mer allmänt

är alla koefficienterna i $(x-x_1)(x-x_2)\dots(x-x_n)$ symmetriska polynom i $x_1,\dots,x_n$: om vi multiplicerar ut så får vi

$$\begin{aligned}&(x-x_1)(x-x_2)\dots(x-x_n)\\ &= x^n - e_1(x_1,\dots,x_n)x^{n-1} + e_2(x_1,\dots,x_n)x^{n-2} + \dots + (-1)^n e_n(x_1,\dots,x_n)\end{aligned}$$

där $e_j(x_1,\dots,x_n)$ är vissa uttryck som är symmetriska polynom i $x_1,\dots,x_n$. De kallas *de elementära symmetriska polynomen* och dyker alltså upp i sambanden mellan rötter och koefficienter. En annan typ av symmetriska polynom är *potenssummorna*

$$p_k(x_1,\dots,x_n) = x_1^k + \dots + x_n^k$$

och i ett exempel nyss såg vi att t ex

$$p_2(x_1,\dots,x_n) = e_1(x_1,\dots,x_n)^2 - 2e_2(x_1,\dots,x_n).$$

En viktig sats i teorin för symmetriska polynom är att *varje symmetriskt polynom kan uttryckas med hjälp av de elementära symmetriska polynomen.* Koefficienterna i $(x-(x_1+x_2))(x-(x_1+x_3))(x-(x_2+x_3))$ är symmetriska polynom i x_1,x_2,x_3 och det är förklaringen till att vi kunde bestämma dem i exemplet nyss. Teorin för symmetriska polynom är mycket omfattande och innehåller många vackra resultat som har massor av tillämpningar både i och utanför matematiken.

Exempel: Som ett sista exempel skall vi än en gång lösa andragradsekvationen. Vi låter som vanligt x_1 och x_2 vara rötterna till ekvationen $x^2+px+q=0$. Då är $x_1+x_2=-p$ och $x_1x_2=q$. Vi skall beteckna uttrycket $(x_1-x_2)^2$ med D och noterar omedelbart att ekvationen har en dubbelrot ($x_1=x_2$) om och endast om $D=0$. Vi skall uttrycka D med hjälp av p och q:

$$\begin{aligned}D &= (x_1-x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2 = x_1^2 + 2x_1x_2 + x_2^2 - 4x_1x_2\\ &= (x_1+x_2)^2 - 4x_1x_2 = p^2 - 4q.\end{aligned}$$

(Att vi lyckades uttrycka D i p och q ser möjligen ut som ett litet under, men det följer ur det faktum att man kan uttrycka alla symmetriska polynom i rötterna x_1,x_2 i den elemtära symmetriska polynomen x_1+x_2 och x_1x_2, som ju är lika med $-p$ respektive q.) Låt d vara ett tal sådant att $d^2=D$. Då är $x_1-x_2=\pm d$ och vi kan anta att $x_1-x_2=d$ (eftersom det inte spelar någon som helst roll vilken av rötterna vi kallar x_1 respektive x_2). Vi har således ett litet ekvationssystem:

$$\begin{cases} x_1+x_2 &= -p\\ x_1-x_2 &= d.\end{cases}$$

Om vi adderar ekvationerna så får vi

$$2x_1 = -p+d \quad \text{dvs} \quad x_1 = -\frac{p}{2}+\frac{d}{2}$$

och subtraherar vi så får vi istället

$$x_2 = -\frac{p}{2}-\frac{d}{2}.$$

Låt oss betrakta fallet då p och q är reella tal. Då är förstås $D = p^2 - 4q$ också reellt. Om $D < 0$, så kan inte rötterna vara reella eftersom i så fall $D = (x_1 - x_2)^2$ vore ≥ 0. Om $D > 0$, så är talet d reellt och båda rötterna reella. Nu börjar kanske läsaren misstänka att D är besläktad med Δ som vi pratade om tidigare och det är förstås riktigt:

$$D = p^2 - 4q = 4\left(\frac{p^2}{4} - q\right) = 4\left(\left(\frac{p}{2}\right)^2 - q\right) = 4\Delta.$$

Formlerna för rötterna ovan är därför inget annat än vår gamla bekanta "p, q-formel". Det är för övrigt fullt berättigat att kalla formeln en gammal bekant, för den har i någon mening varit känd sedan det gamla Babylonien för ca 4000 år sedan. Talet D som tydligen bestämmer flera av ekvationens egenskaper kallas *diskriminanten* till ekvationen $x^2 + px + q = 0$. Ordet har att göra med latinets ord för att skilja åt eller särskilja, jämför med vårt ord diskriminera. Ofta kallas även Δ för diskriminant till ekvationen och då får sammanhanget avgöra vilket av de två talen man menar. Eftersom $D = 4\Delta$, så är $x^2 + px + q$ en kvadrat om och endast om $D = 0$ (Sats 16).

2.3.1 Övningar

1. Låt x_1 och x_2 vara de två rötterna till $x^2 + 5x + 12 = 0$. Bestäm den ekvation som har rötterna x_1^2 och x_2^2.
2. Låt x_1, x_2, x_3, x_4 vara de två rötterna till $x^4 + x^3 - 2x - 4 = 0$. Bestäm den ekvation som har rötterna $x_1^2, x_2^2, x_3^2, x_4^2$.
3. Låt x_1, x_2, x_3 vara rötterna till $x^3 - 3x - 1 = 0$. Bestäm den tredjegradsekvation som har rötterna x_1x_2, x_1x_3 och x_2x_3.
4. Bestäm $x_1^3 + x_2^3 + x_3^3$ då x_1, x_2, x_3 är som i den förra övningen.
5. Bestäm x_1, x_2 och x_3 om
$$\begin{cases} x_1^3 + x_2^3 + x_3^3 &= 8 \\ x_1^2 + x_2^2 + x_3^2 &= 6 \\ x_1 + x_2 + x_3 &= 2 \end{cases}$$
6. De rationella talen x_1, x_2 och x_3 är sådana att $x_1^j + x_2^j + x_3^j$ är heltal för $j = 1, 2, 3$. Bevisa att x_1, x_2 och x_3 är heltal.

2.4 Några speciella ekvationer

Vi har nu vridit och vänt på andragradsekvationer och kan väl anse att vi behärskar deras teori ganska väl. Det händer inte så sällan att man som lärare får frågan hur det är med ekvationer av högre grad; finns det t ex någon motsvarighet till p, q-formeln för tredjegradsekvationer? Vi skall prata om tredjegradsekvationen i det här avsnittet och härleda en sådan formel och i kommande avsnitt helt kort diskutera några andra speciella ekvationer.

2.4.1 Tredjegradsekvationen

En allmän tredjegradsekvation har utseendet $x^3 + ax^2 + bx + c = 0$, men vi skall börja analysen av den med att titta på den enklaste tänkbara, nämligen $x^3 = 1$ eller $x^3 - 1 = 0$. Man ser ju med ett halvt öga att $x = 1$ är en rot och vi kan faktorisera $x^3 - 1 = (x-1)(x^2 + x + 1)$. De återstående två rötterna får vi genom att lösa $x^2 + x + 1 = 0$. Diskriminanten är $(1/2)^2 - 1 = -3/4 < 0$, så båda rötterna är icke-reella. Kvadratkomplettera:

$$x^2 + x + 1 = x^2 + 2 \cdot \frac{1}{2}x + \left(\frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2 + 1 = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4}.$$

Alltså får vi $(x + 1/2)^2 = -3/4$ och $x = -1/2 \pm i\sqrt{3}/2$. Vi skall använda beteckningen

$$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Kontrollera själv att $\omega^2 = -1/2 - i\sqrt{3}/2$ och minns att $\omega^3 = 1$.[4] Betrakta nu ekvationen $x^3 = A$. Om α är *en* rot till den, så kan de andra två rötterna skrivas $\omega\alpha$ och $\omega^2\alpha$ eftersom

$$(\omega^j\alpha)^3 = (\omega^3)^j\alpha^3 = 1^j \cdot A = A$$

för $j = 1$ och 2.

Vi återgår till den allmänna ekvationen $x^3 + ax^2 + bx + c = 0$. I slutet av avsnitt 2.2.1 löste vi ekvationen $x^2 + px + q = 0$ genom att införa en ny variabel genom $x = t + \alpha$ och bestämma talet α på ett listigt sätt. Vi skall använda samma metod för att förenkla tredjegradsekvationen i ett första steg. Sätt alltså $x = t + \alpha$, där α är ett tal som skall bestämmas om ett ögonblick. Sätter vi in i ekvationen så får vi

$$\begin{aligned} x^3 + ax^2 + bx + c &= (t+\alpha)^3 + a(t+\alpha)^2 + b(t+\alpha) + c \\ &= t^3 + (3\alpha + a)t^2 + (3\alpha^2 + 2a\alpha + b)t \\ &+ (\alpha^3 + a\alpha^2 + b\alpha + c). \end{aligned}$$

Vi ser att om vi väljer α så att $3\alpha + a = 0$, så försvinner t^2-termen. Insättning av $\alpha = -a/3$ ger efter lite räknande

$$t^3 + \left(-\frac{a^2}{3} + b\right)t + \frac{2a^3}{27} - \frac{ab}{3} + c = 0.$$

Vi betecknar koefficienten för t med p och den konstanta termen med q, så att ekvationen blir $t^3 + px + q = 0$. Vi ser alltså att *det räcker att studera tredjegradsekvationer som saknar andragradsterm.*

[4] Bokstaven ω, omega, är den sista bokstaven i det grekiska alfabetet. Stort omega ser ut så här: Ω.

För att spara beteckningar återgår vi till den ursprungliga variabeln x och betraktar ekvationen $x^3+px+q=0$. Det finns flera mer eller mindre upplysande sätt att lösa den, men vi skall göra en systematisk analys med hjälp av sambanden mellan rötter och koefficienter. Vi börjar med att införa de s k *Lagrangeresolventerna*[5]

$$\begin{aligned} L_1 &= \frac{1}{3}(x_1+\omega x_2+\omega^2 x_3) \\ L_2 &= \frac{1}{3}(\omega x_1+x_2+\omega^2 x_3) \end{aligned}$$

och det första steget är att bestämma en andragradsekvation som har rötterna L_1^3 och L_2^3. Ekvationen är förstås

$$X^2-(L_1^3+L_2^3)X+L_1^3L_2^3=0,$$

så vi måste beräkna summan och produkten av L_1^3 och L_2^3. Här skall vi vara så listiga det bara går. Ekvationen $t^3-1=0$ har som vi såg rötterna $1,\omega,\omega^2$, så

$$t^3-1=(t-1)(t-\omega)(t-\omega^2).$$

Om vi byter t mot $-t$ så får vi

$$t^3+1=(t+1)(t+\omega)(t+\omega^2).$$

Sätter vi $t=L_1/L_2$ och multiplicerar med L_2^3 så ger detta

$$L_1^3+L_2^3=(L_1+L_2)(L_1+\omega L_2)(L_1+\omega^2 L_2).$$

Nu kan vi börja räkna och i bakhuvudet har vi dels att enligt sambanden mellan rötter och koefficienter är $x_1+x_2+x_3=0$ (koefficienten för x^2 är ju 0), dels att $1+\omega+\omega^2=0$:

$$\begin{aligned} L_1+L_2 &= \frac{1}{3}((1+\omega)x_1+(1+\omega)x_2+2\omega^2 x_3) \\ &= \frac{1}{3}(-\omega^2 x_1-\omega^2 x_2+2\omega^2 x_3) \\ &= \frac{1}{3}\omega^2(2x_3-x_1-x_2)=\omega^2 x_3. \end{aligned}$$

På exakt samma sätt får vi

$$L_1+\omega L_2=\omega x_2 \quad \text{och} \quad L_1+\omega^2 L_2=x_1.$$

Alltså är

$$L_1^3+L_2^3=\omega^3 x_1x_2x_3=-q,$$

[5]Joseph Louis Lagrange, italiensk-fransk matematiker, 1736-1813.

där vi ytterligare en gång har använt sambanden mellan rötter och koefficienter för $x^3 + px + q = 0$ och att $\omega^3 = 1$. Vi fortsätter:

$$\begin{aligned} 3L_1 \cdot 3L_2 &= (x_1 + \omega x_2 + \omega^2 x_3)(\omega x_1 + x_2 + \omega^2 x_3) \\ &= \omega(x_1^2 + x_2^2 + x_3^2) + (1 + \omega^2)(x_1x_2 + x_1x_3 + x_2x_3) \\ &= \omega((x_1 + x_2 + x_3)^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)) \\ &= \omega \cdot (-3)p, \end{aligned}$$

alltså

$$L_1L_2 = -\frac{1}{3}\omega p \quad \text{och} \quad L_1^3L_2^3 = -\frac{p^3}{27}.$$

Talen L_1^3 och L_2^3 är således rötterna till *resolventekvationen*

$$X^2 + qX - \frac{p^3}{27} = 0.$$

Kvadratkomplettering ger

$$\left(X + \frac{q}{2}\right)^2 = \frac{p^3}{27} + \frac{q^2}{4} = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 = \Delta.$$

Nu skall vi missbruka kvadratrotstecknet lite och skriver rötterna som

$$L_1^3 = -\frac{q}{2} + \sqrt{\Delta}, \quad L_2^3 = -\frac{q}{2} - \sqrt{\Delta}.$$

Om vi missbrukar även kubikrotstecknet och låter

$$L_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}}$$

beteckna en av kubikrötterna ur $-q/2 + \sqrt{\Delta}$, så är L_2 bestämd av sambandet $L_1L_2 = -\omega p/3$, som vi härledde ovan. Vi får nu

$$\begin{aligned} x_1 &= L_1 + \omega^2 L_2 = L_1 + \omega^2\left(-\frac{\omega p}{3L_1}\right) = L_1 - \frac{p}{3L_1} \\ &= \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}. \end{aligned}$$

De andra rötterna blir

$$\begin{aligned} x_2 &= \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}} \\ x_3 &= \omega\sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}. \end{aligned}$$

De fantastiska rotuttrycken kallas *Cardanos formler*, se vidare nedan för deras historia och bakgrund.

Exempel: Lös ekvationen $x^3 + 12x - 12 = 0$. Här är $p = 12, q = -12$ så att

$$\Delta = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 = 4^3 + (-6)^2 = 100.$$

En rot är

$$x_1 = \sqrt[3]{6 + 10} + \sqrt[3]{6 - 10} = \sqrt[3]{16} - \sqrt[3]{4}$$

och de andra två rötterna är

$$\begin{aligned} x_2 &= \omega\sqrt[3]{16} - \omega^2\sqrt[3]{4} \\ x_3 &= \omega^2\sqrt[3]{16} - \omega\sqrt[3]{4}. \end{aligned}$$

Exempel: Lös ekvationen $x^3 + x + 1 = 0$. Här blir

$$\Delta = \left(\frac{1}{3}\right)^3 + \left(\frac{1}{2}\right)^2 = \frac{31}{108}$$

och en rot är således

$$x = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{31}{108}}} + \sqrt[3]{-\frac{1}{2} - \sqrt{\frac{31}{108}}} = \frac{1}{6}\left(\sqrt[3]{12(\sqrt{93} - 9)} - \sqrt[3]{12(\sqrt{93} + 9)}\right).$$

Exempel: Lös ekvationen $x^3 - 15x - 4 = 0$. Här är $\Delta = (-15/3)^3 + (-4/2)^2 = -121$, så en rot är

$$x = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}$$

vilket kanske inte är så mycket att säga om. Men nu är det så att $2 \pm 11i = (2 \pm i)^3$ och då får man

$$x = (2 + i) + (2 - i) = 4,$$

vilken man eventuellt hade kunnat se direkt är en rot. En lite märklig sak, som vi inte har möjlighet att bevisa, är att det finns inget sätt att förenkla uttrycket för x till 4 om man inte genom intuition (?) kommer på att $(2 + i)^3 = 2 + 11i$. Ekvationen i det här exemplet förekommer i en lärobok i algebra av Raffael Bombelli från 1572.

Till sist skall vi säga några ord om diskriminanten till en tredjegradsekvation $x^3 + px + q = 0$. Den definieras som uttrycket

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2,$$

där x_1, x_2, x_3 som förut är ekvationens tre rötter (jämför detta med definitionen av diskriminant till en andragradsekvation). Man ser genast att $D = 0$ om och endast om ekvationen har en dubbelrot, men det har man förstås ingen glädje av om man inte kan räkna ut D på något annat sätt än att först bestämma rötterna. Låt oss utgå från uttrycken

$$\begin{aligned} x_1 &= L_1 + \omega^2 L_2 \\ x_2 &= \omega^2 L_1 + L_2 \\ x_3 &= \omega L_1 + \omega L_2. \end{aligned}$$

Vi får genast

$$\begin{aligned} x_1 - x_2 &= (1-\omega^2)(L_1 - L_2) \\ x_1 - x_3 &= (1-\omega)(L_1 - \omega L_2) \\ x_2 - x_3 &= (\omega^2 - \omega)(L_1 - \omega^2 L_2). \end{aligned}$$

Alltså blir

$$\begin{aligned} &(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\ &= -\omega(1-\omega)^2(1-\omega^2)(L_1 - L_2)(L_1 - \omega L_2)(L_1 - \omega^2 L_2). \end{aligned}$$

Produkten

$$(L_1 - L_2)(L_1 - \omega L_2)(L_1 - \omega^2 L_2) = L_1^3 - L_2^3,$$

vilket följer ur likheten $t^3 - 1 = (t-1)(t-\omega)(t-\omega^2)$ på samma sätt som ovan. Kvadraten på detta är alltså $(L_1^3 - L_2^3)^2$, som inte är något annat än *diskriminanten* till resolventekvationen $X^2 + qX - p^3/27 = 0$, dvs $q^2 + 4p^3/27$. Det återstår att beräkna uttrycket med alla ω:

$$\begin{aligned} (-\omega)^2(1-\omega)^4(1-\omega^2)^2 &= \omega^2(1-\omega)^6(1+\omega)^2 = \omega^6(1-2\omega+\omega^2)^3 \\ &= (-3\omega)^3 = -27 \end{aligned}$$

(här har vi använt identiteten $1+\omega+\omega^2 = 0$ flera gånger, men inte det explicita uttrycket $\omega = (-1+i\sqrt{3})/2$). Slutligen får vi

$$D = -27(q^2 + 4p^3/27) = -27q^2 - 4p^3 = -108\left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right) = -108\Delta.$$

Reella ekvationer och casus irreducibilis

Tredjegradsekvationer med reella koefficienter och reella rötter är särskilt intressanta, inte minst av historiska skäl, och vi skall studera dem ett ögonblick. Om p och q är reella så finns det två möjligheter: antingen är alla tre rötterna reella eller så är en av dem x_1 reell och de andra två x_2 och x_3 konjugerade komplexa tal. I det första fallet är förstås $D > 0$ (vi antar att rötterna är enkla, så att $D \neq 0$). I det andra fallet skriver vi $x_2 = \alpha + i\beta$, $x_3 = \alpha - i\beta$. Då är $x_2 - x_3 = 2i\beta$ och alltså $(x_2 - x_3)^2 = -4\beta^2$. Vidare är

$$(x_1 - x_2)(x_1 - x_3) = (x_1 - x_2)(x_1 - \bar{x}_2) = |x_1 - x_2|^2,$$

så att

$$D = -4|x_1 - x_2|^4\beta^2 < 0.$$

Sammanfattningsvis gäller således att $D > 0$ *om och endast om alla tre rötterna är reella.*

Eftersom $D > 0$ så är $\Delta < 0$ och vi sätter $\Delta' = -\Delta$. Cardanos formler för en av rötterna får utseendet

$$x_1 = \sqrt[3]{-\frac{q}{2} + i\sqrt{\Delta'}} + \sqrt[3]{-\frac{q}{2} - i\sqrt{\Delta'}}.$$

Vi behöver nu den polära formen av komplexa tal. Skriver vi

$$-\frac{q}{2}+i\sqrt{\Delta'}=re^{i\phi}$$

så blir

$$r^2=\left|-\frac{q}{2}+i\sqrt{\Delta'}\right|^2=\left(\frac{q}{2}\right)^2+\Delta'=\left(\frac{q}{2}\right)^2-\Delta=\left(\frac{q}{2}\right)^2-\left(\frac{q}{2}\right)^2-\left(\frac{p}{3}\right)^3=-\left(\frac{p}{3}\right)^3.$$

(Här bör man observera att eftersom $\Delta=(q/2)^2+(p/3)^3<0$, så är $p<0$.) Vinkeln ϕ får man som argumentet till $-q/2+i\sqrt{\Delta'}$ och vi får

$$\sqrt[3]{-\frac{q}{2}+i\sqrt{\Delta'}}=\sqrt{-\frac{p}{3}}\,e^{i\phi/3+2ni\pi/3}.$$

Vi får alla tre rötterna på en gång:

$$\begin{aligned}x_1&=2\sqrt{-\frac{p}{3}}\cos\frac{\phi}{3}\\ x_2&=2\sqrt{-\frac{p}{3}}\cos\left(\frac{\phi}{3}+\frac{2\pi}{3}\right)\\ x_3&=2\sqrt{-\frac{p}{3}}\cos\left(\frac{\phi}{3}+\frac{4\pi}{3}\right).\end{aligned}$$

Exempel: Vi skall lösa $x^3-9x+9=0$, för vilken

$$\Delta=\left(\frac{9}{2}\right)^2+\left(-\frac{9}{3}\right)^3=-\frac{27}{4}$$

och vi skall bestämma r och ϕ så att

$$-\frac{9}{2}+i\sqrt{\frac{27}{4}}=re^{i\phi}.$$

Vi får $r=\sqrt{27}$ och

$$\tan(\pi-\phi)=\frac{\sqrt{27/4}}{9/2}=\frac{1}{\sqrt{3}},$$

varav $\phi=5\pi/6$. Rötterna blir

$$\begin{aligned}x_1&=2\sqrt{3}\cos\frac{5\pi}{18}\\ x_2&=2\sqrt{3}\cos\left(\frac{5\pi}{18}+\frac{2\pi}{3}\right)=-2\sqrt{3}\cos\frac{\pi}{18}\\ x_3&=2\sqrt{3}\cos\left(\frac{5\pi}{18}+\frac{4\pi}{3}\right)=2\sqrt{3}\cos\frac{7\pi}{18}.\end{aligned}$$

Det historiskt och matematiskt intressanta med casus irreducibilis är att det *trots att rötterna är reella så förekommer det komplexa tal i Cardanos formler.* Det var i det här sammanhanget som matematikerna på allvar började fundera över de komplexa talen. I skolan och på universitetet börjar man studera komplexa tal när man kommer till andragradsekvationen $x^2 + 1 = 0$, men så var det inte historiskt. Andragradsekvationer med komplexa rötter betraktades som absurda och ointressanta och dem struntade man helt enkelt i. Men i samband med casus irreducibilis blev man helt enkelt tvungen att ta komplexa tal på allvar, men det var inte lätt och först under 1800-talet började man känna sig trygg vid att räkna med dem.

Vi slutar det här avsnittet med en pedagogisk reflektion. I lösningen av tredjegradsekvationen gjorde vi en hel mängd listiga saker, som t ex att införa Lagrangeresolventerna. När man som lärare gör sådant i en föreläsning, så får man emellanåt frågan "Hur skall man komma på det?", ofta i ett uppgivet röstläge. Svaret i just det här fallet är att det skall man inte. Lösningen av tredjegradsekvationen är 500 år gammal och har naturligtvis finslipats och strömlinjeformats genom seklerna. Den eller de som löste ekvationen första gången slet mycket med att komma på hur man skulle göra. Likadant är det med väldigt mycket av den matematik man undervisar om både i skola och på universitet. Stoffet är i allmänhet flera hundra eller tusen år gammalt och som student får man ingen känsla för hur svårt det var när det tillkom en gång i tiden, eftersom det har bearbetats och förenklats många gånger på vägen. Det här är utan tvekan ett av matematikdidaktikens stora problem.

2.4.2 Fjärdegradsekvationen

Det finns en liknande teori för fjärdegradsekvationen som den vi just har utarbetat för tredjegradsekvationen, men jag tror att läsaren kommer att känna sig nöjd med ett enda exempel istället för en fullständig härledning av en lösningsformel. En allmän ekvation har formen $x^4 + ax^3 + bx^2 + cx + d = 0$ och genom att använda samma knep som ovan kan vi förvandla den till en ekvation utan x^3-term, alltså $x^4 + px^2 + qx + r = 0$.

Låt oss betrakta ekvationen $x^4 = 6x^2 + 8x + 1$. Det avgörande tricket nu är att införa ytterligare en variabel y och utveckla $(x^2 + y)^2$:

$$\begin{aligned}(x^2+y)^2 &= x^4 + 2x^2y + y^2 = 6x^2 + 8x + 1 + 2x^2y + y^2\\ &= (2y+6)x^2 + 8x + (y^2+1)\\ &= (2y+6)\left(x^2 + \frac{8}{2y+6}\cdot x + \frac{y^2+1}{2y+6}\right).\end{aligned}$$

Anledningen till att detta mystiska räknande är att *vi kan välja y hur som helst och speciellt så att högerledet är en kvadrat.* Villkoret för att $x^2 + 8x/(2y+6) + (y^2+1)/(2y+6)$ skall vara en kvadrat finns i Sats 16 och det är att diskriminanten

är 0, dvs

$$\left(\frac{4}{2y+6}\right)^2 - \frac{y^2+1}{2y+6} = 0.$$

Vi förenklar:

$$16 - (y^2+1)(2y+6) = 0 \quad \text{eller} \quad y^3 + 3y^2 + y - 5 = 0.$$

Den här tredjegradsekvationen kan vi lösa med metoden i det förra avsnittet, men man ser ganska lätt att en rot är $y = 1$ och insättning av detta ger

$$(x^2+1)^2 = 8x^2 + 8x + 2 = 2(4x^2 + 4x + 1) = 2(2x+1)^2$$

så om vi drar kvadatroten ur båda leden får vi två *andragradsekvationer*

$$\begin{aligned} x^2 &= \sqrt{2}(2x+1) \\ x^2 &= -\sqrt{2}(2x+1). \end{aligned}$$

Läsaren får nu i uppgift att lösa dessa och därmed för första gången (?) lösa en fjärdegradsekvationen.

2.4.3 Ekvationer av högre grad och kortkort historik

Andragradsekvationer kunde som sagt redan de gamla babylonierna lösa för 4000 år sedan, även om de naturligtvis inte skrev som vi. Då de inte accepterade negativa tal så var de inte intresserade av ekvationer med negativa rötter, men för övrigt var deras lösning densamma som vår moderna. Att de inte arbetade med negativa tal ledde dessutom till att de var tvungna att behandla ekvationerna $x^2+10x-4 = 0$ och $x^2-10x+4 = 0$ som två helt olika problem, nämligen som $x^2+10x = 4$ respektive $x^2+4 = 10x$. Grekerna (ca 500-300 f Kr) löste också andragradsekvationer, men de gjorde det helt geometriskt. Efter antiken vidareutvecklades det grekiska arvet av arabiska matematiker, medan matematiken i Västeuropa i stort sett låg i träda fram till senmedeltiden och renässansen. Ofta säger man att det första stora framsteget efter den grekiska tiden var lösningen av tredjegradsekvationen, vilket gjordes i Italien i slutet av 1400-talet (vissa tredjegradsekvationer kunde man lösa tidigare och det fanns även geometriska metoder). Den förste som löste den fullständigt var förmodligen Scipione del Ferro (ca 1465-1526), men han publicerade aldrig sin upptäckt. Han berättade om den för sin student Fior (enligt legenden gjorde han det på sin dödsbädd), som försökte använda den som ett redskap i de offentliga dueller i ekvationslösning som förekom vid den här tiden. En av Fiors motståndare var Niccolo Fontana (ca 1500-1557), kallad Tartaglia (”den stammande”), och han hörde ryktesvägen att Fior hade lösningen till tredjegradsekvationen. Tartaglia kunde rekonstruera den på egen hand och gjorde med hjälp av sin formel stor succé i tävlingarna. Här tätnar intrigen och in kommer Gerolamo (Hieronymus) Cardano (1501-1576) från Milano. Cardano var en riktig renässansmänniska som sysslade med teknik, ingenjörskonst, medicin, astrologi, matematik mm. Hans namn lever

kvar bl a i orden kardanknut och kardanupphängning. Genom en list som skulle platsa i vilken tv-såpa som helst lyckades han locka Tartaglia att avslöja sin formeln för tredjegradsekvationens rötter, men var samtidigt tvungen att svära en ed att aldrig publicera den, vilket var synd eftersom han gärna ville ha sitt namn inskrivet i matematikhistorien. Cardano hade en utomordentligt begåvad student, Ludovico Ferrari (1522-1565), som lyckades lösa fjärdegradsekvationen med den metod vi använde ovan, men som vi noterade dyker det upp en tredjegradsekvation på vägen. Den olycksaliga eden tycktes alltså sätta stopp även för publiceringen av lösningen av fjärdegradsekvationen. I det här prekära läget fick Ferrari en briljant idé, nämligen att försöka leta fram del Ferros gamla lösning och publicera den istället för Tartaglias och på det sättet kringgå eden. Detta lyckades och Cardano publicerade lösningen i en bok med titeln *Ars magna*, Den stora konsten, år 1545. Tartaglia blev naturligtvis fullständigt rasande, men hade ingen framgång med sina protester, utan försvann ut ur historien. Historien är ju full av ironier och en av dem är att formlerna för tredjegradsekvationens rötter kallas Cardanos formler.

Hur är det då med ekvationer av högre grad? Finns det formler (i så fall gissningsvis enormt invecklade) för deras rötter också? Det dröjde ända till 1824 innan svaret på den frågan kom och det är "nej" i allmänhet. Det finns inga formler liknande Cardanos och Ferraris för tredje- respektive fjärdegradsekvationens rötter för allmänna ekvationer av grad fem och högre. Med "formler" menas här uttryck för rötterna som bara innehåller ekvationens koefficienter, de vanliga aritmetiska operationerna samt rotutdragningar. Den som visade det här var en av matematikhistoriens absolut största begåvningar, nämligen den unge norrmannen Niels Henrik Abel (1802-1829). Det finns formler för vissa speciella (typer av) ekvationer, men alltså inga allmänna. Man skall inte förväxla detta med att ekvationer av högre grad har rötter; det har de alltid enligt algebrans fundamentalsats, men för det mesta kan man inte hitta dem med hjälp av en enkel formel. Den moderna algebran har en av sina rötter i Abels bevis. En annan person som skall nämnas i det här sammanhanget är fransmannen Evariste Galois (1811-1832), också ett romantiskt geni,[6] som hittade på ett nytt sätt att se på ekvationer. Tyvärr kan vi inte gå in på hans idéer här, de hör hemma i en högre kurs i algebra.

2.4.4 Ytterligare ett exempel

Vi skall diskutera ytterligare en intressant ekvation. En typ som faktiskt *kan* lösas med rotutdragningar, dvs med en "formel" av Cardano-Ferrarityp, är den av formen

$$x^n - 1 = 0.$$

Vi har inte de verktyg som behövs för att bevisa att den kan lösas med rotutdragningar, utan skall istället titta på några specialfall. Eftersom $x = 1$ är en

[6] Abel dog av lungtuberkulos, Galois i en duell.

trivial rot, så dividerar man oftast med $x-1$ och får då

$$x^{n-1}+x^{n-2}+\ldots+x^2+x+1=0.$$

För $n=3$ lyder den $x^2+x+1=0$ och den har vi redan löst; rötterna är $\omega=-1/2+i\sqrt{3}/2$ och $\omega^2=-1/2-i\sqrt{3}/2$ ovan. För $n=4$ får vi $x^4=1$ med rötter $\pm 1,\pm i$. För $n=5$ får vi

$$x^4+x^3+x^2+x+1=0,$$

vilken är intressant så det förslår och vi skall lösa den lite senare.

Vi skall nu analysera $x^n=1$ geometriskt och här behöver man känna till den polära formen för komplexa tal. Tar vi absolutbeloppet av båda leden så får vi $|x|^n=|1|=1$, dvs $|x|=1$. Alla rötter har tydligen absolutbelopp 1, vilket är ett annat sätt att säga att de ligger på enhetscirkeln (cirkeln med radie 1 och medelpunkt i 0 i det komplexa talplanet). En punkt på enhetscirkeln kan vi skriva på formen $x=\cos\phi+i\sin\phi$, där ϕ är x:s argument (den grekiska bokstaven fi, som motsvarar vårt f). Enligt de Moivres formel är $x^n=\cos(n\phi)+i\sin(n\phi)$ och vi får ekvationen $\cos(n\phi)+i\sin(n\phi)=1$, varav $\cos(n\phi)=1$, $\sin(n\phi)=0$. Detta ger $n\phi=k\cdot 2\pi$ för något heltal k (positivt eller negativt). Sätt $\phi_k=2k\pi/n$ och $x_k=\cos\phi_k+i\sin\phi_k$; då är x_k lösningar till $x^n=1$ för alla heltal k. Här kanske man blir orolig och undrar om ekvationen $x^n=1$ som har grad n har oändligt många lösningar, men det behöver man inte bli, för man kontrollerar lätt att $x_{k+l\cdot n}=x_k$ för alla multipler $l\cdot n$ av n, ty $\phi_{k+ln}=2(k+ln)\pi/n=2k\pi/n+2l\pi$, så de två vinklarna ϕ_k och ϕ_{k+ln} motsvarar *samma* punkt på enhetscirkeln. Det är därför bara $k=0,1,\ldots,n-1$ som ger olika punkter och därmed olika rötter till $x^n=1$. Rötterna kan sammanfattningsvis skrivas

$$x_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},\quad \text{där}\quad k=0,1,\ldots,n-1.$$

Vinkeln mellan två på varandra följande x_k är alltid lika med $2\pi/n$, vilket betyder att x_k:na är hörnen i en regelbunden n-hörning i det komplexa talplanet.

Exempel: Nu är vi redo att ta itu med $x^5=1$ eller $x^4+x^3+x^2+x+1=0$ om vi dividerar bort roten $x=1$. Sätt $\epsilon=e^{2\pi i/5}$; då är rötterna lika med ϵ^k för $k=1,2,3,4$. Vi skall lösa ekvationen genom ett systematiskt användande av sambanden mellan rötter och koefficienter. Det första vi lägger märke till är att

$$\epsilon^4+\epsilon^3+\epsilon^2+\epsilon=-1.$$

Sätt nu $\eta_1=\epsilon+\epsilon^4$ och $\eta_2=\epsilon^2+\epsilon^3$.[7] Då är tydligen

$$\eta_1+\eta_2=\epsilon^4+\epsilon^3+\epsilon^2+\epsilon=-1.$$

Vidare blir

$$\eta_1\eta_2=(\epsilon+\epsilon^4)(\epsilon^2+\epsilon^3)=\epsilon^3+\epsilon^4+\epsilon^6+\epsilon^7=\epsilon^3+\epsilon^4+\epsilon+\epsilon^2=-1$$

[7] ϵ och η är de grekiska bokstäverna epsilon respektive eta.

eftersom $\epsilon^5 = 1$. Det följer att η_1 och η_2 är rötterna till ekvationen

$$X^2 - (-1)X + (-1) = X^2 + X - 1 = 0.$$

Dessa är

$$\frac{-1 \pm \sqrt{5}}{2}.$$

Frågan är nu vilken som är vilken av dessa. Men

$$\begin{aligned}
\eta_1 &= \epsilon + \epsilon^4 \\
&= \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} + \cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5} \\
&= \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} + \cos\left(2\pi - \frac{2\pi}{5}\right) + i\sin\left(2\pi - \frac{2\pi}{5}\right) \\
&= \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} + \cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5} \\
&= 2\cos\frac{2\pi}{5} > 0,
\end{aligned}$$

så vi har

$$\eta_1 = \frac{\sqrt{5}-1}{2}, \quad \eta_2 = -\frac{\sqrt{5}+1}{2}.$$

För att bestämma ϵ använder vi att $\epsilon^4 = \epsilon^{-1}$ och får ekvationen

$$\epsilon + \frac{1}{\epsilon} = \eta_1 = \frac{\sqrt{5}-1}{2}.$$

Alltså

$$\epsilon^2 - \eta_1\epsilon + 1 = 0,$$

varav

$$\left(\epsilon - \frac{\sqrt{5}-1}{4}\right)^2 = \left(\frac{\sqrt{5}-1}{4}\right)^2 - 1 = \frac{-10-2\sqrt{5}}{16}$$

och

$$\epsilon = \frac{\sqrt{5}-1}{4} \pm i\frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Imaginärdelen av ϵ är $\sin(2\pi/5) > 0$, så vi har till slut

$$\epsilon = \frac{\sqrt{5}-1}{4} + i\frac{\sqrt{10+2\sqrt{5}}}{4},$$

vilket i sin tur innebär att

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}, \quad \sin\frac{2\pi}{5} = \frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Att konstruera regelbundna månghörningar[8] (polygoner) med passare och linjal var något som redan de grekiska geometrikerna höll på med. Det är lätt att konstruera en liksidig triangel ($n = 3$), en kvadrat ($n = 4$) och en regelbunden sexhörning och i Euklides Elementa från ca 300 f Kr finns en mycket elegant konstruktion av den regelbundna femhörningen. Det är klart (varför?) att om man kan konstruera en regebunden n-hörning, så kan man konstruera även $2n$-hörningen och genom upprepning $2^m n$-hörningen. Euklides visade också att om man kan konstruera polygoner med n och m hörn, där n och m är relativt prima, så kan man konstruera även en regelbunden nm-hörning (Euklides diskuterade $n = 3, m = 5$). Alltså kan vi konstruera regelbundna polygoner med 3, 4, 5, 6, 8, 10, 12, 15, 16,. . .-hörningar, men det är några tal som fattas. Hur är det t ex med sjuhörningar och niohörningar? Svaret på den frågan dröjde mer än 2000 år efter den grekiska antiken och gavs först i början av 1800-talet. Det är kanske inte så förvånande att teorin för konstruktion av regelbundna polygoner är nära hopkopplad med den algebraiska teorin för ekvationerna $x^n = 1$. Vi skall inte alls diskutera några detaljer eller något bevis, utan bara skriva ner själva resultatet. Först en definition. Ett tal av formen $F_m = 2^{2^m} + 1$ kallas ett *Fermat-tal*[9] Här är $m = 0, 1, 2, \ldots$. Sviten av Fermattal börjar

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257, F_4 = 65537,\ F_5 = 4294967297.$$

Fermat var road av primtal och försökte hitta en formel som producerar primtal. Han formulerade som en ganska vild gissning att alla talen F_m är primtal. De första fem är verkligen det, men $F_5 = 641 \cdot 6700417$ är inget primtal. Trots mycket letande och räknande har man inte hittat något mer *Fermat-primtal*, men det är fortfarande ett öppet problem huruvida det finns några andra eller ej. Men vad har då det här med konstruktion av regelbundna polygoner att göra? Jo, en hel del:

Sats 17 (Gauss-Wantzel) *En regelbunden n-hörning kan konstrueras med passare och linjal om och endast om n har formen $n = 2^k \cdot p_1 \cdot \ldots \cdot p_l$, där p_i:na är olika Fermat-primtal.*

Läsaren måste hålla med om att det här är elegant! Eftersom 3 är ett Fermatprimtal, så är en regelbunden trehörning (dvs en liksidig triangel) konstruerbar (vilket vi förstås visste sedan tidigare). På samma sätt ser vi att även 5-, 17-, 257- och 65537-hörningarna är konstruerbara, liksom 15-hörningen eftersom $15 = 3 \cdot 5$ är en produkt av olika Fermatprimtal. Däremot har 7 inte den rätta formen (det är ett primtal, men inte ett Fermatprimtal), så en regelbunden sjuhörning är inte konstruerbar. Visserligen är $9 = 3 \cdot 3$ en produkt av Fermatprimtal, men inte av *olika* Fermatprimtal, så en niohörning är inte konstruerbar. Gauss konstruerade själv den regelbundna 17-hörningen och även 257- och 65537-hörningarna har studerats ingående, se t ex *The simple and straightforward construction of the 257-gon* av Christian Gottlieb i The Mathematical Intelligencer **21** (1999), no.

[8] En polygon säges vara regelbunden om alla sidor är lika långa och alla vinklar lika stora.
[9] Pierre de Fermat, fransk jurist och matematiker, 1601-1665.

1, 31-37. Vi sade ovan att ekvationerna $x^n = 1$ kan lösas med rotutdragningar och det direkta sambandet med konstruktionen av regelbundna polygoner är att den regelbundna n-hörningen är konstruerbar om och endast om rötterna till ekvationen $x^n = 1$ kan uttryckas med hjälp av enbart kvadratrötter (dvs inga kubikrötter eller högre).

2.4.5 Övningar

1. Lös ekvationen $x^3 + 12x + 12 = 0$.
2. Lös ekvationen $x^3 - 6x - 6 = 0$.
3. Lös ekvationen $x^3 - 3x^2 - 6x - 4 = 0$.
4. Lös ekvationen $x^3 - 3x - 1 = 0$.
5. Lös ekvationen $x^4 - 7x^2 + 2x + 2 = 0$.
6. Lös ekvationen $x^7 = 1$ och uttryck rötterna med hjälp av rotutdragningar. Ledning: Börja med att dividera bort roten $x = 1$ och sätt sedan $t = x + 1/x$. Härled en tredjegradsekvation för t och lös den med Cardanos formler.

2.5 Ekvationer med rationella rötter

Det finns ett systematiskt sätt att bestämma eventuella rationella rötter till polynom med heltalskoefficienter. Metoden bygger på delbarhetsteorin för heltal och vi beskriver den i form av ett exempel.

Exempel: Avgör huruvida ekvationen $2x^3 - 5x^2 + 7x + 5 = 0$ har några rationella rötter och bestäm i så fall dessa. Idén är att ansätta en rationell rot p/q, där p och q är heltal och där vi har förkortat så långt som möjligt (så att $SGD(p, q) = 1$). Alltså har vi

$$2\left(\frac{p}{q}\right)^3 - 5\left(\frac{p}{q}\right)^2 + 7\left(\frac{p}{q}\right) + 5 = 0.$$

Vi multiplicerar med q^3 för att bli av med nämnarna:

$$2p^3 - 5p^2q + 7pq^2 + 5q^3 = 0$$

Flytta över alla termer som innehåller (minst) en faktor q till högerledet:

$$2p^3 = 5p^2q - 7pq^2 - 5q^3.$$

Alla termer i högerledet innehåller nu en faktor q som vi bryter ut:

$$2p^3 = q(5p^2 - 7pq - 5q^2).$$

Minns nu att p och q är heltal. I högerledet står då en produkt av två heltal, nämligen q och $5p^2 - 7pq - 5q^2$, vilket betyder att vänsterledet $2p^3$ är delbart med q, i symboler

$$q|2p^3.$$

Nu finns det en sats i delbarhetsteorin för heltal som säger att om a och b är två relativt prima heltal (dvs $SGD(a,b) = 1$) och a delar en produkt bc, så måste a dela c (talteorins motsvarighet till Sats 7 ovan). Eftersom $q|2p^3 = 2p^2 \cdot p$ och $SGD(p,q) = 1$, så måste $q|2p^2$ och fortsätter vi så, så får vi $q|2$.[10] De enda heltal som delar 2 är ± 1 och ± 2, så det finns bara fyra möjligheter för q. Lägg således på minnet att man måste ta med alla möjliga delare till 2, inte bara de positiva.

För att ta reda på vilka möjligheter det finns för täljaren p så går vi tillbaka till $2p^3 - 5p^2q + 7pq^2 + 5q^3 = 0$ men flyttar nu över alla termer som innehåller en faktor p till högerledet: $5q^3 = -2p^3 + 5p^2q - 7pq^2 = p(-2p^2 + 5pq - 7q^2)$. Härav följer på precis samma sätt som nyss att $p|5q^3$ och sedan att $p|5$. Alltså måste p vara något av talen ± 1 och ± 5.

De möjliga rationella rötterna är således

$$\frac{1}{1}, \frac{1}{-1}, \frac{1}{2}, \frac{1}{-2}, \frac{-1}{1}, \frac{-1}{-1}, \frac{-1}{2}, \frac{-1}{-2}, \frac{5}{1}, \frac{5}{-1}, \frac{5}{2}, \frac{5}{-2}, \frac{-5}{1}, \frac{-5}{-1}, \frac{-5}{2}, \frac{-5}{-2}.$$

(Man kan kontrollräkna; antalet möjligheter är fyra för p och fyra för q, alltså $4 \cdot 4 = 16$ sammantaget.) Kom ihåg att vi ännu så länge *inte* har bevisat att ekvationen har några rationella rötter. Vi har bara bevisat att *om* den har en rationell rot, *så måste* den vara några av talen ovan. För att avgöra om det finns några rationella rötter, så måste vi *testa alla möjligheter*. Prövning visar att $-1/2$ faktiskt är en rot. Det kan bli ganska mycket räknande när man skall testa rötter, men emellanåt kan man genom ett eller annat knep reducera antalet tal att prova. Några av talen i uppräkningen är lika och man kan börja med att stryka uprepningar. När man testar kan man dessutom tänka på t ex att ett polynom med positiva koefficienter inte kan ha några positiva nollställen.

Vi har nu sett att $-1/2$ är en rot till $f(x) = 2x^3 - 5x^2 + 7x + 5 = 0$. Det betyder enligt faktorsatsen att $f(x)$ är delbart med $x - (-1/2) = x + 1/2$. Det går utmärkt att dividera bort den här faktorn ur f, men räkningarna blir lite enklare om man multiplicerar med 2 och noterar att $2x + 1 = 2(x + 1/2)$ också är en faktor i $f(x)$. Vi får

$$2x^3 - 5x^2 + 7x + 5 = (2x + 1)(x^2 - 3x + 5).$$

Om man vill bestämma de andra rötterna till ekvationen så har man nu att lösa $x^2 - 3x + 5 = 0$. Kvadratkomplettring ger $(x - 3/2)^2 - (3/2)^2 + 5 = (x - 3/2)^2 + 11/4 = 0$, vilket resulterar i $x = (3 \pm i\sqrt{11})/2$. Låt oss till sist sammanfatta den första delen av exemplet i en sats:

[10] Man kan alternativt först konstatera att vi måste ha $SGD(q, p^3) = 1$ och då följer direkt att $q|2$.

Sats 18 *Låt $a_0+a_1x+\ldots+a_nx^n=0$ vara en ekvation med heltalskoefficienter och $x=p/q$ en rationell rot. Då gäller att*

$$p|a_0 \quad och \quad q|a_n.$$

Ett specialfall som dyker upp ganska ofta är när högstagradskoefficienten $a_n=1$. Då ger satsen att nämnaren i en eventuell rationell rot måste dela 1, så den är ± 1. Men då måste den rationella roten faktiskt vara ett *heltal*.

2.5.1 Övningar

1. Visa att ekvationen $6x^3+2x^2+18x+6=0$ har en rationell rot. Lös ekvationen fullständigt.
2. Ekvationen $5x^3-3x^2+15x-9=0$ har en rationell rot. Lös ekvationen fullständigt.
3. Lös ekvationen $2x^4+3x^3+2x^2+6x-4=0$, om vilken man vet att den har två rationella rötter.
4. Lös ekvationen $6x^4+25x^3+12x^2-25x+6=0$, vars rötter alla är rationella.
5. Lös ekvationen $x^3+6x^2+10x+5=0$.
6. Lös ekvationen $4x^3+16x^2-x-4=0$.
7. Lös ekvationen $x^3-5x+2=0$.
8. Ekvationen $x^3+3x^2+x-1=0$ har en rationell rot. Lös den.
9. Lös ekvationen $x^3-x^2-3x+2=0$.
10. Ekvationen $3x^3-2x^2-4x-1=0$ har en rationell rot. Lös den.
11. Ekvationen $5x^3-3x^2+15x-9=0$ har en rationell rot. Lös ekvationen fullständigt.
12. Visa att ekvationen $6x^3+2x^2+18x+6=0$ har en rationell rot. Lös ekvationen fullständigt.
13. Bestäm samtliga lösningar till ekvationen $6x^3-4x^2+x+1=0$.
14. Lös ekvationen $2x^3+9x^2+6x+1=0$.
15. Lös ekvationen $4x^3-7x^2-10x-2=0$.
16. Ekvationen $3x^3+7x^2+17x+5=0$ har en rationell rot. Lös den fullständigt.
17. Ekvationen $6x^4+19x^3-9x^2-38x-6=0$ har två rationella rötter. Lös den.
18. Ekvationen $3x^4-5x^3+x^2-5x-2=0$ har två rationella rötter. Lös ekvationen fullständigt.

19. Avgör om polynomen $3x^3 - 4x^2 - 2x + 1$ och $x^3 - 17x^2 + 58x + 1$ är primpolynom eller ej (betraktade som polynom med rationella koefficienter). Ledning: Bevisa först att om ett tredjegradspolynom (med rationella koefficienter) inte är primt, så har det ett rationellt nollställe.
20. Lös ekvationen $3x^4 - 8x^3 + 4x + 1 = 0$.
21. Ekvationen $x^3 + 3x^2 + x - 1 = 0$ har en rationell rot. Lös ekvationen den.
22. Ekvationen $3z^4 + 16z^3 + 20z^2 - 4z - 3 = 0$ har två rationella rötter. Lös den.
23. Lös ekvationen $2x^3 - 9x^2 + 2x + 1 = 0$.
24. Ekvationen $3x^4 - 5x^3 + x^2 - 5x - 2 = 0$ har två rationella rötter. Lös den fullständigt.
25. Bestäm alla rationella nollställen till polynomen $3x^3 - 4x^2 - 2x + 1$ och $x^3 - 17x^2 + 58x + 1$. Bestäm sedan samtliga nollställen.
26. Lös fullständigt ekvationen $12x^3 - 16x^2 + 7x - 1 = 0$.
27. Bestäm alla lösningar till ekvationen $5x^3 + 22x^2 + 13x + 2 = 0$. Man vet att ekvationen har minst en rationell rot.
28. Bestäm samtliga lösningar till ekvationen $x^3 + x - 10 = 0$.
29. Ett orakel har avslöjat att ekvationen $3x^3 - 7x^2 + 8x - 2 = 0$ säkert har någon rationell rot. Bestäm samtliga rötter.
30. Betrakta ekvationer av typen $4x^3 + ax^2 + bx + 12 = 0$ där a och b är heltal. Vilka av talen $-\frac{1}{2}, \frac{2}{3}, 2, 5$ och 6 kan ej vara rötter till en sådan ekvation?

2.6 Andragradsekvationer med komplexa koefficienter

Andragradsekvationer har vi löst *en masse*, men hittills har de bara haft reella koefficienter, även om några har haft icke-reella rötter. Vi skall diskutera hur man löser ekvationer med komplexa koefficienter. Det är egentligen inte svårare än när man har reella koefficienter och metoden är exakt densamma (nämligen kvadratkomplettering), men räkningarna blir mer omfattande. Vi gör det här i form av ett par exempel.

Exempel: Lös ekvationen $z^2 - (4 - 3i)z + 7 - i = 0$ (av gammal tradition heter den obekanta oftast z i det här sammanhanget). Kvadratkompletteringen är det inget konstigt med:

$$\begin{aligned} z^2 - (4-3i)z + 7 - i &= \left(z - \frac{4-3i}{2}\right)^2 - \left(\frac{4-3i}{2}\right)^2 + 7 - i \\ &= \left(z - \frac{4-3i}{2}\right)^2 + \frac{21}{4} + 5i. \end{aligned}$$

Sätt $w = z - (4-3i)/2$; då skall vi alltså lösa $w^2 = -21/4 - 5i$. Vi skriver $w = a + bi$ (där som vanligt a och b är reella) och sätter in:

$$w^2 = a^2 - b^2 + 2iab = -\frac{21}{4} - 5i$$

Identifierar vi real- och imaginärdelar så får vi $a^2 - b^2 = -21/4$ och $2ab = -5$. Det går att lösa detta ekvationssystem genom att lösa ut t ex b ur den andra ekvationen ($b = -5/2a$) och sedan sätta in i den första, men räkningarna blir lite kortare om man gör så här:

$$\begin{aligned}(a^2+b^2)^2 &= a^4 + 2a^2b^2 + b^4 = a^4 - 2a^2b^2 + b^4 + 4a^2b^2 \\ &= (a^2-b^2)^2 + (2ab)^2 = (-21/4)^2 + (-5)^2 = (29/4)^2,\end{aligned}$$

så att $a^2 + b^2 = 29/4$ ($a^2 + b^2$ är ju positivt eftersom a och b är reella). Ett alternativt sätt att bestämma $a^2 + b^2 = |w|^2$ är att ta absolutbeloppet av båda sidor i $w^2 = -21/4 - 5i$. Adderar vi så får vi

$$2a^2 = (a^2 - b^2) + (a^2 + b^2) = -21/4 + 29/4 = 2$$

alltså $a = \pm 1$. Nu bestämmer man b med hjälp av $2ab = -5$ och man får således följande möjligheter:

$$\left\{ \begin{array}{rcl} a &=& 1 \\ b &=& -5 \end{array} \right. \qquad \left\{ \begin{array}{rcl} a &=& -1 \\ b &=& 5 \end{array} \right.$$

Till sist får man z ur $z = (4-3i)/2 + w$ och rötterna blir $z_1 = 3 - 4i$ och $z_2 = 1 + i$.

Exempel: Lös ekvationen $z^2 - (2+i)z - 1 + 7i = 0$. Kvadratkomplettering ger

$$\left(z - \frac{2+i}{2}\right)^2 - \left(\frac{2+i}{2}\right)^2 - 1 + 7i = \left(z - \frac{2+i}{2}\right)^2 - \frac{7}{4} + 6i = 0,$$

dvs

$$\left(z - \frac{2+i}{2}\right)^2 = \frac{7}{4} - 6i.$$

Sätt $z - (2+i)/2 = a + ib$. Då blir

$$a^2 - b^2 = \frac{7}{4},\ 2ab = -6.$$

Tar vi absolutbeloppet av båda leden i $(z - (2+i)/2)^2 = 7/4 - 6i$ så får vi

$$a^2 + b^2 = \sqrt{\left(\frac{7}{4}\right)^2 + 6^2} = \frac{25}{4}.$$

Alltså blir

$$2a^2 = \frac{7}{4} + \frac{25}{4} = \frac{32}{4} = 8, \quad \text{dvs} \quad a = \pm 2, \quad b = -3/a = \mp\frac{3}{2}.$$

Rötterna blir till sist

$$z_1 = \frac{2+i}{2} + 2 - \frac{3i}{2} = 3 - i \quad \text{och} \quad z_2 = \frac{2+i}{2} - 2 + \frac{3i}{2} = -1 + 2i.$$

2.6.1 Övningar

1. Lös ekvationen $z^4 - 2z^2 + 2 = 0$.
2. Lös ekvationen $z^4 + 6z^2 + 5 = 0$.
3. Lös ekvationen $z^2 - z(3 - 2i) + 5 - i = 0$.
4. Lös $z^4 + 5z^2 + 6 = 0$.
5. Lös $z^2 + z(1 + 3i) + 3 + i\frac{27}{2} = 0$.
6. Lös ekvationen $iz^2 + (2 - 4i)z - 8 + 6i = 0$.
7. Lös ekvationen $z^2 - (2 + 2i)z - 1 + 2i = 0$.
8. Hitta alla komplexa tal z sådana att $z^2 = -i$.
9. Lös ekvationen $z^2 - 6iz - 12 - 4i = 0$.
10. Bestäm alla komplexa rötter till $z^6 = -1$. Rötterna ska ges på formen $a + bi$ (där a och b är reella tal) och får inte innehålla trigonometriska funktioner.
11. Lös ekvationen $z^2 + (3 + i)z + 6i + 2 = 0$.
12. Lös ekvationen $z^2 + \frac{29}{5-2i}z - 11 + 23i = 0$.
13. Lös ekvationen $iz^2 + (2 - 4i)z - 8 + 6i = 0$.
14. Bestäm två komplexa tal z och w med summan $z + w = 3$ och produkten $zw = 10i$.

2.7 Algebraiska tal

Läsaren känner sedan tidigare till uppdelningen av talen i rationella och irrationella. Man kan ”finindela” de irrationella talen vidare:

Definition: Ett (komplext) tal α säges vara *algebraiskt* och det är rot till någon ekvation av formen $p(x) = 0$ med *heltalskoefficienter*.

Det är lätt att hitta exempel på algebraiska tal. För det första är alla rationella tal algebraiska eftersom ekvationen $bx - a = 0$ har roten a/b. För det andra är $\sqrt{2}$, $-\sqrt{7}$ och i algebraiska eftersom de är rötter till $x^2 - 2 = 0$, $x^2 - 7 = 0$ respektive $x^2 + 1 = 0$. Ett tal av formen $\sqrt[n]{a}$ för heltal a är algebraiskt eftersom det är rot till $x^n - a = 0$. Mindre uppenbart är möjligen att $\alpha = \sqrt{11} + 2$ är algebraiskt då det inte är alldeles trivialt att hitta den ekvation det uppfyller. Men vi har ju $\alpha - 2 = \sqrt{11}$, så att $(\alpha^2 - 2)^2 = 11$ eller $\alpha^2 - 4\alpha - 7 = 0$. Talet α är således rot till $x^2 - 4x - 7 = 0$ och därmed algebraiskt.

Exempel: Bevisa att $\sqrt{2}-\sqrt{7}$ är algebraiskt och finn en ekvation som det är rot till. Kalla talet för β. Då har vi

$$\beta^2 = 2 - 2\sqrt{14} + 7 = 9 - 2\sqrt{14}.$$

Alltså är

$$\beta^2 - 9 = -2\sqrt{14}$$

och kvadrerar vi detta så får vi

$$(\beta^2 - 9)^2 = 4 \cdot 14 = 56.$$

Utveckling ger

$$\beta^4 - 18\beta^2 + 81 = 56,$$

så att β är rot till fjärdegradsekvationen $x^4 - 18x^2 + 25 = 0$ och således algebraiskt.

Man kan använda ekvationen $x^4 - 18x^2 + 25 = 0$ för att bevisa att β är irrationellt. Ty antag att $\beta = a/b$ vore rationellt. Enligt satsen i förra avsnittet måste då $a|25$ och $b|1$, så att $a \pm 1, \pm 5$ eller ± 25 och $b = \pm 1$; alltså $\beta = \pm 1, \pm 5$ eller ± 25. Men man kontrollerar (nästan) omedelbart att inget av dessa tal är en rot, varför β är irrationellt.

Vi såg att alla tre talen $\sqrt{2}$, $\sqrt{7}$ och $\sqrt{2}-\sqrt{7}$ är algebraiska. Det här kan generaliseras och man kan visa att summan, produkten och kvoten av algebraiska tal är algebraiska. Man brukar uttrycka det så att de algebraiska talen är *slutna* under de aritmetiska operationerna. En fråga som inte är så lätt att svara på är om det finns tal som inte är algebraiska. Euler[11] kallade sådana för *transcendenta*, men han kunde inte påvisa existensen av dem. Det dröjde till 1854 innan någon visade att det finns sådana, då Liouville[12] bevisade att talet

$$0,110001000000000000000001000\ldots$$

där ettorna kommer på platserna 1!, 2!, 3!, 4! osv är transcendent. Senare under 1800-talet bevisades det att e och π också är transcendenta tal. I en viss mening är de transcendenta talen oändligt många fler än de algebraiska, eftersom de senare kan bevisas vara en uppräknelig mängd, vilket inte de förra är. Ett grovt sätt att uttrycka detta är att om man sätter sin (oändligt vassa) pennspets på måfå på tallinjen, så är sannolikheten 0 att träffa ett algebraiskt tal och alltså 1 att man träffar ett transcendent. "Transcendent" kommer av latinets ord för överskrida.

2.7.1 Övningar

1. Bestäm ett polynom med heltalskoefficienter sådant att talet $\sqrt{5}-\sqrt{2}$ är ett nollställe till detta polynom. Visa även att $\sqrt{5}-\sqrt{2}$ är irrationellt.

[11] Leonhard Euler, schweizisk matematiker, 1707-1783.
[12] Joseph Liouville, fransk matematiker,1809-1882.

2. Bestäm en ekvation med heltalskoefficienter som har $\sqrt{5}+\sqrt{3}$ som en av sina rötter. Vilka är ekvationens övriga rötter?

3. Bestäm en tredjegradsekvation med heltalskoefficienter som har roten $1+\sqrt[3]{2}$ och bestäm de övriga rötterna.

4. Bestäm en ekvation som har talet $\sqrt[3]{14}$ som rot. Visa sedan att $\sqrt[3]{14}$ är irrationellt.

2.8 Filosofisk och numerisk epilog

Vad innebär det att lösa en ekvation? Låt oss fundera lite över den allra enklaste sortens andragradsekvation, säg $x^2-5=0$. Den är lätt att lösa säger Du, rötterna är ju $\pm\sqrt{5}$. OK, säger jag, men vad menar Du med $\sqrt{5}$? Jo, svarar Du kanske då, $\sqrt{5}$ är det positiva tal som i kvadrat blir 5, dvs som uppfyller $(\sqrt{5})^2=5$. Aha, säger jag, Din "lösning" av ekvationen $x^2-5=0$ består bara i att *Du inför en beteckning* för en av rötterna! Inte kan Du väl hävda att du därmed har *löst* ekvationen? Gör Du på samma sätt när Du skall lösa en mer komplicerad ekvation, som exempelvis $7x^6-5x^5+100x^4+1256x^3-x^2-78x-365=0$? Är det inte lite fusk att bara så här lättvindigt införa en beteckning för en rot till en ekvation?

Den här lilla dialogen visar att det finns skäl att fundera över vad man menar med att lösa en ekvation. Låt oss titta på $x^2+x-1=0$ också. Efter att ha gjort kvadratkompletteringen $(x+1/2)^2-(1/2)^2-1=(x+1/2)^2-5/4=0$ och fått rötterna $x=(-1\pm\sqrt{5})/2$ så känner man sig förstås nöjd, men vad har man egentligen därmed vunnit? Kan vi verkligen – utan att skämmas – säga att vi har *löst* ekvationen? Tja, det vi har bevisat är att *rötterna kan uttryckas med hjälp av talet* $\sqrt{5}$, dvs den positiva roten till $x^2-5=0$, men mer än så är det svårt att hävda att vi har åstadkommit.

Det finns flera olika svar på frågan vad det innebär att lösa en ekvation. Det svar som vår gamla vän p,q-formeln ger är att rötterna till en allmän andragradsekvation $x^2+px+q=0$ kan uttryckas med hjälp av en rot till en enklare ekvation, nämligen $t^2-\Delta=0$, där $\Delta=(p/2)^2-q$, men mer än det säger den faktiskt inte. Å andra sidan är ju det i sig ett intressant faktum som inte alls är självklart. Precis likadant förhåller det sig med Cardanos formler för tredjegradsekvationens rötter. Vad de visar är att rötterna till en tredjegradsekvation kan uttryckas med hjälp av rötterna till ekvationer av formen $t^2-a=0$ och $t^3-b=0$.

Vad man skall mena med att "lösa" en ekvation beror väldigt mycket på vad man har för syfte med lösningen, dvs helt enkelt vad man skall använda den till. Om man sysslar med algebra så är det oerhört intressant att rötterna till de allmänna ekvationerna av grad 2, 3 och 4 kan uttryckas med hjälp av rötter till enkla ekvationer av formen $t^k-a=0$ och lika intressant är det faktum att det inte är möjligt för allmänna ekvationer av högre grad än 4. Men om man är ingenjör och med hjälp av Pythagoras sats har räknat ut att längden av en balk

skall vara $\sqrt{5}$ meter, så duger förmodligen inte det som svar, utan då vill man veta ungefär hur stort detta tal är, dvs man vill hitta ett närmevärde i form av ett rationellt tal, som t ex $\sqrt{5} \approx 2,236$.

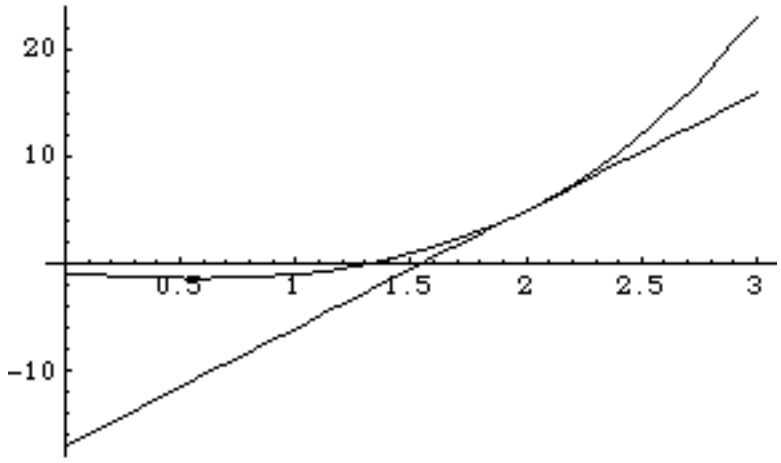
Man kan fortsätta de här funderingarna och exempelvis fråga sig om det verkligen *finns* ett tal $\sqrt{5}$ som har kvadraten 5. I inlednade kurser i aritmetik brukar man bevisa att tal av formen $\sqrt{5}$ inte är rationella, men vad är de då? Finns det sådana tal överhuvudtaget? Det är klart att eftersom $\sqrt{5}$ är längden av hypotenusan i en rätvinklig triangel med kateterna 1 och 2, så bör $\sqrt{5}$ i någon ganska konkret mening faktiskt existera. Det finns flera olika sätt att utvidga talområdet från de rationella talen; ett är att införa de *reella talen*, som s a s fyller ut hela tallinjen (trots att de rationella talen är väldigt många, ja t o m så många att det mellan två olika rationella tal alltid finns oändligt många andra, så fyller de inte ut hela tallinjen; punkten som motsvarar $\sqrt{5}$ motsvarar ju t ex inte ett rationellt tal). Konstruktionen av de reella talen är en utomordentligt komplicerad historia, men man kan hur som helst bevisa att det finns ett och endast ett positivt reellt tal som har kvadraten 5. Att tal som $\sqrt{5}$ som kan ges en enkel geometrisk tolkning existerar tycker antagligen de flesta är ganska uppenbart, men hur är det med något så obehagligt som $2^{\sqrt{2}}$? Och hur är det med komplexa tal, som t ex $3-4i$? Finns de? Och vad är de egentligen?[13] Begreppen "existera" och "existens" är inte enkla, vare sig i matematiken eller någon annanstans, och istället för att ge mig in i en lång, snårig förklaring av den mening i vilken $3-4i$ existerar, så svarar jag ibland med en motfråga: Vad är 2? Finns det verkligen? Se där en nöt att försöka knäcka! Nu skall vi emellertid bli lite mer jordnära.

Att hitta närmevärden till rötter till ekvationer är ett viktigt problem i tillämpningar, men det har även intressanta matematiska sidor. Det finns mängder av olika sätt att göra det på och vi skall titta på två sådana metoder.

Newton-Raphsons metod

Newton-Raphsons metod hör till den del av matematiken som kallas *analys* eller *differentialkalkyl* och för att förstå den måste man känna till derivata. Säg att vi vill bestämma närmevärden till nollstället α till funktionen f (som kommer att vara ett polynom nedan). Låt x_0 vara en punkt som vi av en eller annan anledning vet ligger i närheten av α (vad detta mer konkret betyder beror på hur f ser ut). Det kan se ut som i figuren nedan.

[13] Ordet "egentligen" är väldigt vanligt, och författaren till de här raderna tycker emellanåt att det förorenar språket, för vad betyder det *egentligen*? (Sic!)



$y = f(x)$, $x_0 = 2$

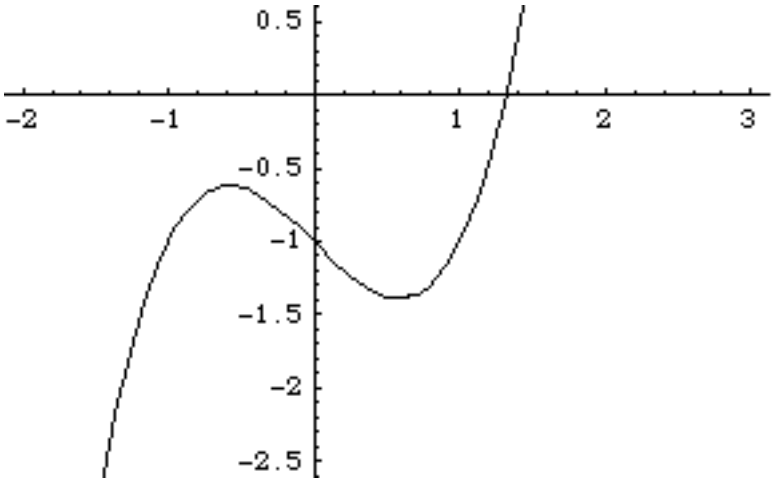
I figuren har vi även ritat in tangenten till kurvan $y = f(x)$ i punkten x_0 och dess skärningspunkt x_1 med x-axeln. I figuren verkar det ju faktiskt som om x_1 vore ett bättre närmevärde till α än x_0. Så här kan man fortsätta och nästa gång således dra tangenten i x_1 och hoppas på att dess skärningspunkt x_2 med x-axeln är ett ännu bättre närmevärde osv. På så sätt får man en svit av punkter $x_0, x_1, x_2, x_3, \ldots$ som med en gnutta tur närmar sig α mer och mer. Ekvationen för tangenten i x_0 är

$$y - f(x_0) = f'(x_0)(x - x_0)$$

och skärningspunkten med x-axeln får vi genom att sätta $y = 0$. Den blir $x_1 = x_0 - f(x_0)/f'(x_0)$. Allmänt får vi alltså den $(n+1)$:a punkten x_{n+1} från den n:te x_n genom formeln

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Vi skall demonstrera metoden med $f(x) = x^3 - x - 1$.



$y = x^3 - x - 1$

Vi har $f(1) = -1 < 0$ och $f(2) = 8 - 2 - 1 = 5 > 0$, så enligt satsen om mellanliggande värden har f ett nollställe α sådant att $1 < \alpha < 2$ (det är lätt att visa att det är det enda reella nollstället till f). Sätter vi in $f'(x) = 3x^2 - 1$ och förenklar så får vi formeln

$$x_{n+1} = \frac{2x_n^3 + 1}{3x_n^2 - 1}.$$

De första x_n:na blir

$$\begin{aligned} x_0 &= 2 \\ x_1 &= 1,545454545 \\ x_2 &= 1,359614916 \\ x_3 &= 1,325801345 \\ x_4 &= 1,324719049 \\ x_5 &= 1,324717979 \\ x_6 &= 1,324717957 \\ x_7 &= 1,324717957. \end{aligned}$$

Det ser verkligen ut som om vi redan efter sju upprepningar (*iterationer* brukar det heta i den här delen av matematiken) har fått ett bra närmevärde på roten α. Man kan uppskatta felet om man använder medelvärdessatsen:

$$|f(x_n) - f(\alpha)| = |f'(\xi)| \cdot |x_n - \alpha|$$

för något ξ mellan x_n och α. Vi får $|f'(\xi)| = |3\xi^2 - 1| \leq |3 \cdot 1^2 - 1| = 2$, så

$$|x_n - \alpha| \leq \frac{1}{2}|f(x_n)|,$$

eftersom $f(\alpha) = 0$. Insättning ger

$$|x_7 - \alpha| \leq \frac{1}{2}|f(x_7)| = 0,5 \cdot 10^{-9}.$$

Om vi tar hänsyn till avrundningsfelet i sista siffran ($\leq 0,5 \cdot 10^{-9}$), så ser vi att vi i alla fall har 8 korrekta decimaler i x_7.

Kedjebråksutveckling

Kedjebråk är en gammal fin del av matematiken som tyvärr håller på att alldeles glömmas bort. Låt α vara ett positivt reellt tal, som inte är ett heltal. Vi låter a_0 vara det största heltalet som är $\leq \alpha$. Talet a_0 kallas *heltalsdelen* av α och betecknas ofta $[\alpha]$. Om exempelvis $\alpha = 3,14$, så är $a_0 = 3$. Eftersom $\alpha - a_0$ är ett tal mellan 0 och 1, så kan vi skriva $\alpha - a_0 = 1/\alpha_1$, där α_1 är ett tal > 1. Vi har alltså

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Om α_1 skulle råka vara ett heltal, så slutar vi här. Annars kan vi upprepa och låta a_1 vara heltalsdelen av α_1. Då ligger $\alpha_1 - a_1$ också mellan 0 och 1 och vi kan skriva $\alpha_1 - a_1 = 1/\alpha_2$, dvs $\alpha_1 = a_1 + 1/\alpha_2$, där $\alpha_2 > 1$. Sätter vi ihop dessa så får vi

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}}.$$

Om α_2 skulle vara ett heltal, så slutar vi, annars fortsätter vi och får i nästa steg

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\alpha_3}}}$$

där $\alpha_3 > 1$ osv. Vi kan fortsätta på det här sättet tills vi stöter på ett α_i som är ett heltal. Låt oss se på ett exempel: För $\alpha = 83/35$ ger upprepade divisioner

$$\begin{aligned}
\frac{83}{35} &= 2 + \frac{13}{35} = 2 + \frac{1}{35/13} = 2 + \frac{1}{2 + 9/13} = 2 + \cfrac{1}{2 + \cfrac{1}{13/9}} \\
&= 2 + \cfrac{1}{2 + \cfrac{1}{1 + 4/9}} = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{9/4}}} \\
&= 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4}}}}.
\end{aligned}$$

Här kan vi inte fortsätta längre eftersom 4 är ett heltal. Lägg märke till att de upprepade divisionerna faktiskt inte är något annat än Euklides algoritm. Eftersom den alltid "tar slut", så ser vi att varje (positivt) rationellt tal kan skrivas på formen

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \cfrac{1}{a_n}}} \tag{2.13}$$

där som sagt alla a_i är positiva heltal. Å andra sidan är det ju självklart att ett uttryck som (*) är ett rationellt tal när alla a_i är heltal. Härav följer att om vi utför samma procedur med ett *irrationellt* tal istället, så tar den aldrig slut. Sviten av heltal $a_0, a_1, a_2, \ldots$ (som alltså är ändlig då α är rationellt och oändlig annars) kallas *kedjebråksutvecklingen* av α. Om man sätter

$$A_0 = a_0,\ A_1 = a_0 + \frac{1}{a_1},\ A_2 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}},\ \ldots,\ A_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots \cfrac{1}{a_n}}}$$

osv, så kan man bevisa att (de rationella) talen A_n närmar sig α då n växer. Talen A_n brukar kallas *konvergenterna* till α.

Vi skall studera hur kedjebråksutveklingen av några irrationella tal kan se ut och som första exempel tar vi $\alpha = \sqrt{2}+1$, som uppfyller sambandet $\alpha^2 - 2\alpha - 1 = 0$. Nu ser vi direkt att α ligger mellan 2 och 3, så att $a_0 = 2$, men annars hade vi kunnat resonera så här: Om vi sätter $p(x) = x^2 - 2x - 1$ så har vi $p(2) = -1$, $p(3) = 2$, så ekvationen $p(x) = 0$ har en rot α mellan 2 och 3. Den andra roten är negativ (t ex eftersom produkten av rötterna är $-1 < 0$). Vi får $a_0 = 2$ och inför α_1 genom $\alpha = 2 + 1/\alpha_1$. Insättning av detta uttryck i sambandet $\alpha^2 - 2\alpha - 1 = 0$ ger efter hyfsning $\alpha_1^2 - 2\alpha_1 - 1 = 0$, dvs α_1 uppfyller samma ekvation som α. Då båda talen är > 0, så är $\alpha = \alpha_1$ och $a_1 = 2$. I nästa steg inför vi α_2 genom $\alpha_1 = 2 + 1/\alpha_2$ och får $\alpha_2 = \alpha_1$ osv och vi ser att alla $a_n = 2$, så kedjebråksutvecklingen av α har det enkla utseendet $2, 2, 2, \ldots$. (Att alla a_n är lika är naturligtvis bara en lycklig slump, som vi skall se nedan.) Man räknar

snabbt ut konvergenterna:

$$\begin{aligned}
A_0 &= 2 \\
A_1 &= 2 + \frac{1}{2} = \frac{5}{2} = 2,5 \\
A_2 &= 2 + \frac{1}{2 + \frac{1}{2}} = \frac{12}{5} = 2,4 \\
A_3 &= 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \frac{29}{12} \approx 2,4167 \\
A_4 &= 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = \frac{70}{29} \approx 2,4138 \\
A_5 &= 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}}} = \frac{169}{70} \approx 2,4143.
\end{aligned}$$

Närmevärdet A_5 ger tre korrekta decimaler i α. [14]

Som ett andra exempel skall vi ta $\beta = 2 + \sqrt{7}$, som uppfyller $\beta^2 - 4\beta - 3 = 0$. Med samma teknik som i det förra exemplet får man

$$\begin{aligned}
\beta &= 4 + \frac{1}{\beta_1}, \quad 3\beta_1^2 - 4\beta_1 - 1 = 0 \\
\beta_1 &= 1 + \frac{1}{\beta_2}, \quad 2\beta_2^2 - 2\beta_2 - 3 = 0 \\
\beta_2 &= 1 + \frac{1}{\beta_3}, \quad 3\beta_3^2 - 2\beta_3 - 2 = 0 \\
\beta_3 &= 1 + \frac{1}{\beta_4}, \quad \beta_4^2 - 4\beta_4 - 3 = 0
\end{aligned}$$

Tydligen är $\beta_4 = \beta$ och kedjebråksutvecklingen av β är

$$4, 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, \ldots$$

[14] Observationen $A_{n+1} = 2 + 1/A_n$ gör de successiva beräkningarna av konvergenter enkel och man får $A_6 = 408/169$ och $A_7 = 985/408$. Om man använder Newton-Raphsons metod på ekvationen $x^2 - 2x - 1 = 0$ med $x_0 = 2$, så får man $x_1 = 5/2$, $x_2 = 29/12$, $x_3 = 985/408$, dvs en delmängd av konvergenterna. Detta fenomen är inte heller en tillfällighet, men vi har ingen möjlighet att gå djupare in på detta här.

De första konvergenterna är

$$
\begin{aligned}
B_0 &= 4 \\
B_1 &= 4 + \frac{1}{1} = 5 \\
B_2 &= 4 + \cfrac{1}{1 + \cfrac{1}{1}} = \frac{9}{2} = 4,5 \\
B_3 &= 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}} = \frac{14}{3} \approx 4,6667 \\
B_4 &= 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}} = \frac{65}{14} \approx 4,6429 \\
B_5 &= 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1}}}}} = \frac{79}{17} \approx 4,6471
\end{aligned}
$$

Det korrekta värdet är $\beta = 4,64575\ldots$. I de här två exemplen har utvecklingen visat sig vara *periodisk*, dvs de successiva kvoterna upprepar sig. Man kan bevisa att alla rötter till andragradsekvationer – och *bara* sådana tal – har periodiska kedjebråksutvecklingar. Dock är det inte säkert att de successiva kvoterna upprepar sig från början, det kan se ut så här också:

$$2,\ 1,\ 4,\ 4,\ 4,\ \ldots,$$

som är utvecklingen av $(15 + \sqrt{3})/6$.

Till sist skall vi kedjebråksutveckla en rot till tredjegradsekvationen $x^3 - x - 1 = 0$. Som vi såg ovan så har den bara en enda reell rot α som ligger mellan 1 och 2. Med samma teknik som i de tidigare exemplen får man kedjebråksutvecklingen

$$1,\ 3,\ 12,\ 1,\ 1,\ 3,\ 2,\ 3,\ \ldots,$$

vilken den här gången inte är periodisk. Konvergenten $A_7 = 2770/2091 \approx 1,3247$, som skall jämföras med det närmevärde vi fick med Newton-Raphson.

2.8.1 Övning

Bevisa att kedjebråksutvecklingen av det gyllene snittet $\gamma = (\sqrt{5}+1)/2$ är $1, 1, 1, 1, \ldots$. Låt konvergenterna vara Γ_n och skriv $\Gamma_n = p_n/q_n$ med $SGD(p_n, q_n) = 1$.

Bevisa att $q_n = p_{n-1}$ och att $p_0 = 1$, $p_1 = 2$, $p_{n+1} = p_n + p_{n-1}$ för $n \geq 2$. Talen p_n kallas *Fibonacci-tal* efter den italienske matematikern Fibonacci (Leonardo av Pisa, ca 1180-1250). De dyker upp i många olika delar av matematiken, men även i naturen. Mer om detta får dock läsaren ta reda på själv!

Kapitel 3

Blandade övningar

1. Polynomen $f(x) = x^4 - x^3 + 2x^2 + x + 3$ och $g(x) = x^4 + x^3 - 4x^2 - 5x - 5$ har minst ett gemensamt nollställe. Bestäm polynomens samtliga nollställen.

2. Bevisa att rötterna till ekvationen $z^3 + 2z^2 - 3 + i = 0$ är enkla samt att de ligger utanför enhetscirkelskivan i det komplexa talplanet (dvs att de har absolutbelopp > 1).

3. Visa följande implikation:

$$z^3 - 2z^2 + 12 - 11i = 0 \quad \Rightarrow \quad |z| > 2.$$

4. Ekvationen $z^3 + (3+2i)z^2 - (13-7i)z + 30 - 30i = 0$ har en reell rot. Lös ekvationen.

5. Bestäm rötterna till ekvationen $2z^3 - (6+i)z^2 + 3(3+i)z + 4i - 3 = 0$ då man vet att en av dem är rent imaginär.

6. Ekvationen $x^4 - 14x^2 + 32x - 15 = 0$ har roten $2 - i$. Lös ekvationen fullständigt.

7. Ekvationen $z^5 + 2z^3 + 8z^2 + 16 = 0$ har två rent imaginära rötter. Bestäm samtliga rötter.

8. Ekvationen $z^4 + z^3 - 2z^2 - 3z - 3 = 0$ har två olika reella rötter som har samma absolutbelopp. Lös ekvationen fullständigt.

9. Polynomen $f(x) = 3x^3 - x^2 + 6x - 2$ och $g(x) = 6x^2 + x - 1$ har ett gemensamt nollställe. Lös ekvationerna $f(x) = 0$ och $g(x) = 0$.

10. Bestäm de gemensamma rötterna till ekvationerna $z^4 - 4z^2 + 36 = 0$ och $z^4 + 2z^3 - 4z + 12 = 0$. Lös dem fullständigt.

11. Ekvationerna $x^4 - x^3 + 3x^2 - 2x + 2 = 0$ och $x^4 + x^3 + 4x^2 + 2x + 4 = 0$ har minst en gemensam rot. Lös dem.

12. En ekvation av fjärde graden med reella koefficienter har dubbelroten $1-i$. Ange ekvationen på formen $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$.

13. Bestäm det hela talet a så att $a\sqrt{3}$ är en rot till ekvationen $x^4 - 4x^3 - 47x^2 + 192x - 48 = 0$. Lös den sedan fullständigt.