SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Femtegradsekvationen

av

Niklas Fransson

2017 - No 44

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Femtegradsekvationen

Niklas Fransson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Torbjörn Tambour

2017

Femtegradsekvationen

Niklas Fransson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Torbjörn Tambour

2017

Sammanfattning

En femtegradsekvation är en algebraisk ekvation som kan skrivas på formen $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$, där $a, b, c, d, e \in \mathbb{C}$. I denna uppsats kommer vi visa att dessa ekvationer alltid har fem lösningar samt att reella femtegradsekvationer alltid har minst en och högst fem olika lösningar i $\mathbb{C}$ varav minst en är reell. Dock kommer vi även visa att det finns femtegradsekvationer som inte är lösbara med radikaler. Det går således inte att konstruera en generell algebraisk lösningsformel för femtegradsekvationen.

Innehåll

Inledning

I detta arbete kommer vi undersöka femtegradsekvationen algebraiskt. Arbetet inleds med ett kapitel om generell algebra där vi först går igenom inledande teori för talkroppar för att sedan redovisa olika egenskaper hos polynom och algebraiska ekvationer. Vi kommer sedan i andra kapitlet gå in mer specifikt på femtegradsekvationen och börja med att undersöka om det generellt finns reella och/eller komplexa lösningar till femtegradsekvationen och i så fall hur många för att sedan undersöka huruvida femtegradsekvationen är lösbar med radikaler.

Ambitionen har varit att skriva detta arbete så att det ska vara läsligt för andra (blivande) gymnasielärare i matematik, möjligtvis med undantag för vissa bevis. Av den anledningen finns det även ett kort nedslag om algebrans förekomst inom det svenska obligatoriska skolväsendet som presenteras ihop med beskrivningen av ekvationer av lägre grad. Strävan har även varit att så långt som möjligt definiera och bevisa alla de begrepp och satser som används i uppsatsen så att den endast förutsätter kunskap i matematik motsvarande vad en högskolestudent i matematik på grundläggande nivå kan antas ha hunnit uppnå.

Huvuddelen av satserna och deras bevis är hämtade från *Lärobok i algebra* av Nagell [5] samt material från min handledare Torbjörn Tambour. Många av satserna som presenteras i detta arbete är dock grundläggande inom algebra och kan även hittas i exempelvis Christofferson [1].

1 Inledande algebra

I detta kapitel kommer vi ge en generell algebraisk grund som vi kommer arbeta vidare med i senare kapitel. Vi kommer börja med ett antal definitioner som är speciellt viktiga för denna uppsats för att sedan formulera och bevisa några användbara grundsatser inom algebra. För att kunna tillgodogöra sig uppsatsen krävs viss kunskap inom exempelvis aritmetik, algebra och mängdlära. För en genomgång av denna grundkunskap, se exempelvis Hellström [3].

1.1 Inledande teori för talkroppar

Vanligtvis när vi löser ekvationer, åtminstone på gymnasienivå, arbetar vi med reella ekvationer och reella eller möjligtvis komplexa lösningar. När vi ska ta oss an teorin kring femtegradsekvationer som kommer senare i uppsatsen kräver den dock att vi kan hantera polynom och ekvationer i andra talkroppar. För att göra det behöver vi därför ett antal inledande definitioner och satser om talkroppar.

Definition 1.1.1: En *talkropp* är en icke-tom delmängd $K \subseteq \mathbb{C}$ sådan att alla summor, differenser, produkter och kvoter av element i K även de är element i K (med undantag för division med 0).

Den minsta talkroppen är $\mathbb{Q}$, mängden av de rationella talen. Även $\mathbb{R}$ och $\mathbb{C}$ är exempel på talkroppar. Ibland är det användbart att utvidga en viss talkropp så att den även innehåller vissa tal som den annars inte skulle gjort.

Definition 1.1.2: Om varje tal l i talkroppen $L \supseteq K$ kan skrivas som en ändlig summa $l = k_1 l_1 + k_1 l_2 + \cdots + k_n l_n$ av bestämda $l_i \in L$ och där $k_i \in K$ så sägs att L är en *ändlig utvidgning av* □ och att talen l_i är *generatorer* för utvidgningen L *över* K.

Sats 1.1.3: Om $L \supseteq K$ är en ändlig utvidgning av talkroppen K så går det att generera L med endast en generator för L över K om och endast om $L = K$.

Bevis: Antag att $L = K$. Då kan alla tal l i talkroppen $L = K$ skrivas som $l = k_1 k_2$ för $k_1, k_2 \in K$ enligt definitionen för en talkropp (Definition 1.1.1). Exempelvis är 1 en ensam generator för L över K.

Antag istället att det existerar en ensam generator för L över K, det vill säga att den finns ett $l_1 \in L$ så att alla tal l i talkroppen $L \supseteq K$ kan skrivas som $l = k_1 l_1$ för något $k_1 \in K$.

Eftersom vi vet att L är en ändlig utvidgning av K så måste även alla element i K ligga i L. Därmed kan alla tal $k \in K$ skrivas som $k = k_1 l_1$ för något $k_1 \in K$. För $k \neq$

0 så måste $k_1 \neq 0$ och då gäller $k = k_1 l_1 \Leftrightarrow l_1 = \frac{k}{k_1}$ vilket innebär $l_1 \in K$ eftersom det kan skrivas som en kvot av två tal i K.

Men om $l_1 \in K$ så måste alla tal $l \in K$ eftersom de kan skrivas som en produkt att två tal i K enligt $l = k_1 l_1$. Därmed är $L \subseteq K$ men eftersom $L \supseteq K$ enligt antagandet så måste $L = K$. Alltså är satsen bevisad.

Exempelvis är $\mathbb{C}$ en ändlig utvidgning av $\mathbb{R}$ med generatorerna 1 och i. Dock går det inte att konstruera $\mathbb{R}$ genom en ändlig utvidgning av $\mathbb{Q}$. Däremot går det att skapa äkta delmängder av $\mathbb{R}$ som innehåller irrationella tal genom ändliga utvidgning av $\mathbb{Q}$. Genom att konstruera $\mathbb{Q}(\sqrt{2})$ som en ändlig utvidgning av $\mathbb{Q}$ med generatorerna 1 och $\sqrt{2}$ så har vi *adjungerat* talet $\sqrt{2}$ till $\mathbb{Q}$. $\mathbb{Q}(\sqrt{2})$ är därmed den minsta utvidgningen av $\mathbb{Q}$ som även innehåller talet $\sqrt{2}$.

Eftersom roten ur ett element i en talkropp inte nödvändigtvis också är ett element i talkroppen är det vanligt att sådana tal kan behöva läggas till talkroppen. Vi kan då göra vad vi kallar radikala utvidgningar.

Definition 1.1.4: Ett tal β kallas en *radikal över K* om det är lösningen till en ekvation $\beta^m = k$ för något $k \in K$ och $m \in \mathbb{N} > 1$.

Definition 1.1.5: En utvidgning $L = K(a_1, a_2, \dots, a_n)$ sägs vara en *radikal utvidgning* av talkroppen K om a_1 är en radikal över K och a_i är en radikal över $K(a_1, a_2, \dots, a_{i-1})$ för alla $2 \leq i \leq n$.

Förutom generatorerna 1 och i så är det också exempelvis möjligt att konstruera $\mathbb{C}$ genom en ändlig utvidgning av $\mathbb{R}$ med generatorerna $1, -1, i$ och $-i$. Detta innebär dock att samma element i $\mathbb{C}$ kan uttryckas genom generatorerna på flera olika sätt. Vi undviker detta genom att använda generatorer som är linjärt oberoende.

Definition 1.1.6: Om $L \supseteq K$ är en ändlig utvidgning av talkroppen K så sägs generatorerna $l_i \in L$ vara *linjärt oberoende över K* om $k_1 l_1 + k_2 l_2 + \cdots + k_n l_n = 0$, där $k_i \in K$, om och endast om $k_1 = k_2 = \cdots = k_n = 0$. Då sägs även att generatorerna bildar en *bas* för utvidgningen L över K.

Vi ser här att en ensam generator alltid är linjärt oberoende och därmed en bas. Vi ska nu visa några fler egenskaper hos baser för ändliga utvidgningar.

Sats 1.1.7: Om $L \supset K$ är en ändlig utvidgning av talkroppen K och L genereras av två generatorer för L över K så bildar dessa två generatorer en bas för utvidgningen L över K.

Bevis: Antag att $l_1, l_2 \in L$ är två generatorer för L över K och att dessa inte är bas, det vill säga att de inte är linjärt oberoende. Därmed existerar enligt Definition 1.1.6 $k_1, k_2 \in K$, inte båda lika med noll, så att $k_1 l_1 + k_2 l_2 = 0$. Låt därför $k_2 \neq 0$ och därmed $k_1 l_1 + k_2 l_2 = 0 \Leftrightarrow l_2 = -\frac{k_1 l_1}{k_2}$. Därmed ser vi att l_1 själv kan generera L, vilket enligt Sats 1.1.3 måste innebära att $L =$ □, vilket är en motsägelse med vår utgångspunkt att $L \supset K$. Alltså måste vårt antagande att l_1 och l_2 inte är linjärt oberoende vara felaktigt. Därmed måste de vara en bas för utvidgningen L över K och satsen är bevisad.

1 och i är alltså en bas för $\mathbb{C}$ över $\mathbb{R}$ medan 1, -1, i och $-i$ inte är det. Vi ska nu visa att om en utvidgning är ändlig så existerar alltid en bas (av linjärt oberoende generatorer) för den utvidgningen.

Sats 1.1.8: Om L är en ändlig utvidgning av talkroppen K så existerar en bas för L över K.

Bevis: Eftersom L är en ändlig utvidgning över K så finns det generatorer från K till L enligt Definition 1.1.2. Antag därför att $l_1, l_2, \dots, l_n$ är en uppsättning generatorer för L över K. Om dessa är linjärt oberoende, så är de även en bas och satsen är visad.

Om $l_1, l_2, \dots, l_n$ inte är linjärt oberoende, så existerar enligt Definition 1.1.6 $k_1, k_2, \dots, k_n \in K$, inte alla lika med noll, så att $k_1 l_1 + k_2 l_2 + \cdots + k_n l_n = 0$. Låt exempelvis $k_n \neq 0$. Då kan vi lösa ut l_n genom $k_1 l_1 + k_2 l_2 + \cdots + k_n l_n = 0 \Leftrightarrow l_n = -\frac{k_1}{k_n} l_1 - \frac{k_2}{k_n} l_2 - \cdots - \frac{k_{n-1}}{k_n} l_{n-1}$. Eftersom $l_1, l_2, \dots, l_n$ genererar L kan alla tal $l \in L$ skrivas som $l = k_{l,1} l_1 + k_{l,2} l_2 + \cdots + k_{l,n} l_n = k_{l,1} l_1 + k_{l,2} l_2 + \cdots + k_{l,n} \left(-\frac{k_1}{k_n} l_1 - \frac{k_2}{k_n} l_2 - \cdots - \frac{k_{n-1}}{k_n} l_{n-1} \right) = (k_{l,1} - \frac{k_1}{k_n} k_{l,n}) l_1 + (k_{l,2} - \frac{k_2}{k_n} k_{l,n}) l_2 + \cdots + (k_{l,n-1} - k_{l,n} \frac{k_{n-1}}{k_n}) l_{n-1}$ där $k_{l,i} \in K$. Vi ser här att koefficienterna för $l_1, l_2, \dots, l_{n-1}$ ligger i K eftersom $k_n \neq 0$. Eftersom alla element i L kan genereras av $l_1, l_2, \dots, l_{n-1}$ så är därmed $l_1, l_2, \dots, l_{n-1}$ generatorer för L över K. Om nu dessa är linjärt oberoende är de en bas för L över K. Om de inte är det upprepar vi förra resonemanget tills vi har ett antal generatorer som är linjärt oberoende och alltså bildar en bas för L över K, vilket vi kan göra tack vare Sats 1.1.3 och Sats 1.1.7. Satsen är alltså bevisad.

Det existerar många olika baser för en ändlig utvidgning över en talkropp. Vi ska dock visa att de har något gemensamt, de har nämligen samma antal element. För att visa det behöver vi först en hjälpsats.

Sats 1.1.9: Antag att $m, n \in \mathbb{N}$, att $m > n > 0$ och att $a_{i,k} \in K$ där K är en talkropp. Då har ekvationssystemet $\begin{cases} a_{1,1}x_1+\cdots+a_{1,\square}x_m=0 \\ a_{2,1}x_1+\cdots+a_{2,m}x_m=0 \\ \cdots \\ a_{n,1}x_1+\cdots+a_{n,m}x_m=0 \end{cases}$ minst en lösning $x_i \in K$ sådan att inte alla x_i är 0.

Bevis: Vi ska alltså visa att ett ekvationssystem med fler variabler än ekvationer alltid har en lösning där inte alla variabler är lika med noll oavsett koefficienter. Vi ska börja med ett induktionsbevis över m.

För $m = 2$ och därmed $n = 1$ har vi $a_{1,1}x_1 + a_{1,2}x_2 = 0$. Om $a_{1,1} = a_{1,2} = 0$ är det uppenbart att alla $x_i \in K$ uppfyller likheten. Om $a_{1,1} = 0$ ser vi att alla $x_1 \in K$ uppfyller likheten och om $a_{1,2} = 0$ ser vi att alla $x_2 \in K$ uppfyller likheten. Om $a_{1,1}, a_{1,2} \neq 0$ ser vi att exempelvis $\begin{cases} x_1 = a_{1,2} \\ x_2 = -a_{1,1} \end{cases}$ uppfyller likheten. Alltså finns det lösningar för $m = 2$ och $n = 1$ oavsett koefficienternas värde.

Antag nu att ekvationssystemet har minst en lösning $x_i \in K$ sådan att inte alla x_i är 0 för $m - 1$ variabler och $m - 2$ rader, det vill säga att ett linjärt ekvationssystem med $m - 1$ variabler och $m - 2$ rader har minst en lösning där inte alla variabler är lika med noll.

Låt oss nu betrakta ekvationssystemet med m variabler och $n = m - 1$ ekvationer: $\begin{cases} a_{1,1}x_1+\cdots+a_{1,m}x_m=0 \\ a_{2,1}x_1+\cdots+a_{2,m}x_m=0 \\ \cdots \\ a_{n,1}x_1+\cdots+a_{n,m}x_m=0 \end{cases}$. Om alla $a_{i,j} = 0$ är det uppenbart att ekvationssystemet har sådana lösningar oavsett m och n. Vi utgår därför från att någon koefficient inte är lika med noll, låt denna vara $a_{n,m}$. Om vi då betraktar den sista raden i ekvationssystemet ser vi att vi kan skriva om ekvationen som $a_{n,1}x_1 + \cdots + a_{n,m}x_m = 0 \Leftrightarrow \frac{a_{n,1}}{a_{n,m}}x_1 + \frac{a_{n,2}}{a_{n,m}}x_2 \ldots + x_m = 0$ eftersom $a_{n,m} \neq 0$. Subtraherar vi multiplar av denna ekvation från övriga ekvationer i systemet (enligt motsvarade koefficient till x_m) kan vi eliminera x_m från dessa ekvationer. Då bildar dessa ekvationer ett system med $m - 1$ variabler och $n - 1 = m - 2$ ekvationer. Detta system har minst en lösning $x_i \in K$ sådan att inte alla x_i är 0 enligt antagandet. Sätter vi in dessa lösningar i sista ekvationen får vi även hophörande värde på x_m. Vi ser även att det inte hade spelat någon roll om vi hade valt en annan koefficient än $a_{n,m}$ att inte vara lika med noll för då hade vi använt samma metod och resonemang och fått samma resultat ändå. Alltså har vi visat att ekvationssystemet har minst en lösning $x_i \in K$ sådan att inte alla x_i är 0 och induktionssteget är klart.

Enligt vårt induktionsbevis finns det alltså en lösning för alla m och $n = m - 1$. Men en lösning som gäller för ett ekvationssystem med m variabler och n ekvationer måste även gälla om en eller flera av ekvationerna ”togs bort”. Om det finns minst en lösning för alla ekvationssystem m variabler och $n = m - 1$ ekvationer måste det

således även finnas minst en lösning för alla ekvationssystem av m variabler och $n < m$ ekvationer. Alltså är satsen bevisad.

Denna sats använder vi nu för att visa att alla baser har samma antal element.

Sats 1.1.10: Om L är en ändlig utvidgning av talkroppen K så har alla baser av L över K samma antal element.

Bevis: Låt $b_1, b_2 \dots b_m$ vara en bas för L över K. Vi ska först visa att fler än m tal i L alltid är beroende över K. Låt därför $l_1, l_2 \dots l_n \in L$ och $n > m$. Då finns $a_{i,j} \in K$ så att $\begin{cases} l_1 = a_{1,1}b_1 + \cdots + a_{1,m}b_m \\ l_2 = a_{2,1}b_1 + \cdots + a_{2,m}b_m \\ \dots \\ l_n = a_{n,1}b_1 + \cdots + a_{n,m}b_m \end{cases}$ och vi ska visa att det finns $x_i \in K$, ej alla 0, sådana att $x_1 l_1 + \cdots + x_n l_n = 0$ ty i så fall är de beroende.

Eftersom $x_1 l_1 + \cdots + x_n l_n = \sum_{i=1}^{n} x_i l_i = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j} x_i b_j = \sum_{j=1}^{m} (\sum_{i=1}^{n} a_{i,j} x_i) b_j$ och basen b är linjärt oberoende så är alltså $\sum_{i=1}^{n} x_i l_i = 0 \Leftrightarrow \sum_{i=1}^{n} a_{i,j} x_i = 0$ för $j = 1,2, \dots, m$. Den högra likheten ger ekvationssystemet $\begin{cases} a_{1,1}x_1 + \cdots + a_{n,1}x_n = 0 \\ a_{1,2}x_1 + \cdots + a_{n,2}x_n = 0 \\ \dots \\ a_{1,m}x_1 + \cdots + a_{n,m}x_n = 0 \end{cases}$ där antalet x_i är större än antalet ekvationer eftersom $n > m$. Enligt Sats 1.1.9 har detta ekvationssystem minst en lösning där $x_i \in K$ sådan att inte alla x_i är 0 och därmed är talen l_i beroende över K.

Låt nu $c_1, c_2, \dots, c_r$ vara en annan bas för L över K. Enligt ovanstående resonemang gäller att $r \leq m$ ty annars skulle $c_1, c_2, \dots, c_r$ vara beroende och därmed inte alls en bas. Men om vi vet att $c_1, c_2, \dots, c_r$ är en annan bas så gäller enligt samma resonemang att $m \leq r$ ty annars skulle $b_1, b_2, \dots, b_m$ vara beroende och därmed inte en bas. Alltså måste $m = r$, det vill säga att baserna b och c har samma antal element. Samma resonemang gäller för alla baser och alltså måste alla baser för L över K ha samma antal element, vilket skulle visas.

Definition 1.1.11: Antalet generatorer i en bas för utvidgningen L över K kallas *graden av L över K* och betecknas med $[L:K]$.

Det går såklart även att utvidga en redan utvidgad talkropp. Vi ska nu visa en egenskap som gäller när detta sker.

Sats 1.1.12: Låt L vara en utvidgning av talkroppen K och M vara en utvidgning av L. Utvidgningen M över K är då ändlig om och endast om M över L och L över K är det. I så fall gäller att graden av M över K är lika med produkten av graden av M över L och graden av L över K, det vill säga att $[M:K] = [M:L][L:K]$.

Bevis: Antag först att utvidgningen M över K är ändlig och sätt $[M:K] = n$. Enligt Sats 1.1.10 vet vi att alla baser för M över K har samma antal element så fler än n element i M måste vara linjärt beroende över K. Vi ska nu hitta en bas för L över K. Välj därför ett $a_1 \in L$. Om a_1 genererar L över K så är utvidgningen L över K ändlig. Om a_1 inte genererar L över K så måste det finnas ett $a_2 \in L$ sådan att a_1 och a_2 är linjärt oberoende. På samma sätt ser vi att om nu a_1 och a_2 genererar L över K så är utvidgningen L över K ändlig. Om inte a_1 och a_2 genererar L över K så fortsätter vi välja $a_3, a_4, \dots, a_m$ tills vi hittat en bas för L över K. Eftersom fler än n element i M är linjärt beroende över K och $a_1, a_2, \dots, a_{\square} \in M$ så måste $m \leq n$. Alltså är antalet $a_1, a_2, \dots, a_m$ ändligt och utvidgningen L över K är ändlig.

Låt nu $b_1, b_2, \dots, b_n$ vara generatorer för M över K. Då är $b_1, b_2, \dots, b_n$ även generatorer för M över L. Eftersom utvidgningen M över L har ett ändligt antal generatorer så är M över L en ändlig utvidgning.

Antag istället att utvidgningarna M över L och L över K är ändliga. Låt $a_1, a_2, \dots, a_n$ vara en bas för utvidgningen L över K och $b_1, b_2, \dots, b_m$ vara en bas för utvidgningen M över L. Vi kan alltså skriva alla $m \in M$ som $m = \sum_{i=1}^{m} l_i b_i$ med $l_i \in L$. Men vi kan även uttrycka alla $l \in L$ som $l = \sum_{j=1}^{n} k_j a_j$ med $k_j \in K$. Alltså måste $m = \sum_{i=1}^{m} l_i b_i = \sum_{i=1}^{m} \sum_{j=1}^{n} k_{i,j} b_i a_j$. Nu ser vi att talen $b_i a_j$ genererar utvidgningen M över K och eftersom n och m är ändliga måste även antalet $b_i a_j$ vara ändligt. Alltså är utvidgningen M över K ändlig.

Antag sist att $\sum_{i=1}^{m} \sum_{j=1}^{n} k_{i,j} b_i a_j = 0$ vilket kan skrivas $\sum_i b_i \sum_j k_{i,j}\, a_j = 0$. Eftersom alla b_i är linjärt oberoende över L måste $\sum_j k_{i,j}\, a_j = 0$ för alla i. Och eftersom alla a_j är linjärt oberoende över K måste då $k_{i,j} = 0$ för alla i, j. Alltså är talen $b_i a_j$ linjärt oberoende och därmed en bas för utvidgningen M över K. Enligt Sats 1.1.10 är då antalet $b_i a_j$ lika med $[M:K]$ och eftersom antalet $b_i a_j$ är lika med produkten mn är alltså $[M:K] = [M:L][L:K]$. Satsen är bevisad.

Detta var en inledande genomgång av olika egenskaper hos talkroppar. Vi ska nu gå vidare med att definiera olika begrepp och egenskaper hos polynom.

1.2 Begrepp och satser om polynom

I detta delkapitel kommer vi definiera majoriteten av de begrepp som vi kommer använda oss av senare i uppsatsen, nämligen begreppet polynom och olika varianter av och egenskaper hos dessa. Vi kommer utifrån definitionerna vi gjorde i det förra delkapitlet formulera några nyckelbegrepp om och metoder för hur vi arbetar med polynom i olika talkroppar. Vi kommer sedan formulera några användbara grundsatser inom algebra och bevisa dem.

Definition 1.2.1: Med ett *polynom* i variablerna $x_1, x_2, \dots, x_r$ *över talkroppen* K menas ett uttryck av formen $\sum a_{k_1,k_2,\dots,k_r} x_1^{k_1} x_2^{k_2} \dots x_r^{k_r}$ där *koefficienterna* $a \in K$ och där $k_1 = 0,1, \dots, n_1; k_2 = 0,1, \dots, n_2; \dots; k_r = 0,1, \dots, n_r$. Mängden av polynom med koefficienter i K betecknas $K[x]$.

Som exempel kan nämnas att både $3x + 2$ och $x^2 + 2yx - z$ är polynom. Vi noterar även att uttryck som enbart består av en konstant också räknas som polynom. Eftersom vi i denna text huvudsakligen inriktar oss på vissa typer av polynom som är speciellt intressanta för de ekvationer vi kommer studera kan det dock vara lämpligt att skapa ett smalare begrepp för dessa polynom.

Definition 1.2.2: Ett polynom i variabeln x *av graden* n över talkroppen K är ett polynom av formen $p(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, där $a_k \in K$, $n \in N, n \geq 0$ och $a_n \neq 0$. Vi skriver att $deg\, p(x) = n$.

Räkneoperationer för polynom över en godtycklig talkropp är samma som för reella och komplexa polynom. Summan, differensen och produkten av polynom är återigen polynom. Graden av summan eller differensen av två polynom kan ha olika grad beroende på polynomens grader och koefficienter. Om $p(x) = a_1 x^2 + b_1 x$ och $\square(x) = x^2 + 3x + 4$ är två polynom med graden två har exempelvis differensen $p(x) - q(x) = a_1 x^2 + b_1 x - (x^2 + 3x + 4) = (a_1 - 1)x^2 + (b_1 - 3)x - 4$ graden två om $a_1 \neq 1$, graden ett om $a_1 = 1, b_1 \neq 3$ och graden noll om $a_1 = 1, b_1 = 3$. Däremot finns ett mer entydigt samband mellan graden av produkten av två polynom.

Sats 1.2.3: Graden av en produkt av två polynom (inget lika med noll) är lika med summan av polynomens grader. Om $p(x), q(x) \neq 0$ och är två polynom gäller alltså att $\deg p(x)q(x) = \deg p(x) + \deg q(x)$.

Bevis: Låt $p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \neq 0$, där $a_i \in K$ för någon talkropp K, $a_n \neq 0$ och $n \in N \geq 0$ och låt $q(x) = \sum_{j=0}^{m} b_j x^j = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \neq 0$, där $b_j \in K$, $b_m \neq 0$ och $m \in N, m \geq 0$.

Då är $p(x)q(x) = \sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^{\square}$, vilket efter utveckling kan skrivas som $p(x)q(x) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m}$ där varje c_k är en summa av termer av typen $a_i b_j$. Exempelvis är $c_1 = a_0 b_1 + a_1 b_0$. Vi ser alltså att $p(x)q(x)$ ligger i talkroppen K samt att $\deg p(x)q(x) = n + m$ eftersom $c_{n+m} = a_n b_m \neq 0$. Alltså har vi visat att $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ och beviset är klart.

Kvoten av två polynom är dock inte nödvändigtvis ett polynom så därför inför vi ett begrepp för vad vi menar med delbarhet för polynom.

Definition 1.2.4: Ett polynom $q(x)$ över talkroppen *K delar* ett annat polynom $p(x)$ över talkroppen K om $p(x) = q(x)g(x)$ för något polynom $g(x)$ över talkroppen K. Detta skrivs $q(x)|p(x)$.

Exempelvis kan vi se att $x-1|x^5+x^4-3x^3+4x^2-4x+1$ eftersom $x^5+x^4-3x^3+4x^2-4x+1=(x-1)(x^4+2x^3-x^2+3x-1)$. Vi kan även se att ett polynom kan ha delare i en talkropp men sakna delare i en annan. Polynomet $p(x)=x^2-2$ har exempelvis delaren $x+\sqrt{2}$ över talkroppen $\mathbb{Q}(\sqrt{2})$ medan $p(x)$ saknar delare över talkroppen $\mathbb{Q}$ (förutom konstanter eller multiplar av $p(x)$). Vi inför därför följande begrepp för om polynom har delare eller inte i en specifik talkropp.

Definition 1.2.5: Ett polynom av variabeln x av graden n sägs vara *reducibelt* över talkroppen K om polynomet går att skriva som en produkt av polynom av variabeln x över talkroppen K med respektive grad ≥ 1 och $< n$. I motsatt fall är polynomet *irreducibelt* över talkroppen K.

Nu har vi definierat tillräckligt många begrepp för att kunna härleda en hel del resultat. Vi börjar med Divisionsalgoritmen, en sats som vi kommer använda oss av mycket framöver.

Sats 1.2.6 (Divisionsalgoritmen): Låt $p(x)$ och $g(x)\neq 0$ vara två polynom över talkroppen K så att $g(x)$ har högst samma grad som $p(x)$. Då finns entydigt bestämda polynom $q(x)$ och $r(x)$, också över talkroppen K, sådana att $p(x)=q(x)g(x)+r(x)$ där graden av $r(x)$ är lägre än graden av $g(x)$.

Följande bevis är hämtat från Nagell [5]. Antag att $p(x)=\sum_{k=0}^{n}a_k x^{n-k}$, där $a_k \in K$, $a_0\neq 0$ och $n\in N\geq 1$ samt att $g(x)=\sum_{k=0}^{m}b_k x^{m-k}$, där $\mathrm{b_k}\in \mathrm{K}$, $\mathrm{b_0}\neq 0$ och $m\leq n$. Eftersom $r(x)$ har lägre grad än $g(x)$ så måste $q(x)$ ha graden $n-m$ för att $p(x)$ och $q(x)g(x)+r(x)$ ska ha samma grad.

Sätt alltså $q(x)=\sum_{k=0}^{n-m}q_k x^{n-m-k}$ och $r(x)=\sum_{k=0}^{m-1}r_k x^{m-1-k}$. Sätt nu in dessa två uttryck i ekvationen $p(x)=q(x)g(x)+r(x)$ vilket ger att $\sum_{k=0}^{n}a_k x^{n-k}=\sum_{k=0}^{n-m}q_k x^{n-m-k}\sum_{k=0}^{m}b_k x^{m-k}+\sum_{k=0}^{m-1}r_k x^{m-1-k} \Leftrightarrow (a_0x^n+a_1x^{n-1}+\cdots+a_n)=(q_0x^{n-m}+q_1x^{n-m-1}+\cdots+q_{n-m})(b_0x^m+b_1x^{m-1}+\cdots+b_m)+(r_0x^{m-1}+r_1x^{m-2}+\cdots+r_{m-1})$. Utvecklar vi nu parentesprodukten i sista likheten får vi $(a_0x^n+a_1x^{n-1}+\cdots+a_n)=b_0q_0x^n+(b_1q_0+b_0q_1)x^{n-1}+\cdots+(b_0q_{n-m}+b_1q_{n-m-1}+\cdots+b_{n-m}q_0)x^m+(b_1q_{n-m}+\cdots+b_{n-m+1}q_0)x^{m-1}+\cdots+b_mq_{n-m}+(r_0x^{m-1}+r_1x^{m-2}+\cdots+r_{m-1})$.

Genom att jämföra alla termer med samma potens av x kan vi nu se att koefficienterna q_k och r_k blir entydigt bestämda av koefficienterna a_k och b_k i samma talkropp samt att $q_0\neq 0$. Jämför vi de potenser av x där exponenten är större än $m-1$ kan vi succesivt bestämma alla $q_0, q_1, \ldots q_{n-m}$ utifrån a_k och b_k. Ty

eftersom $n > m - 1$ så måste $a_0 = q_0 b_0$ och eftersom $a_0, b_0 \neq 0$ så måste $q_0 = \frac{a_0}{b_0} \neq 0 \in K$. Vidare är $a_1 = b_1 q_0 + b_0 q_1 = b_1 \frac{a_0}{b_0} + b_0 q_1 \Leftrightarrow q_1 = \frac{a_1 - b_1 \frac{a_0}{b_0}}{b_0} \in K$ och så vidare till och med $q_{n-m} = \frac{a_{n-m} - b_1 q_{n-m-1} - \cdots - b_{n-m} q_0}{b_0} \in K$. Vi är därmed klara med koefficienterna till $q(x)$ och går vidare med koefficienterna till $r(x)$. Vi ser nu att vi succesivt kan beräkna $r_0, r_1, \ldots r_{m-1}$ utifrån a_k, b_k och $q_0, q_1, \ldots q_{n-m}$ genom att betrakta koefficienterna till de potenser av x där exponenten är mindre än m. Ty genom att betrakta koefficienterna till x^{m-1} ser vi att $a_{n-m+1} = b_1 q_{n-m} + \cdots + b_{n-m+1} q_0 + r_0 \Leftrightarrow r_0 = a_{n-m+1} - b_1 q_{n-m} - \cdots - b_{n-m+1} q_0$ och därmed att $r_0 \in K$. Vidare är även $r_1 = a_{n-m+2} - b_2 q_{n-m} - \cdots - b_{n-m+2} q_0$ fram till och med $r_{m-1} = a_n - b_m q_{n-m}$. Därmed är koefficienterna för $r(x)$ bestämda och ligger i K. Vi har alltså visat att koefficienterna q_k och r_k blir entydigt bestämda av koefficienterna a_k och b_k i samma talkropp samt att $q_0 \neq 0$. Därmed har vi visat både existensen och entydigheten av $q(x)$ och $r(x)$ och således är satsen bevisad.

Utifrån Divisionsalgoritmen (Sats 1.2.6) får vi flera andra satser.

Sats 1.2.7: Låt $p(x)$ och $g(x)$ vara två polynom över talkroppen K. Då finns det ett entydigt bestämt polynom $h(x)$ över talkroppen K sånär som på multiplikation med konstanter som delar både $p(x)$ och $g(x)$ och som uppfyller att om något polynom delar både $p(x)$ och $g(x)$ så delar det även $h(x)$.

Bevis: Låt oss börja med att visa att om det existerar ett sådant polynom så är det entydigt sånär som på multiplikation med konstanter. Antag därför att det finns två polynom $h_1(x)$ och $h_1(x)$ som uppfyller kraven. Därmed måste $h_1(x) | h_2(x)$ och $h_2(x) | h_1(x)$ men detta är bara möjligt om $h_2(x) = k h_1(x)$ för något $k \in K, k \neq 0$. Alltså är $h(x)$ entydigt sånär som på multiplikation med konstanter.

Vi ska nu visa att det faktiskt existerar ett sådant polynom. Om något av $p(x)$ och $g(x)$ är nollpolynomet är det klart att $h_0(x) = 1$ uppfyller kraven. Antag därför att $p(x), g(x) \neq 0$ och att $g(x)$ har högst samma grad som $p(x)$. Enligt Divisionsalgoritmen vet vi att det finns entydiga bestämda polynom $q(x)$ och $r(x)$, också över talkroppen K, sådana att $p(x) = q(x)g(x) + r(x)$ där graden av $r(x)$ är lägre än graden av $g(x)$.

Om nu $r(x) = 0$ så är $p(x) = q(x)g(x)$ och därmed gäller att $g(x) | p(x)$ och att $h_3(x) = g(x)$ uppfyller kraven.

Om istället $r(x) \neq 0$ kan vi återigen använda Divisionsalgoritmen, fast för $g(x)$ och $r(x)$ och får då att det finns entydigt bestämda polynom $g_1(x)$ och $r_1(x)$, också över talkroppen K, sådana att $g(x) = g_1(x)r(x) + r_1(x)$ där graden av $r_1(x)$ är lägre än graden av $r(x)$.

Om nu $r_1(x) = 0$ gäller att $g(x) = g_1(x)r(x)$. Alltså måste $r(x)|g(x)$ och eftersom $p(x) = q(x)g(x) + r(x)$ måste då även $r(x)|f(x)$. Vi ser att $h_4(x) = r(x)$ uppfyller villkoren.

Om istället även $r_1(x) \neq 0$ så fortsätter vi använda Divisionsalgoritmen, nu för $r(x)$ och $r_1(x)$ och fortsätter tills vi får att $r_n(x) = 0$. Eftersom $r_n(x)$ har lägre grad än $r_{n-1}(x)$ som har lägre grad än alla $r_k(x)$ för $k < n - 1$ behöver vi endast utföra Divisionsalgoritmen ett ändligt antal gånger. Eftersom $r_n(x) = 0$ ser vi att $r_{n-2}(x) = g_n(x)r_{n-1}(x)$. Därmed ser vi tydligt att $r_{n-1}(x)|r_{n-2}(x)$ och eftersom $r_{n-3}(x) = g_{n-1}(x)r_{n-2}(x) + r_{n-1}(x)$ måste $r_{n-1}(x)|r_{n-3}(x)$ och så vidare tills vi ser att $r_{n-1}(x)|r(x)$ och därmed att $r_{n-1}(x)|g(x)$ och därmed att $r_{n-1}(x)|p(x)$. Vi ser här att $h_5(x) = r_{n-1}(x)$ uppfyller villkoren. Ty om något polynom delar $p(x)$ och $g(x)$ så måste det även dela $r(x)$ eftersom $p(x) = q(x)g(x) + r(x)$ och därmed även $r_1(x)$ eftersom $g(x) = g_1(x)r(x) + r_1(x)$ och så vidare ner till $r_{n-1}(x)$.Vi har alltså visat existensen av $h(x)$. Alltså är satsen bevisad.

Vi har visat att det till två godtyckliga polynom $p(x)$ och $g(x)$ över en talkropp alltid finns ett entydigt nollskilt polynom $h(x)$ över samma talkropp sånär som på multiplikation med konstanter som delar både $p(x)$ och $g(x)$ och som delas av alla polynom som delar både $p(x)$ och $g(x)$. Det kan inte finnas något polynom av högre grad än $h(x)$ som delar $p(x)$ och $g(x)$ eftersom det då inte skulle dela $h(x)$. Av samma anledning kan det heller inte finnas något polynom över samma talkropp av samma grad som $h(x)$ som delar $p(x)$ och $g(x)$ såvida det inte är en konstantmultipel av $h(x)$. Ett speciellt intressant polynom är den konstantmultipel av $h(x)$ där koefficienten för den högsta potensen av x är lika med 1. Vi ska införa ett speciellt begrepp för detta polynom.

Definition 1.2.8: Den *största gemensamma delaren* till två polynom $p(x)$ och $q(x)$ över talkroppen K är det polynom $d(x)$, också över talkroppen K, som, av alla polynom som delar både $p(x)$ och $q(x)$, har den högsta graden och där koefficienten för den högsta potensen av x är lika med 1.

Sats 1.2.9: Låt $p(x)$ och $g(x) \neq 0$ vara två polynom över talkroppen K så att $g(x)$ har högst samma grad som $p(x)$. Då finns det två polynom $p_0(x)$ och $g_0(x)$, också över talkroppen K, så att $p_0(x)p(x) + g_0(x)g(x) = d(x)$ där $d(x)$ är största gemensamma delaren till $p(x)$ och $g(x)$ över talkroppen K.

Beviset följer av Divisionsalgoritmen (Sats 1.2.6) och är väldigt likt beviset för Sats 1.2.7. Enligt Divisionsalgoritmen vet vi att det finns entydiga bestämda polynom $q(x)$ och $r(x)$, också över talkroppen K, sådana att $p(x) = q(x)g(x) + r(x)$ där graden av $r(x)$ är lägre än graden av $g(x)$.

Om nu $r(x) = 0$ så är $p(x) = q(x)g(x)$ och därmed gäller att $g(x)|p(x)$ och att största gemensamma delaren till $p(x)$ och $g(x)$ är $g(x)$ så när som på en konstant. Om $a_n \in \mathbb{R}$ är koefficienten för den högsta potensen av x för $g(x)$ så går det att konstruera $p_0(x) = 0$ och $g_0(x) = \frac{1}{a_n}$ vilket ger $p_0(x)p(x) + g_0(x)g(x) = d(x)$ och satsen gäller.

Om istället $r(x) \neq 0$ kan vi återigen använda Divisionsalgoritmen, fast för $g(x)$ och $r(x)$ och får då att det finns entydigt bestämda polynom $g_1(x)$ och $r_1(x)$, också över talkroppen K, sådana att $g(x) = g_1(x)r(x) + r_1(x)$ där graden av $r_1(x)$ är lägre än graden av $r(x)$.

Om nu $r_1(x) = 0$ gäller att $g(x) = g_1(x)r(x)$. Alltså måste $r(x)|g(x)$ och eftersom $p(x) = q(x)g(x) + r(x)$ måste då även $r(x)|f(x)$. Vi ser även att $r(x)$ måste vara största gemensamma delaren till $p(x)$ och $g(x)$ så när som på en konstant eftersom alla deras gemensamma delare till $p(x)$ och $g(x)$ även måste dela $r(x)$. Om $b_n \in \mathbb{R}$ är koefficienten för den högsta potensen av x för $r(x)$ så går det att konstruera $p_0(x) = \frac{1}{b_n}$ och $g_0(x) = -\frac{1}{b_n}q(x)$ vilket ger $p_0(x)p(x) + g_0(x)g(x) = d(x)$ och satsen gäller.

Om istället även $r_1(x) \neq 0$ så fortsätter vi använda Divisionsalgoritmen, nu för $r(x)$ och $r_1(x)$ och fortsätter tills vi får att $r_n(x) = 0$. Eftersom $r_n(x)$ har lägre grad än $r_{n-1}(x)$ som har lägre grad än alla $r_k(x)$ för $k < n - 1$ behöver vi endast utföra Divisionsalgoritmen ett ändligt antal gånger. Eftersom $r_n(x) = 0$ ser vi att $r_{n-2}(x) = g_n(x)r_{n-1}(x)$. Därmed ser vi tydligt att $r_{n-1}(x)|r_{n-2}(x)$ och eftersom $r_{n-3}(x) = g_{n-1}(x)r_{n-2}(x) + r_{n-1}(x)$ måste $r_{n-1}(x)|r_{n-3}(x)$ och så vidare tills vi ser att $r_{n-1}(x)|r(x)$ och därmed att $r_{n-1}(x)|g(x)$ och därmed att $r_{n-1}(x)|p(x)$. Men $r_{n-1}(x)$ måste även vara största gemensamma delare för $p(x)$ och $g(x)$ sånär som på en konstant eftersom alla gemensamma delare även måste dela $r(x)$ och då även $r_1(x)$ (ty $g(x) = g_1(x)r(x) + r_1(x)$) och i förlängningen även $r_{n-1}(x)$.

Men $r_{n-3}(x) = g_{n-1}(x)r_{n-2}(x) + r_{n-1}(x)$ kan också skrivas om som $r_{n-1}(x) = r_{n-3}(x) - g_{n-1}(x)r_{n-2}(x)$ och fortsätter vi gå baklänges i Divisionsalgoritmen får vi $r_{n-1}(x) = r_{n-3}(x) - g_{n-1}(x)r_{n-2}(x) = r_{n-3}(x) - g_{n-1}(x)\big(r_{n-4}(x) - g_{n-2}(x)r_{n-3}(x)\big) = -g_{n-1}(x)r_{n-4}(x) + (1 + g_{n-2}(x))r_{n-3}(x)$ och fortsätter vi ända till början får vi tillslut $r_{n-1}(x) = p_0(x)p(x) + g_0(x)g(x)$ för något polynom $p_0(x)$ och $g_0(x)$ och satsen är bevisad.

Det ovan använda sättet att få ut största gemensamma delare genom upprepad användning av Divisionsalgoritmen kallas *Euklides algoritm* och finns beskriven i *Elementa* för heltal (se exempelvis Thompson [6]). Vi ska även formulera detta samband för heltal här då vi kommer att använda den en gång vid ett senare tillfälle. Enligt definitionen för största gemensamma delare av polynom (Definition 1.2.8) ser

vi att denna definition leder till att största gemensamma delaren av alla konstanter är 1, vilket inte är den definitionen vi vanligtvis har för heltal. Vi formulerar därför satsen för heltal på ett sätt som låter oss ha kvar denna definition.

Sats 1.2.10: Låt $a, b \in \mathbb{Z}$ och ej båda vara lika med noll. Då finns $a_0, b_0 \in \mathbb{Z}$ så att $a_0 a + b_0 b = c$ där $c \in \mathbb{Z}$ är det största möjliga heltal där $\frac{a}{c}, \frac{b}{c} \in \mathbb{Z}$.

Bevis: Om $a = 0$ ser vi att $b_0 = 1, c = b$ uppfyller likheten så att satsen gäller och om $b = 0$ ser vi att $a_0 = 1, c = a$ uppfyller likheten så att satsen gäller. Om $a = b$ ser vi att $a_0 = b_0 = \frac{1}{2}$ och $c = a = b$ uppfyller likheten så att satsen gäller.

Om varken a eller b är noll och $a \neq b$ så är beviset i princip samma som för Sats 1.2.9. Först bevisar vi Divisionsalgoritmen för heltal som säger att om $a, b \in \mathbb{Z}$ och $b > 0$ så existerar entydigt bestämda heltal $q, r \in \mathbb{Z}$ så att $a = qb + r$ där $0 \leq r \leq b$. Sedan använder vi denna likhet upprepade gånger tills resten blir noll och arbetar oss sedan tillbaka såsom vi gjorde i beviset i Sats 1.2.9. Till slut får vi att satsen gäller.

Vi fortsätter med ytterligare några satser om polynoms delbarhet.

Sats 1.2.11: Antag att $p(x)$ är irreducibelt över talkroppen K och att $p(x)|q(x)g(x)$. Då måste $p(x)|q(x)$ eller $p(x)|g(x)$.

Följande bevis är taget från Nagell [5]. Antag att $p(x) \nmid q(x)$. Eftersom $p(x)$ är irreducibelt kan $p(x)$ och $q(x)$ då heller inte ha några gemensamma polynom som delar dem annat än konstanter, det vill säga är deras största gemensamma delare 1. Enligt Sats 1.2.9 existerar då $p_1(x)$ och $q_1(x)$ så att $p_1(x)p(x) + q_1(x)q(x) = 1$. Denna likhet kan vi skriva som $q_1(x)q(x) = 1 - p_1(x)\square(x)$. Antar vi på samma sätt att $p(x) \nmid g(x)$ så ser vi att $g_1(x)g(x) = 1 - p_2(x)p(x)$.

Med hjälp av dessa likheter skapar vi nu produkterna $q_1(x)q(x)g_1(x)g(x) = \big(1 - p_1(x)p(x)\big)\big(1 - p_2(x)p(x)\big) \Leftrightarrow q_1(x)g_1(x)q(x)g(x) = 1 - \big(p_1(x) + p_2(x) - p(x)\big)p(x)$. Enligt förutsättningen måste $p(x)$ dela vänsterledet. Men $p(x)$ kan inte dela högerledet eftersom $p(x) \nmid 1$. Alltså har vi en motsägelse och därmed måste något av våra antaganden $p(x) \nmid q(x)$ eller $p(x) \nmid g(x)$ vara felaktigt. Alltså gäller satsen.

Utifrån denna sats kan vi bevisa en annan mycket viktig sats som säger att faktorisering i irreducibla polynom är entydig.

Sats 1.2.12 (Aritmetikens fundamentalsats för polynom över talkroppen *K*): Frånsett ordningen och multiplikation med konstanter kan varje polynom $p(x)$ över

talkroppen K på ett och endast ett sätt skrivas som en produkt av irreducibla polynom i K.

Bevis: Om $p(x)$ är irreducibelt är det uppenbart att satsen stämmer.

Om $p(x)$ är reducibelt så innebär det enligt definitionen för reducibla polynom (Definition 1.2.5) att $p(x)$ kan faktoriseras som en produkt av två andra polynom över talkroppen K. Om dessa polynom inte är irreducibla så är det möjligt att fortsätta faktorisera tills vi får en produkt av enbart irreducibla polynom. Detta är möjligt eftersom faktorerna har lägre grad än produkten och att alla polynom av grad 1 är irreducibla.

Då ska vi även visa entydigheten. Antag därför att $p(x)$ kan faktoriseras på två sätt i irreducibla faktorer på så sätt att $p(x) = q_1(x)q_2(x) \dots q_n(x) = g_1(x)g_2(x) \dots g_m(x)$.

Eftersom $q_1(x)|p(x)$ måste enligt Sats 1.2.11 $q_1(x)$ även dela någon av faktorerna i högerledet. Låt $g_1(x)$ vara denna faktor. Men även $g_1(x)$ är irreducibelt så därför måste $q_1(x) = k_1 g_1(x)$ för någon konstant $k_1 \in K$. Gör nu på samma sätt för alla $q_i(x)$.

Vi ser att $n = m$ ty annars skulle inte båda leden ha samma grad. Därmed har vi visat att $g_1(x)g_2(x) \dots g_m(x) = k_1 k_2 \dots k_n q_1(x)q_2(x) \dots q_n(x)$ alltså att entydigheten är bevisad sånär som på ordningen och multiplikation med konstanter, vilket skulle visas.

En annan följd av Divisionsalgoritmen (Sats 1.2.6) är den så kallade Faktorsatsen.

Sats 1.2.13 (Faktorsatsen): För ett polynom $p(x)$ över talkroppen K gäller att $p(a) = 0$ om och endast om $(x - a)|p(x)$.

Bevis: Om vi vet att $(x - a)|p(x)$ är det uppenbart att $p(a) = 0$ enligt definitionen för delbarhet av polynom (Definition 1.2.4).

I övrigt följer beviset av Divisionsalgoritmen (Sats 1.2.6): Om $g(x) = x - a$ vet vi att det finns entydigt bestämda polynom $q(x)$ och $r(x)$, också över talkroppen K, så att $p(x) = q(x)g(x) + r(x)$. Men vi vet även enligt Divisionsalgoritmen att $r(x)$ har lägre grad än $g(x)$ det vill säga att $r(x) = m$ för något $m \in K$. Eftersom vi vet att $p(a) = g(a) = 0$ så följer att $r(a) = m = 0$ och därmed att $r(x) = 0$. Då har vi visat att $p(x) = q(x)g(x) = (x - a)q(x)$ för ett entydigt $q(x)$ och även att $(x - a)|p(x)$.

Sats 1.2.14: Ett irreducibelt polynom $p(x)$ över talkroppen K av grad > 1 saknar nollställen i K.

Bevis: Antag att polynomet $p(x)$ över talkroppen K har ett nollställe a i K. Enligt Faktorsatsen (Sats 1.2.13) vet vi då att $(x-a)|p(x)$. Enligt definitionen för delbarhet (Definition 1.2.4) vet vi då att $p(x) = (x-a)q(x)$ för något $q(x)$ över K och därmed att $p(x)$ är reducibelt i K.

Alltså är ett polynom $p(x)$ i talkroppen K reducibelt i K om det har minst ett nollställe i K. Alltså kan ett polynom $p(x)$ i talkroppen K inte ha ett nollställe i K om det är irreducibelt i K, vilket skulle visas.

Även om ett polynom över talkroppen K inte har några nollställen i K är det såklart möjligt att polynomet har nollställen som ligger utanför K. Exempelvis kan vi se att polynomet $p(x) = x^2 + 1$ enbart har icke-reella nollställen. Som vi sett kan vi dock skapa en utvidgning som innehåller dessa nollställen.

Definition 1.2.15: Låt $p(x)$ vara ett polynom över talkroppen K. *Sönderfallskroppen till $p(x)$ över K* är då den minsta utvidgade talkroppen $L \supseteq K$ som innehåller alla nollställen till $p(x)$.

Vi inför nu även ett begrepp för när ett tal är ett nollställe till något polynom i en viss talkropp.

Definition 1.2.16: Låt K vara en talkropp. Ett tal $a \in \mathbb{C}$ sägs vara *algebraiskt över K* om det finns ett polynom $p(x) \neq 0$ över talkroppen K sådant att $p(a) = 0$.

Om vi vet att ett tal är ett nollställe till något polynom i en viss talkropp så måste det även finnas ett irreducibelt polynom i den talkroppen med det nollstället. Ty om det finns ett reducibelt polynomet med det nollstället så kan polynomet skrivas som en produkt av irreducibla polynom enligt Aritmetikens fundamentalsats för polynom över talkroppen K (Sats 1.2.12). Men då måste något av dessa irreducibla polynom ha detta nollställe för att produkten ska ha det nollstället.

Definition 1.2.17: Om a är algebraiskt över talkroppen K så säger vi att ett irreducibelt polynom över K med högstagradskoefficienten 1 och nollstället a är minimipolynomet till a över K. Graden av minimipolynomet till a över K betecknas $\deg_K a$.

Vi ska nu visa att detta minimipolynom är entydigt.

Sats 1.2.18: För varje algebraiskt tal a över talkroppen K existerar ett och endast ett minimipolynom till a över K.

Bevis: Enligt definitionen för ett algebraiskt tal (Definition 1.2.16) vet vi att det finns ett polynom över talkroppen K som har nollstället a. Enligt Aritmetikens fundamentalsats för polynom över talkroppen K (Sats 1.2.12) vet vi att detta polynom kan faktoriseras till irreducibla polynom över K. Eftersom a är ett nollställe till produkten av dessa irreducibla polynom måste det även vara ett nollställe till minst ett av de irreducibla polynomen. Ty om $p_1(a)q_1(a) = 0$ för två nollskilda polynom $p_1(x), q_1(x)$ så måste antingen $p_1(a)$ eller $q_1(a)$ vara noll. Alltså vet vi att det finns ett irreducibelt polynom över talkroppen K med nollstället a. Men om det finns ett $p_1(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, där $a_k \in K$, $a_n \neq 0$ och $n \in N \geq 0$ så måste även polynomet $p_2(x) = \frac{a_0}{a_n} + \frac{a_1}{a_n}x + \frac{a_2}{a_n}x^2 + \cdots + x^n$, där $a_k \in K$, $a_n \neq 0$ och $n \in N \geq 0$ existera i talkroppen □ med nollstället a. Därmed måste det även finnas ett irreducibelt polynom över K med högstagradskoefficienten 1 och nollstället a.

Antag nu att $p(x)$ och $q(x)$ är två irreducibla polynom över talkroppen K med nollstället a. Eftersom $p(x)$ och $q(x)$ är irreducibla så måste största gemensamma delaren av $p(x)$ och $q(x)$ över talkroppen K vara antingen 1 eller $b_1p(x) = b_2q(x)$ där $b_1, b_2 \in K$. Enligt Sats 1.2.9 existerar $p_0(x)$ och $g_0(x)$, också över talkroppen K, så att $p_0(x)p(x) + g_0(x)g(x) = d(x)$ där $d(x)$ är största gemensamma delaren till $p(x)$ och $g(x)$ över talkroppen K. Här ser vi att $d(x) \neq 1$ ty annars skulle $p_0(a)p(a) + g_0(a)g(a) = d(a) \Leftrightarrow 0 = 1$, vilket såklart är omöjligt. Alltså måste $d(x) = b_1p(x) = b_2q(x)$ där $b_1, b_2 \in K$ och därmed är $p(x)$ och $q(x)$ multipler av varandra. Samma sak kan enligt samma argument sägas gälla för alla irreducibla polynom över talkroppen K med nollstället a. Eftersom alla irreducibla polynom över K med nollstället a är multipler av varandra innebär det att det endast finns ett irreducibelt polynom över K med högstagradskoefficienten 1 och nollstället a. Alltså är satsen bevisad.

Utifrån dessa begrepp kan vi även formulera en sats kommer vi kommer behöva senare i arbetet.

Sats 1.2.19: Om talet a är algebraiskt över talkroppen K så är $K[a]$ en talkropp.

Bevis: Antag att a är algebraiskt över talkroppen K. Att alla element i $K[a]$ är tal ser vi eftersom dessa kan skrivas på formen $p(a) = k_0 + k_1a + \cdots + k_na^n$ där $k_i \in K$, $n \in \mathbb{N}$ och a är ett algebraiskt tal över talkroppen K. Vi ska även visa att $K[a]$ är sluten under addition, subtraktion, multiplikation och division (med undantaget division med noll). Eftersom alla element i $K[a]$ är polynom i a med koefficienter i K så måste summan, differensen och produkten av element i $K[a]$ också vara polynom i a med koefficienter i K och därmed element i $K[a]$. $K[a]$ är sluten under division om och endast om $\frac{1}{k_0+k_1a+\cdots+k_na^n} \in K[a]$.

Låt nu $g(x)$ vara minimalpolynomet till a över K och $p(x) \neq 0$ vara ett polynom över talkroppen K. Om $deg\ g(x) < 2$ så är det uppenbart att $a \in K$ och därmed att $K[a]$ är en talkropp. Om $deg\ g(x) > 1$ ska vi nu visa att $\frac{1}{p(a)}$ är ett polynom i a över K om $p(a) \neq 0$ och därmed är $K[a]$ slutet under division.

Om $p(x)|g(x)$ så måste antingen $p(x) = k$ eller $p(x) = kg(x)$ för något $k \in K$ eftersom $g(x)$ är irreducibelt. Men om $p(x) = k$ är det självklart att $\frac{1}{p(x)} \in K[x]$ eftersom $\frac{1}{k} \in K$ och i så fall måste även $\frac{1}{p(a)}$ vara ett polynom i a över K. Men om $p(x) = \square g(x)$ så är $p(a) = kg(a) = 0$ och i så fall behöver vi inte kunna uttrycka $\frac{1}{p(a)}$ som ett polynom i a över K för att $K[a]$ ska vara en talkropp. Om $p(x)|g(x)$ så måste alltså $\frac{1}{p(x)} \in K[x]$ och därmed $\frac{1}{p(a)} \in K[a]$ och således $K[a]$ vara talkropp.

Antag därför $p(x) \nmid g(x)$. Enligt Sats 1.2.9 existerar det därför $p_0(x)$ och $g_0(x)$ över K så att $g_0(x)g(x) + p_0(x)p(x) = 1$. Eftersom $g(a) = 0$ så är $p_0(a)p(a) = 1 \Leftrightarrow \frac{1}{p(a)} = p_0(a)$ och således måste $\frac{1}{p(a)}$ vara ett polynom i a över K. Alltså är $K[a]$ slutet under division och därmed är $K[a]$ en talkropp, vilket skulle visas.

Sats 1.2.20: Låt a vara ett algebraiskt tal över talkroppen K och låt $K[a]$ vara den utvidgning av K som består av alla polynom i a med koefficienter i K. Då gäller att $[K[a]: K] = \deg_K a$.

Bevis: Låt $g(x)$ vara minimalpolynomet till a över K och låt $p(x)$ vara ett polynom över talkroppen K med graden $n \geq \deg g(x) = \deg_K a = m$. Enligt Divisionsalgoritmen (Sats 1.2.6) finns det då entydigt bestämda polynom $q(x)$ och $r(x)$, också över talkroppen K, sådana att $p(x) = q(x)g(x) + r(x)$ där graden av $r(x)$ är lägre än graden av $g(x)$. Eftersom $g(a) = 0$ så måste $p(a) = r(a)$. Eftersom $\deg r < \deg g$ så måste $r(a) = r_0 + r_1 a + \cdots + r_{m-1}a^{m-1} = p(a)$ för några $r_i \in K$ och därmed måste $1, a, a^2, \dots, a^{m-1}$ generera $K[a]$. Dessa generatorer är linjärt oberoende eftersom det inte finns $k_0 + k_1 a + \cdots + k_{m-1}a^{m-1} = 0$ där $k_i \in K$ ty denna ekvation har grad $m - 1$ och vi vet att minimalpolynomet till a över K har grad m. Eftersom $1, a, a^2, \dots, a^{m-1}$ är en bas för $K[a]$ över K innebär det att $[K[a]: K] = m = \deg_K a$, vilket skulle visas.

Sats 1.2.21: Låt $p(x)$ vara ett irreducibelt polynom av grad n över talkroppen K där n är ett primtal. Låt $L \supseteq K$ vara en utvidgning av K sådant att $p(x)$ är reducibelt i talkroppen L. Då gäller att $n|[L: K]$. Om även $[L: K]$ är ett primtal, så är $[L: K] = n$.

Bevis: Låt a vara ett nollställe till $p(x)$ samt $L[a]$ och $K[a]$ vara de talkroppar som utvidgats med alla polynom av a med koefficienter i L respektive K.

Enligt Sats 1.1.12 är $[L[a]:L][L:K] = [L[a]:K] = [L[a]:K[a]][K[a]:K]$. Men enligt Sats 1.2.20 är $[K[a]:K] = \deg_K a$ och eftersom $p(x)$ är irreducibelt över K så är $\deg_K a = \deg p(x) = n$. Alltså är $[L[a]:K[a]][K[a]:K] = n[L[a]:K[a]]$. Eftersom $p(x)$ är reducibelt i L så gäller att $[L[a]:L] < n$. Då ser vi att eftersom $[L[a]:L][L:K] = n[L[a]:K[a]]$ och $[L[a]:L] < n$ så måste $n|[L:K]$, vilket skulle visas.

Vi har nu definierat en mängd begrepp för polynom och bevisat ett antal egenskaper hos olika typer av polynom. Vi ska nu gå vidare till algebraiska ekvationer, vilka vi ska definiera huvudsakligen utifrån begrepp vi redan infört om polynom.

1.3 Ekvationer av grad ett till fyra samt historisk bakgrund

Vi har tidigare skrivit att vi i detta arbete är intresserade av att undersöka huruvida femtegradsekvationen generellt är lösbar med radikaler. Vad är då en femtegradsekvation och vad innebär det att den är lösbar med radikaler? Vi kommer börja detta delkapitel med att ge en kort historik bakgrund till ekvationer och deras tillämpning samt aktualitet inom det svenska skolväsendet. Vi kommer sedan definiera begreppet ekvation utifrån begreppet polynom och några få egenskaper hos ekvationer för att slutligen ange lösningsformlerna för ekvationer i en variabel av första, andra, tredje och fjärde graden.

Före 1600-talet var den matematik som utvecklades huvudsakligen retorisk och inte symbolisk (se exempelvis Thompson [6]) och därmed var algebran som matematiskt område outvecklat. Dock löste matematiker det vi idag skulle relatera till som ekvationer på andra sätt, bland annat inom geometrin. Idag saknas tillräckliga källor för att veta exakt hur matematiken började utvecklas men det är däremot känt att flera tidiga kulturer hade metoder för att lösa förstagradsekvationer och vissa andragradsekvationer även om de saknade det symboliska språk som vi använder idag. Exempelvis löste babylonierna vissa andragradsproblem inom geometri och handel omkring 3200 år före vår tideräknings början (Thompson [6]). Metoder för att lösa olika tredjegradsekvationer utvecklades under 1000-talet av den arabiske matematikern Omar Khayyam genom studiet av kägelsnitt men de generella lösningarna skulle dröja, dels eftersom symbolspråket saknades och dels på grund av en ovillighet att införa negativa tal. Den generella lösningen av tredjegradsekvationen konstruerades så vitt vi vet först av Scipione del Ferro och av fjärdegradsekvationen av Lodovico Ferrari; båda lösningarna publicerades i *Ars Magna* av Girolamo Cardano 1545 (Nagell [5]).

Historiskt sett så har formell utbildning och studier varit något som endast en liten del av världens befolkning haft tillgång till, oftast då i form av hemundervisning eller

särskilda läroverk för samhällets övre skikt. I Sverige lagstadgades 1686 för första gången att det var föräldrars och husbönders plikt att lära barn att läsa och att kyrkan hade en plikt att kontrollera detta genom husförhör (se exempelvis Hartman [2]). Räkning blev obligatoriskt kunskapsområde för Sveriges befolkning i och med folkskolans införande 1842 och sedan dess har matematikinnehållet i det obligatoriska skolväsendet kontinuerligt ökat. I undervisningsplanen för folkskolan 1955 införs i ämnet matematik i sjunde klass ”[e]nkla sifferekvationer med en obekant jämte tillämpningar” (Skolöverstyrelsen [9, s. 123]). I vår nuvarande läroplan för grundskolan från 2011 står algebra med som ett centralt innehåll i alla årskurser. För årskurs 7-9 är innehållet i algebra:

> *Algebra*
> - Innebörden av variabelbegreppet och dess användning i algebraiska uttryck, formler och ekvationer.
> - Algebraiska uttryck, formler och ekvationer i situationer som är relevanta för eleven.
> - Metoder för ekvationslösning.
>
> Skolverket [7, s. 51]

På gymnasienivå införs algebraiska lösningar av andragradsekvationer i Matematik 2 och för vissa ekvationer av högre grad i Matematik 3 (se Skolverket [8]). Ekvationer och metoder för att lösa dessa är alltså något som alla elever i dagens grund- och gymnasieskola kommer möta och även något som alla matematiklärare således kommer undervisa i.

Låt oss nu gå in närmare på ekvationer och definiera några nyckelbegrepp för en speciell typ av ekvationer.

Definition 1.3.1: En *algebraisk ekvation* är en ekvation som kan skrivas på formen $p(x) = 0$ där $p(x)$ är ett polynom.

Vi kommer hädanefter mena algebraiskt ekvation även när vi enbart skriver ekvation, trots att det även finns andra typer av ekvationer såsom exempelvis exponentialekvationer. Vi kommer i fortsättningen även främst intressera oss för ekvationer med endast en variabel. Vi fortsätter nu att definiera vad som menas med graden av en algebraisk ekvation.

Definition 1.3.2: Om $p(x)$ är ett polynom i variabeln x av graden $n \geq 1$, sägs ekvationen $p(x) = 0$ vara en algebraisk ekvation av *graden* n.

Vi fortsätter nu med att definiera vad som menas med en ekvations lösningar och att en ekvation är lösbar.

Definition 1.3.3: För en algebraisk ekvation $p(x) = 0$ sägs alla värden på x som uppfyller att $p(x) = 0$ vara *lösningar* till ekvationen.

Att en ekvation är lösbar med en viss metod innebär att metoden alltid genererar alla lösningar till ekvationen. Vi ska nu definiera vad som menas med att en ekvation är lösbar med radikaler.

Definition 1.3.4: En algebraisk ekvation $p(x) = 0$ där $p(x)$ är ett polynom är *lösbar med radikaler* om och endast om alla lösningar går att beräkna utifrån ändliga kombinationer av polynomets koefficienter genom de fyra räknesätten och rotdragningar.

Låt oss nu diskutera vad som menas med en generell lösningsformel. Det finns ingen matematisk definition av vad en generell lösningsformel är. Detta på grund av att begreppet huvudsakligen införs av didaktiska anledningar och inte matematiska. Inom gymnasieskolan används begreppet oftast om en formel som kan beräkna lösningarna till en ekvation genom insättning av värdena av ekvationens koefficienter.

Här ska nu göras ett försök till en mer tydlig förklaring av vad som kommer menas med generell lösningsformel i resten av uppsatsen. Detta kommer sedan exemplifieras med lösningsformlerna för ekvationer av grad ett till fyra.

Om alla nollställen till ett polynom $p(x)$ går att uttrycka i polynomets koefficienter genom ett ändligt antal algebraiska operationer säger vi att det existerar en generell lösningsformel till den algebraiska ekvationen $p(x) = 0$.

Låt nu $p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$, där $c_i \in \mathbb{C}$ och $n \in \mathbb{N}, n \geq 1$, ha de n nollställena $x_1, x_2, \dots, x_n$ (i delkapitel 2.1 ska vi visa att detta gäller för alla polynom). Om dessa nollställen kan beräknas med samma ekvationssystem $\begin{cases} x_1 = u_1(c_0, c_1, \dots, c_n) \\ x_2 = u_2(c_0, c_1, \dots, c_n) \\ \dots \\ x_n = u_n(c_0, c_1, \dots, c_n) \end{cases}$, där $u_1(c_0, c_1, \dots, c_n)$ är ett algebraiskt uttryck med ett ändligt antal algebraiska operationer, oavsett värdena på $c_0, c_1, \dots, c_n$ så sägs detta ekvationssystem vara den generella lösningsformeln till n:tegradsekvationen. Exempelvis kan lösningsformlerna för ekvationer av första, andra och tredje graden formuleras på detta sätt.

Om istället alla polynom $p(x)$ av grad n kan delas upp i ett ändligt antal grupper $p_1[x], p_2[x], \dots, p_m[x]$ beroende av polynomens koefficienter där alla nollställen till varje polynom i samma grupp kan beräknas med samma ekvationssystem $\begin{cases} x_1 = u_1(c_0, c_1, \dots, c_n) \\ x_2 = u_2(c_0, c_1, \dots, c_n) \\ \dots \\ x_n = u_n(c_0, c_1, \dots, c_n) \end{cases}$, där $u_1(c_0, c_1, \dots, c_n)$ är ett algebraiskt uttryck med ett ändligt antal algebraiska operationer, oavsett värdena på $c_0, c_1, \dots, c_n$ så sägs systemet

$$\begin{cases} \text{Om } p(x)\in p_1[x] \text{ så är } \begin{cases} x_1=u_{1,1}(c_0,c_1,\dots,c_n) \\ x_2=u_{2,1}(c_0,c_1,\dots,c_n) \\ \dots \\ x_n=u_{n,1}(c_0,c_1,\dots,c_n) \end{cases} \\ \text{Om } p(x)\in p_2[x] \text{ så är } \begin{cases} x_1=u_{1,2}(c_0,c_1,\dots,c_n) \\ x_2=u_{2,2}(c_0,c_1,\dots,c_n) \\ \dots \\ x_n=u_{n,2}(c_0,c_1,\dots,c_n) \end{cases} \\ \dots \\ \text{Om } p(x)\in p_m[x] \text{ så är } \begin{cases} x_1=u_{1,m}(c_0,c_1,\dots,c_n) \\ x_2=u_{2,m}(c_0,c_1,\dots,c_n) \\ \dots \\ x_n=u_{n,m}(c_0,c_1,\dots,c_n) \end{cases} \end{cases}$$ vara den generella lösningsformeln till n:tegradsekvationen. Exempelvis kan lösningsformeln för ekvationer av fjärde graden formuleras på detta sätt.

Om och endast om alla algebraiska ekvationer av en viss grad är lösbara med radikaler är det möjligt att konstruera generell lösningsformel för ekvationer av denna grad. Låt oss därför gå in närmare på ekvationer av första, andra, tredje och fjärde graden och visa att dessa är lösbara med radikaler samt hur de generella lösningsformlerna för dessa ser ut.

Definition 1.3.1: En *förstagradsekvation* är en algebraisk ekvation som kan skrivas på formen $kx + m = 0$, där $k, m \in \mathbb{C}$ och $k \neq 0$.

Sats 1.3.2: Lösningen till förstagradsekvationen $kx + m = 0$ ges av $x = -\frac{m}{k}$ och ger alltid en och endast en lösning.

Beviset är trivialt eftersom $kx + m = 0 \Leftrightarrow x = -\frac{m}{k}$.

Exempel: Förstagradsekvationen $2x - 4 = 0$ har lösningen $x = 2$.

Om vi betraktar en förstagradsekvation $kx + m = 0$ och $k, m \in K$ för någon talkropp K så ser vi även att lösningen till ekvationen också måste tillhöra K, eftersom lösningen kan skrivas som en kvot av två element i K. Förstagradsekvationens lösning ligger alltså alltid i samma talkropp som koefficienterna till ekvationen.

Definition 1.3.3: En *andragradsekvation* är en algebraisk ekvation som kan skrivas på formen $x^2 + px + q = 0$, där $p, q \in \mathbb{C}$.

Sats 1.3.4 (Rotformeln): Lösningarna till andragradsekvationen $x^2 + px + q = 0$ ges av $x = -\frac{p}{2} \pm \sqrt{(\frac{p}{2})^2 - q}$.

Bevis: Antag att $x^2 + px + q = 0$. Adderar vi $(\frac{p}{2})^2 - q$ till ekvationen får vi $x^2 + px + (\frac{p}{2})^2 = (\frac{p}{2})^2 - q$. Vänsterledet kan vi nu skriva om med första kvadreringsregeln och får således $(x + \frac{p}{2})^2 = (\frac{p}{2})^2 - q$. Genom rotutdragning får vi att $x + \frac{p}{2} =$

$\pm\sqrt{(\frac{p}{2})^2-q}$ och genom att subtrahera $\frac{p}{2}$ får vi slutligen $x=-\frac{p}{2}\pm\sqrt{(\frac{p}{2})^2-q}$. Om $(\frac{p}{2})^2-q$ inte är ett positivt reellt tal så är inte $\sqrt{(\frac{p}{2})^2-q}$ entydigt. Dock ser vi att om vi väljer en av de två lösningarna till ekvationen $y^2=(\frac{p}{2})^2-q$ att vara $\sqrt{(\frac{p}{2})^2-q}$ så kommer den andra lösningen att ges av $-\sqrt{(\frac{p}{2})^2-q}$. Därmed kommer även $x=-\frac{p}{2}\pm\sqrt{(\frac{p}{2})^2-q}$ att ge båda lösningarna till ekvationen $x^2+px+q=0$ oavsett vilken av de möjliga värdena vi sätter som $\sqrt{(\frac{p}{2})^2-q}$. Alltså är satsen bevisad.

Exempel: Andragradsekvationen $x^2-3x+2=0$ har lösningarna $x_1=1$ och $x_2=2$ ty $x_1=-\frac{(-3)}{2}-\sqrt{\left(\frac{(-3)}{2}\right)^2-2}=1$ och $x_2=-\frac{(-3)}{2}+\sqrt{\left(\frac{(-3)}{2}\right)^2-2}=2$.

Betraktar vi en andragradsekvation $x^2+px+q=0$ där $p,q\in K$ för någon talkropp K så ser vi att lösningarna inte nödvändigtvis också ligger i K. Exempelvis är det möjligt att en reell andragradsekvation endast har komplexa lösningar. Från lösningsformeln ser vi att lösningarna endast ligger i samma talkropp som ekvationen om $\sqrt{(\frac{p}{2})^2-q}\in K$. En reell andragradsekvation har antingen en (dubbel) reell lösning, två olika reella lösningar eller två olika komplexa (icke-reella) lösningar.

Definition 1.3.5: En *tredjegradsekvation* är en algebraisk ekvation som kan skrivas på formen $x^3+ax^2+bx+c=0$, där $a,b,c\in\mathbb{C}$.

Sats 1.3.6 (Cardanos formel): Lösningarna till tredjegradsekvationen $x^3+ax^2+bx+c=0$ ges av:

$$x=\begin{cases} x_1=-\frac{a}{3}+u+v \\ x_{2,3}=-\frac{a}{3}-\frac{1}{2}(u+v)\pm\frac{\sqrt{3}}{2}(u-v)i \end{cases}$$

$$\text{där } u=\sqrt[3]{\frac{\frac{9ab-2a^3}{27}-c}{2}+\sqrt{\frac{(\frac{9ab-2a^3}{27}-c)^2}{4}+\frac{(b-\frac{a^2}{3})^3}{27}}} \quad v=\sqrt[3]{\frac{\frac{9ab-2a^3}{27}-c}{2}-\sqrt{\frac{\left(\frac{9ab-2a^3}{27}-c\right)^2}{4}+\frac{\left(b-\frac{a^2}{3}\right)^3}{27}}}$$

Bevis: Vi kommer här inte använda oss av det bevis om Cardano gav då det numera finns andra bevis som är något enklare. Istället ger vi ett snarlikt bevis som ursprungligen kommer från François Viète, publicerat postumt 1615.

Antag att $x^3 + ax^2 + bx + c = 0$. Genom variabelsubstitutionen $x = z - \frac{a}{3}$ skriver vi om tredjegradsekvationen till $(z - \frac{a}{3})^3 + a(z - \frac{a}{3})^2 + b(z - \frac{a}{3}) + c = 0 \Leftrightarrow z^3 + \left(b - \frac{a^2}{3}\right)z + \left(c + \frac{2a^3 - 9ab}{27}\right) = 0$. Genom att införa $p = b - \frac{a^2}{3}$ och $q = c + \frac{2a^3 - 9ab}{27}$ har vi således skrivit om den ursprungliga tredjegradsekvationen till den komprimerade formen $z^3 + pz + q = 0$.

Genom det ytterligare variabelbytet $z = w - \frac{p}{3w}$ skriver vi om den komprimerade tredjegradsekvationen till $(w - \frac{p}{3w})^3 + p(w - \frac{p}{3w}) + q = 0 \Leftrightarrow w^3 + q - \frac{p^3}{27w^3} = 0$. Vi multiplicerar nu denna ekvation med w^3 och får således $w^6 + qw^3 - \frac{p^3}{27} = 0$, vilket är en andragradsekvation i w^3. Enligt Rotformeln (Sats 1.3.4) är alltså $w^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. Inför nu $\alpha = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ och $\beta = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ så $w_1^3 = \alpha$ och $w_2^3 = \beta$.

Låt oss börja med att betrakta tredjegradsekvationen $w_1^3 = \alpha$. Vi skriver om denna som $w_1^3 - \alpha = 0$ och låter $w_{1,a} = \sqrt[3]{\alpha}$ vara en av de tre lösningarna. Därmed vet vi enligt Faktorsatsen (Sats 1.2.13) att $w_1 - \sqrt[3]{\alpha} | w_1^3 - \alpha$ och att vi därmed kan faktorisera $w_1^3 - \alpha$. Gör vi detta i ekvationen $w_1^3 - \alpha = 0$ får vi $(w_1 - \sqrt[3]{\alpha})(w_1^2 + w_1\sqrt[3]{\alpha} + (\sqrt[3]{\alpha})^2) = 0$. Använder vi Rotformeln (Sats 1.3.4) för den högra parentesen får vi således att $w_{1,b} = \sqrt[3]{\alpha}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ och $w_{1,c} = \sqrt[3]{\alpha}(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$. På samma sätt får vi att $w_{2,a} = \sqrt[3]{\beta}$, $w_{2,b} = \sqrt[3]{\beta}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ och $w_{2,c} = \sqrt[3]{\beta}(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$.

Låt oss införa $u = \sqrt[3]{\alpha} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ och $v = \sqrt[3]{\beta} = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$. Vi antar nu att lösningarna $w \neq 0$ och återgår från variabeln w till variabeln z genom att sätta in lösningarna för w i $z = w - \frac{p}{3w}$. Efter en del förenkling ser vi att $z_{1,a} = z_{2,a} = u + v$, att $z_{1,b} = z_{2,b} = -\frac{1}{2}(u + v) + \frac{\sqrt{3}}{2}(u - v)i$ och att $z_{1,c} = z_{2,c} = -\frac{1}{2}(u + v) - \frac{\sqrt{3}}{2}(u - v)i$. Vi har alltså fått tre lösningar i z. Vi ser även att vi får samma nollställen även om antingen $w_{1,a} = w_{1,b} = w_{1,c} = 0$ eller $w_{2,a} = w_{2,b} = w_{2,c} = 0$. Om $w_{1,a} = w_{1,b} = w_{1,c} = w_{2,a} = w_{2,b} = w_{2,c} = 0$ måste även $p = q = 0$ och så fall gäller även lösningarna men att de alla är lika med 0.

Återgår vi nu till variabeln x genom insättning $x = z - \frac{a}{3}$ och använder att $p = b - \frac{a^2}{3}$ och $q = c + \frac{2a^3 - 9ab}{27}$ får vi återigen efter en del räkning till slut

$$x=\begin{cases} x_1=-\frac{a}{3}+u+v \\ x_{2,3}=-\frac{a}{3}-\frac{1}{2}(u+v)\pm\frac{\sqrt{3}}{2}(u-v)i \end{cases}$$

$$där\ u=\sqrt[3]{\frac{\frac{9ab-2a^3}{27}-c}{2}+\sqrt{\frac{\left(\frac{9ab-2a^3}{27}-c\right)^2}{4}+\frac{(b-\frac{a^2}{3})^3}{27}}}\quad v=\sqrt[3]{\frac{\frac{9ab-2a^3}{27}-c}{2}-\sqrt{\frac{\left(\frac{9ab-2a^3}{27}-c\right)^2}{4}+\frac{\left(b-\frac{a^2}{3}\right)^3}{27}}}$$

vilket skulle visas.

Exempel: Tredjegradsekvationen $x^3-4x^2+9x-10=0$ har lösningarna $x_1=2$ och $x_{2,3}=1\pm 2i$.

Om vi betraktar en tredjegradsekvation $x^3+ax^2+bx+c=0$ och $a,b,c\in K$ för någon talkropp K så ser vi liknande andragradsekvationen att lösningarna inte nödvändigtvis ligger i K. En reell tredjegradsekvationen kan antingen ha en (trippel) reell lösning, två olika (varav en dubbel) reella lösningar, tre olika reella lösningar eller en reell och två olika komplexa (icke-reella) lösningar, vilket kommer visas i delkapitel 2.1.

Definition 1.3.7: En *fjärdegradsekvation* är en algebraisk ekvation som kan skrivas på formen $x^4+ax^3+bx^2+cx+d=0$, där $a,b,c,d\in\mathbb{C}$.

Sats 1.3.8 (Ferraris modell): Lösningarna till fjärdegradsekvationen $x^4+ax^3+bx^2+cx+d=0$ ges av:

$$x=-\frac{1}{4}a+\pm_s\frac{1}{2}\sqrt{-\frac{3}{8}a^2+b+2y}\pm_t\frac{1}{2}\sqrt{\frac{9}{8}a^2-3b-2y\mp_s\frac{\frac{1}{4}a^3-ab+2c}{\sqrt{-\frac{3}{8}a^2+b+2y}}}$$

$$\text{där } y=\begin{cases} U+\frac{15a^2}{48}-\frac{5}{6}b-\frac{-\frac{1}{12}\left(-\frac{3a^2}{8}+b\right)^2+\frac{3a^4}{256}-\frac{a^2b}{16}+\frac{ac}{4}-d}{3U} & \text{om } U\neq 0 \\ \frac{15a^2}{48}-\frac{5}{6}b-\sqrt[3]{\frac{(\frac{3a^2}{8}-b)^3}{108}+\frac{(\frac{3a^2}{8}-b)(\frac{3a^4}{256}-\frac{a^2b}{16}+\frac{ac}{4}-d)}{3}-\frac{(\frac{a^3}{8}+\frac{ab}{2}+c)^2}{8}} & \text{om } U=0 \end{cases}$$

$$\text{och } U=\sqrt[3]{-\frac{1}{2}Q\pm\sqrt{\frac{1}{4}Q^2+-\frac{1}{324}\left(\frac{3a^2}{8}-b\right)^2+\frac{1}{27}(\frac{3a^4}{256}-\frac{a^2b}{16}+\frac{ac}{4}-d)^3}}$$

$$\text{och } Q=-\frac{1}{108}(-\frac{3}{8}+b)^3+\frac{1}{3}(-\frac{3a^2}{8}+b)(-\frac{3a^4}{256}+\frac{a^2b}{16}-\frac{ac}{4}+d)-\frac{1}{8}(\frac{a^3}{8}+\frac{ab}{2}+c)^2$$

För samtliga lösningar, beräkna x med samtliga kombinationer av addition och subtraktion för $\pm_s$ och $\pm_t$. Observera att $\pm_s$ och $\mp_s$ måste ha motsatt tecken medan $\pm_t$ är oberende av de andra två.

Beviset för lösningsformeln för algebraiska ekvationer av fjärde graden bygger på liknande principer som för Cardanos formel (Sats 1.3.6) men eftersom det är något mer omständligt hänvisas läsaren till exempelvis Nagell [5].

Exempel: Fjärdegradsekvationen $x^4 + 2x^3 - 2x^2 + 2x - 3 = 0$ har lösningarna $x_1 = 1$ och $x_2 = -3$ och $x_{3,4} = \pm i$.

Om vi betraktar en fjärdegradsekvation $x^4 + ax^3 + bx^2 + cx + d = 0$ och $a, b, c, d \in K$ för någon talkropp K så ser vi liknande andra- och tredjegradsekvationen att lösningarna inte nödvändigtvis ligger i K. En reell fjärdegradsekvation kan ge antingen en (kvadrupel) reell lösning, två olika (varav en trippel *eller* två dubbla) reella lösningar, tre olika (varav en dubbel) reella lösningar, fyra olika reella lösningar, två olika (dubbla) komplexa (icke-reella) lösningar, fyra olika komplexa (icke-reella) lösningar, en (dubbel) reell och två olika komplexa (icke-reella) lösningar eller två olika reella och två olika komplexa (icke-reella) lösningar, vilket kommer visas i delkapitel 2.1.

Efter att de generella lösningsformlerna för tredje- och fjärdegradsekvationen konstruerades i tät följd efter algebrans utveckling jobbade matematiker länge på att hitta en generell lösningsformel även för femtegradsekvationen. Dock visade Niels Henrik Abel 1824 att femtegradsekvationen inte generellt är lösbar med radikaler och att det därför inte är möjligt att konstruera en sådan. Abels sats för detta ska vi bevisa i delkapitel 2.2.

2 Femtegradsekvationen

I detta kapitel kommer vi fokusera på femtegradsekvationen och undersöka denna genom den allmänna algebraiska teori som presenterades i kapitel 1. Vi kommer börja med att undersöka hur många lösningar femtegradsekvationen har och om dessa är reella eller icke-reella, för att sedan ta reda på om femtegradsekvationen generellt är lösbar med radikaler eller inte. Till slut kommer vi kortfattat att diskutera innebörden av detta.

2.1 Femtegradsekvationens lösningar

I tidigare kapitel hävdade vi att förstagradsekvationen alltid har en lösning men att andra-, tredje- och fjärdegradsekvationen kan ha olika antal skilda lösningar beroende på ekvationernas koefficienter och att dessa kan vara reella eller komplexa (icke-reella). I detta delkapitel kommer vi undersöka hur många olika lösningar femtegradsekvationen har och huruvida dessa lösningar är reella eller komplexa. Vi kommer till slut visa att reella femtegradsekvationer kan ha ett till fem olika nollställen i $\mathbb{C}$, varav minst ett ligger i $\mathbb{R}$.

Vi kommer börja med att undersöka det allmänna fallet, det vill säga hur många rötter det finns för en algebraisk ekvation av en variabel av graden n. Som vi visat tidigare är detta ekvivalent med att undersöka hur många nollställen som finns till ett polynom av en variabel av graden n. Vi ska börja med att utgå från att alla polynom av minst grad ett har minst ett nollställe i $\mathbb{C}$.

Sats 2.1.1 (Algebrans fundamentalsats): Ett polynom $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ av graden $n \in N$ där $n \geq 1$ med koefficienter $a_i \in \mathbb{C}$ har minst ett nollställe x i $\mathbb{C}$.

Denna sats bevisades först av Gauss 1799 men finns också i exempelvis Nagell [5]. Vi kommer dock inte ta upp beviset här eftersom det inte är uteslutande algebraiskt utan även använder begrepp och satser från matematisk analys.

Nu när vi vet att alla polynom har minst ett nollställe i $\mathbb{C}$ kan vi med hjälp av Faktorsatsen (Sats 1.2.13) faktorisera polynom i polynom av lägre grad.

Sats 2.1.2: Ett polynom $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ av graden $n \in N \geq 1$ med komplexa koefficienter $a_i \in \mathbb{C}$ kan på ett entydigt sätt sånär som på ordningen skrivas på formen $p(x) = a_n(x - c_1)(x - c_2) \ldots (x - c_n)$ där talen $c_1, c_2, \ldots, c_n \in \mathbb{C}$ är nollställen till $p(x)$.

Bevis: Vi kommer bevisa detta med ett induktionsbevis. Om $n = 1$ är så är $p(x) = kx + m = k(x - (-\frac{m}{k}))$ så är $x = -\frac{m}{k}$ enda nollstället och satsen stämmer då $k, m \in \mathbb{C}$.

Vi ska nu visa att satsen även gäller för ett polynom $p(x)$ av graden n om vi vet att det gäller för ett polynom av graden $n - 1$.

Låt oss anta att satsen stämmen för ett polynom av graden $n - 1$. Genom Algebrans fundamentalsats (Sats 2.1.1) vet vi att polynomet $p(x)$ har minst ett nollställe $c_n \in \mathbb{C}$ och genom Faktorsatsen (Sats 1.2.13) vet vi att vi kan faktorisera polynomet enligt $p(x) = q(x)(x - c_n)$. Om vi nu betraktar $q(x)$ så ser vi att det är ett polynom av graden $n - 1$. Alltså är $q(x) = a_n(x - c_1)(x - c_2) \dots (x - c_{n-1})$ och därmed är $p(x) = (x - c_1)(x - c_2) \dots (x - c_{n-1})\,(x - c_n)$. Alltså är induktionsbeviset klart.

Att detta kan ske på ett entydigt sätt följer av Aritmetikens fundamentalsats för polynom över K (Sats 1.2.12), alltså är satsen bevisad.

Utifrån Sats 2.1.2 är det tydligt att ett polynom av graden n har exakt n stycken rötter. Vi kan även se hur många *olika* nollställen ett polynom av en vissa grad kan ha eftersom vissa av dessa kan vara lika.

Sats 2.1.3: Ett polynom av en variabel av graden $n \in N \geq 1$ har minst 1 och högst n olika nollställen i $\mathbb{C}$.

Från faktoriseringen av polynom i Sats 2.1.2 ser vi att ett polynom av graden n har exakt n stycken rötter. Dock kan vissa av dessa rötter sammanfalla om flera av talen c_i är lika. Om inga av talen c_i sammanfaller har polynomet n *distinkta* (olika) nollställen medan polynomet endast har ett distinkt nollställe om alla talen c_i sammanfaller. För varje m så att $1 \leq m \leq n$ finns det alltså även polynom med graden n som har m distinkta nollställen.

Om ett polynom har ett antal distinkta nollställen som är lägre än dess grad betyder detta att något nollställe skulle förekomma flera gånger vid en faktorisering av polynomet såsom i Sats 2.1.2. Antalet gånger som varje lösning förekommer i en sådan faktorisering kallar vi dess multiplicitet.

Definition 2.1.4: Om polynomet $p(x) = a_n(x - c_1)(x - c_2) \dots (x - c_{n-1})\,(x - c_n)$ där koefficienten $a_n \neq 0$, nollställena $c_i \in \mathbb{C}$ och faktoriseringen av $p(x)$ innehåller faktorn $x - c$ för något $c = c_i$ exakt m gånger, säger vi, att nollstället c har *multipliciteten* m.

Exempelvis kan vi se att polynomet $p(x) = x^2 - 4x + 4$ har nollstället $x = 2$ med multipliciteten två eftersom $p(x) = x^2 - 4x + 4 = (x - 2)^2$.

Sats 2.1.5: Ett irreducibelt polynom har endast distinkta nollställen.

Detta bevis använder några begrepp och satser från matematisk analys men då dessa ingår i gymnasieskolans matematikkurser kommer dessa användas här utan att definieras.

Bevis: Antag att polynomet $p(x)$ över K har ett nollställe a med multipliciteten $m \in \mathbb{N}, m > 1$ i någon utvidgning $L \supseteq K$. Alltså är $p(x) = (x-a)^m q(x)$ för något nollskilt polynom $q(x)$ över L.

Deriverar vi nu $p(x)$ får vi $p'(x) = m(x-a)^{m-1}q(x) + (x-a)^m q'(x) = (x-a)^{m-1}(mq(x) + (x-a)q'(x))$. Eftersom $m > 1$ så ser vi att a är ett nollställe till $p'(x)$. Eftersom $p'(x)$ är derivatan för ett polynom över K så är även $p'(x)$ ett polynom över K.

Enligt Sats 1.2.9 finns det två polynom $p_0(x)$ och ${p_0}'(x)$, också över talkroppen K, så att $p_0(x)p(x) + {p_0}'(x)p'(x) = d(x)$ där $d(x)$ är största gemensamma delaren till $p(x)$ och $g(x)$ över talkroppen K. Eftersom $p(a) = 0$ och $p'(a) = 0$ så måste även $d(a) = 0$ men eftersom $d(x) \neq 0$ så måste $deg\, d(x) \geq 1$. Alltså är $d(x)$ ett polynom över K med graden större än noll. Men graden av $d(x)$ måste vara mindre än graden av $p(x)$ eftersom $d(x) | p'(x)$. Eftersom $d(x) | p(x)$ så är därmed $p(x)$ reducibelt över K.

Alltså har vi visat att om ett polynom har multipla nollställen så är det alltid reducibelt. Därmed innebär att ett irreducibelt polynom inte kan ha multipla nollställen. Ett irreducibelt polynom har således enbart distinkta nollställen, vilket skulle visas.

Av Sats 2.1.3 följer att ett femtegradspolynom i en variabel har minst ett och max fem olika nollställen i $\mathbb{C}$. Vi ska nu visa en egenskap för de komplexa (icke-reella) nollställena (alltså de nollställen i $\mathbb{C}$ som ej ligger i $\mathbb{R}$) till reella polynom, nämligen att de alltid kommer i par.

Sats 2.1.6: Om ett reellt polynom av en variabel har det komplexa nollstället $\xi + \eta i$, där $\xi, \eta \in \mathbb{R}$ så har polynomet även nollstället $\xi - \eta i$. Nollställena $\xi + \eta i$ och $\xi - \eta i$ har samma multiplicitet.

Följande bevis är hämtat från Nagell [5]. Låt $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ vara ett reellt polynom av variabeln x av graden n med nollstället $\xi + \eta i$, där $\xi, \eta \in \mathbb{R}$.

Inför variabelbytet $x = a + bi$ och $a, b \in \mathbb{R}$. Då gäller att $p(x) = p(a,b) = q(a,b) + ir(a,b)$ där $q(a,b)$ och $r(a,b)$ är reella polynom av de reella variablerna a och □.

Eftersom alla potenser $(bi)^c$ där c är ett jämnt heltal ger $(bi)^c = \pm b^c$ så kommer alla jämna potenser av b att ingå i $q(a,b)$. På samma sätt kommer alla udda potenser av b att ingå i $r(a,b)$ eftersom alla potenser $(bi)^d$ där d är ett udda heltal ger $(bi)^d = \pm b^d i$.

Alltså innehåller polynomet $q(a,b)$ endast jämna potenser av b och polynomet $r(a,b)$ innehåller endast udda potenser av b. Därmed gäller att $q(a,-b) = q(a,b)$ och att $r(a,-b) = -r(a,b)$.

Om $x = \xi + \eta i$ är en rot till $p(x)$ så måste även för $p(a,b)$ gälla att $p(\xi,\eta) = 0$. Alltså måste $q(\xi,\eta) + ir(\xi,\eta) = 0$ och därmed även $q(\xi,\eta) = r(\xi,\eta) = 0$. Därmed även $q(\xi,-\eta) = r(\xi,-\eta) = 0$ och alltså är även $p(\xi,-\eta) = 0$. Således är $p(\xi - \eta i) = 0$ och alltså har vi visat att $\xi - \eta i$ är ett nollställe för $p(x)$.

Nu ska vi även visa att dessa nollställen har samma multiplicitet. Eftersom $\big(x - (\xi + \eta i)\big)\big(x - (\xi - \eta i)\big) = x^2 - 2\xi x + \xi^2 + \eta^2$ vet vi enligt Faktorsatsen (Sats 2.1.2) att $p(x) = (x^2 - 2\xi x + \xi^2 + \eta^2)q(x)$ för något reellt polynom $q(x)$.

Om nu $\xi + \eta i$ skulle vara ett nollställe även för $q(x)$, så innebär det även enligt vad vi precis visade att även $\xi - \eta i$ måste vara det. På samma sätt kan vi fortsätta resonera och därmed har vi visat att dessa nollställen alltid kommer i par.

Nu när vi visat att komplexa nollställen till reella polynom alltid kommer i par kan vi enkelt visa att minst ett av det reella femtegradspolynomets nollställen ligger i $\mathbb{R}$.

Sats 2.1.7: Ett reellt polynom av udda grad har minst ett reellt nollställe.

Bevis: Enligt Sats 2.1.2 vet vi att ett polynom alltid har lika många nollställen i $\mathbb{C}$ som sin grad. Alltså har ett polynom av udda grad alltid ett udda antal nollställen. Enligt Sats 2.1.6 kan det dock till ett reellt polynom bara finnas ett jämnt antal nollställen som är komplexa (icke-reella). Alltså måste minst ett nollställe vara reellt, vilket skulle visas.

Vi har nu bevisat alla satser som behövs för att hävda de möjliga rötter till reella tredje- och fjärdegradsekvationer som vi beskrev i delkapitel 1.3. Antalet nollställen är till en algebraisk ekvation är lika med dess grad. Icke-reella polynom har reella eller icke-reella nollställen i någon kombination. För reella polynom kommer alltid icke-reella nollställen i par med sitt komplexkonjugat och om polynomet har udda grad är minst ett nollställe reellt.

Vi kan därmed dra ett antal slutsatser om femtegradsekvationens nollställen, bland annat att ett femtegradspolynom alltid har fem nollställen i $\mathbb{C}$. Komplexa (icke-reella) femtegradspolynom kan inom dessa ha alla möjliga kombinationer av reella och icke-reella nollställen. För reella femtegradspolynom gäller dock att de högst kan ha totalt fem olika nollställen i $\mathbb{C}$, varav ett till fem olika reella nollställen i kombination med två eller fyra komplexa (icke-reella) nollställen. Vi ska exemplifiera dessa möjliga antal nollställen hos reella femtegradsekvationer med en tabell:

Antal distinkta nollställen	**Exempel på polynom**	**Nollställen**
1 reellt, 0 icke-reella	x^5	$x_{1,2,3,4,5} = 0$
1 reellt, 2 icke-reella	$x^5 + x^3$	$x_{1,2,3} = 0, x_4 = i, x_5 = -i$
1 reellt, 4 icke-reella	$x^5 + 5x^3 + 4x$	$x_1 = 0\,,\ x_2 = i\,,\ x_3 = -i\,,\ x_4 = 2i, x_5 = -2i$
2 reella, 0 icke-reella	$x^5 - x^4$	$x_{1,2,3,4} = 0, x_5 = 1$
2 reella, 2 icke-reella	$x^5 - x^4 + x^3 - x^2$	$x_{1,2} = 0\,,\ x_3 = 1\,,\ x_4 = i\,,\ x_5 = -i$
3 reella, 0 icke-reella	$x^5 - x^3$	$x_{1,2,3} = 0, x_4 = 1, x_5 = -1$
3 reella, 2 icke-reella	$x^5 - x$	$x_1 = 0\ ,\ \ x_2 = 1\ ,\ \ x_3 = -1\ ,\ x_4 = i, x_5 = -i$
4 reella, 0 icke-reella	$x^5 - 6x^4 + x^3 - 6x^2$	$x_{1,2} = 0, x_3 = 1, x_4 = 2, x_5 = 3$
5 reella, 0 icke-reella	$x^5 - 5x^3 + 4x$	$x_1 = 0\,,\ x_2 = 1\,,\ x_3 = -1\,,\ x_4 = 2, x_5 = -2$

Tabell 1: Möjliga antal nollställen för reella femtegradspolynom

Vi ska nu gå vidare till det delkapitel som kommer behandla huvudproblemet i denna uppsats, nämligen frågan om huruvida femtegradsekvationen är generellt lösbar med radikaler eller inte.

2.2 Femtegradsekvationens lösbarhet med radikaler

I det förra delkapitlet visade vi att reella femtegradsekvationer kan ha ett till fem olika nollställen i $\mathbb{C}$, varav minst ett ligger i $\mathbb{R}$. I detta delkapitel är vi intresserade av om femtegradsekvationen generellt är lösbar med radikaler eller inte och därmed om det går att göra en generell lösningsformel för femtegradsekvationen såsom vi visat att det går att göra för ekvationer av grad ett till fyra. Till slut kommer vi bevisa Niels Henrik Abels sats från 1824 och använda oss av den för att visa att det finns

femtegradsekvationer som inte går att lösa med radikaler och att det därmed inte går att konstruera en generell algebraisk lösningsformel för femtegradsekvationen.

Först ska vi dock bevisa några hjälpsatser som vi ska använda för att härleda Abels sats. Vi ska börja detta delkapitel med några egenskaper hos en viss speciell typ av polynom som inte förändras om variablerna byter plats med varandra. Dessa kallas symmetriska polynom.

Definition 2.2.1: Ett polynom i de flera variablerna $x_1, x_2, \dots, x_n$ sägs vara *symmetriskt* om $p(x_1, x_2, \dots, x_n) = p\left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}\right)$ för alla permutationer σ.

Exempelvis är $p(x, y) = x^2 + 2xy + y^2$ symmetriskt medan $p(x, y) = 3xy - x$ inte är det. Vi ska nu införa ett begrepp för en speciell typ av symmetriska polynom, nämligen de som är en summa av alla möjliga termer av samma grad där varje term är en produkt av olika variabler med grad 1.

Definition 2.2.2: För de n stycken variablerna $x_1, x_2, \dots, x_n$ så sägs de n olika polynomen $e_k(x_1, x_2, \dots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \dots x_{i_k}$ för $k = 1,2, \dots n$ vara *elementära symmetriska polynom* i variablerna $x_1, x_2, \dots, x_n$.

För de två variablerna x, y är alltså de elementära symmetriska polynomen $e_1(x, y) = x + y$ och $e_2(x, y) = xy$. För de tre variablerna x, y, z så är alltså de elementära symmetriska polynomen $e_1(x, y, z) = x + y + z$, $e_2(x, y, z) = xy + xz + yz$ och $e_3(x, y, z) = xyz$.

Nu ska vi ta oss an en sats som ofta kallas huvudsatsen för symmetriska polynom, som säger att alla symmetriska polynom entydigt kan skrivas som polynom i sina elementära symmetriska polynom.

Sats 2.2.3 (Huvudsatsen för symmetriska polynom): Låt K vara en talkropp eller $\mathbb{Z}$ och låt $p(x_1, x_2, \dots, x_n)$ vara ett symmetriskt polynom över K. Då finns ett entydigt bestämt polynom $p_e(e_1(x_1, x_2, \dots, x_n), \dots, e_n(x_1, x_2, \dots, x_n))$ över K där $e_k(x_1, x_2, \dots, x_n)$ är de elementära symmetriska polynomen sådant att $p(x_1, x_2, \dots, x_n) = p_e(e_1(x_1, x_2, \dots, x_n), \dots, e_n(x_1, x_2, \dots, x_n))$.

Bevis: Följande bevis kommer ursprungligen från Augustin Louis Cauchy och är hämtat från Nagell [5]. Vi ska börja med att visa existensen av p_e med ett induktionsbevis över antalet variabler.

Låt oss börja med ett symmetriskt polynom $p(x_1, x_2)$ av de två variablerna x_1 och x_2. De elementära symmetriska polynomen är således $e_1(x_1, x_2) = x_1 + x_2$ och $e_2(x_1, x_2) = x_1 x_2$. Eftersom $e_1 = x_1 + x_2 \Leftrightarrow x_2 = e_1 - x_1$ så gäller att $p(x_1, x_2) =$

$p(x_1, e_1 - x_1) = E_{1,0}x_1^m + E_{1,1}x_1^{m-1} + \cdots + E_{1,m}$ där koefficienterna $E_{1,i}$ är polynom i e_1 med koefficienter i K.

Betraktar vi nu $P(z) = E_{1,0}z^m + E_{1,1}z^{m-1} + \cdots + E_{1,m}$ och $g(z) = (z - x_1)(z - x_2) = z^2 - (x_1 + x_2)z + x_1x_2 = z^2 - e_1z + e_2$ så gäller enligt Divisionsalgoritmen (Sats 1.2.6) att $P(z) = q(z)g(z) + r(z)$ för entydiga polynom $q(z)$ och $r(z)$ där $\deg r(z) < \deg g(z) = 2$. Alltså måste $r(z) = A + Bz$ där A och B är polynom i e_1 och e_2 över K. Därmed är $P(z) = q(z)g(z) + A + Bz$.

Sätter vi nu $z = x_1$ ser vi att $p(x_1, x_2) = P(x_1) = q(x_1)g(x_1) + A + Bx_1 = A + Bx_1$ eftersom $g(x_1) = 0$. Men eftersom $p(x_1, x_2)$ är symmetriskt så måste även $p(x_1, x_2) = A + Bx_1 = A + Bx_2$. Eftersom x_1 och x_2 är oberoende så gäller därmed att $B = 0$ och att $p(x_1, x_2) = A$. Alltså har vi visat att $p(x_1, x_2)$ entydigt kan skrivas som ett polynom i e_1 och e_2 över K och alltså gäller satsen för symmetriska polynom av två variabler.

Antag nu att satsen gäller för $n - 1$ variabler. Vi antar alltså att $p(x_1, x_2, \dots, x_{n-1})$ över K kan skrivas som ett polynom över K av de elementära symmetriska polynomen $e_{n-1,1}, e_{n-1,2}, \dots, e_{n-1,n-1}$, där $e_{n-1,i}$ är de elementära symmetriska polynomen i variablerna $x_1, x_2, \dots, x_{n-1}$, och ska visa att det innebär att $p(x_1, x_2, \dots, x_n)$ över K kan skrivas som ett polynom över K av de elementära symmetriska polynomen $e_{n,1}, e_{n,2}, \dots, e_{n,\square}$, där $e_{n,i}$ är de elementära symmetriska polynomen i variablerna $x_1, x_2, \dots, x_n$.

Betraktar vi polynomet $g(z) = \prod_{i=1}^{n}(z - x_i) = z^n - e_{n,1}z^{n-1} + \cdots + (-1)^{n-1}e_{n,n-1}z + (-1)^n e_{n,n} = (z - x_n)(z^{n-1} - e_{n-1,1}z^{n-2} + \cdots + (-1)^{n-2}e_{n-1,n-2}z + (-1)^{n-1}e_{n-1,n-1})$ så ser vi genom att jämför koefficienterna för all potenser av z i de två sista leden att $\begin{cases} e_{n-1,1} = -x_n + e_{n,1} \\ e_{n-2,2} = x_n^2 - e_{n,1}x_n + e_{n,2} \\ \dots \\ e_{n-1,n-1} = (-1)^{n-1}x_n^{n-1} + (-1)^{n-2}e_{n,1}x_n^{n-2} + \cdots + e_{n,n-1} \end{cases}$.

Om vi nu ordnar $p(x_1, x_2, \dots, x_n)$ efter fallande potenser av x_n ser vi att $p(x_1, x_2, \dots, x_n) = p_0x_n^m + p_1x_n^{m-1} + \cdots + p_m$ där p_i är polynom över K av de $n - 1$ variablerna $x_1, x_2, \dots, x_{n-1}$. Men ifall vi skulle permutera variablerna $x_1, x_2, \dots, x_{n-1}$ så ser vi även att $p\left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n-1)}, x_n\right) = p_0\left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n-1)}\right)x_n^m + p_1\left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n-1)}\right)x_n^{m-1} + \cdots + p_m\left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n-1)}\right)$. Eftersom $p(x_1, x_2, \dots, x_n)$ är symmetriskt i variablerna $x_1, x_2, \dots, x_n$så måste $p(x_1, x_2, \dots, x_n) = p\left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n-1)}, x_n\right)$. Alltså måste $p_i = p_i\left(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n-1)}\right)$ för alla i och permutationer och därmed är p_i är symmetriska polynom över K av de $n - 1$ variablerna $x_1, x_2, \dots, x_{n-1}$. Enligt antagandet kan dessa uttryckas som polynom av de elementära symmetriska polynomen $e_{n-1,1}, e_{n-1,2}, \dots, e_{n-1,n-1}$. Gör vi detta och använder oss av likheterna från förra stycket får vi till slut efter förenkling och efter

att återigen ordnat efter fallande potenser att $p(x_1, x_2, \dots, x_n) = E_0 x_n^m + E_1 x_n^{m-1} + \cdots + E_m$ där E_i är polynom över K av de elementära symmetriska polynomen $e_{n,1}, e_{n,2}, \dots, e_{n,n}$

Betraktar vi nu $P(z) = E_{1,0} z^m + E_{1,1} z^{m-1} + \cdots + E_{1,m}$ för $m \geq n$ så vet vi enligt Divisionsalgoritmen (Sats 1.2.6) att $P(z) = q(z)g(z) + r(z)$ för entydiga polynom $q(z)$ och $r(z)$ där $\deg r(z) < \deg g(z) = n$. Därmed måste $r(z) = C_0 z^{n-1} + C_1 z^{n-2} + \cdots + C_{n-2} z + C_{n-1}$ där C_j är symmetriska polynom i $e_{n,1}, e_{n,2}, \dots, e_{n,n}$ över K. Alltså är $P(z) = q(z)g(z) + C_0 z^{n-1} + C_1 z^{n-2} + \cdots + C_{n-2} z + C_{n-1}$ och sätter vi nu in $z = x_1$ så är $p(x_1, x_2, \dots, x_n) = P(x_1) = r(x_1) = C_0 {x_1}^{n-1} + C_1 {x_1}^{n-2} + \cdots + C_{n-2} x_1 + C_{n-1}$ eftersom $g(x_1) = 0$. Eftersom $p(x_1, x_2, \dots, x_n)$ är symmetriskt i $x_1, x_2, \dots, x_n$ så måste denna likhet fortfarande gälla om x_1 ersattes med vilken som helst av de andra variablerna.

Vi ser därmed att $C_0 z^{n-1} + C_1 z^{n-2} + \cdots + C_{n-2} z + C_{n-1} - p(x_1, x_2, \dots, x_n) = 0$ för de n stycken värdena $x_1, x_2, \dots, x_n$ på z. Som en följd av Sats 2.1.2 kan dock ett nollskilt polynom av grad $n-1$ endast ha n nollställen i en variabel om polynomet är oberoende av den variabeln (alltså har grad noll). Alltså måste $p(x_1, x_2, \dots, x_n) = C_{n-1}$ och eftersom C_{n-1} är ett symmetriskt polynom i $e_{n_1}, e_{n_2}, \dots, e_{n_n}$ över K har vi alltså visat att om $p(x_1, x_2, \dots, x_{n-1})$ över K kan skrivas som ett polynom över K av elementära symmetriska polynom så innebär att $p(x_1, x_2, \dots, x_n)$ över K kan skrivas som ett polynom över K av de elementära symmetriska polynomen. Alltså är induktionsbeviset klart.

Nu ska vi också visa entydigheten. Detta gör vi genom att visa att de elementära symmetriska polynomen är oberoende och att det därmed inte går att skriva ett polynom i de elementära symmetriska polynomen på två eller fler olika sätt.

Antag att vi har ett polynom $p(e_1, e_2, \dots, e_n) \neq 0$ över talkroppen K där $e_1, e_2, \dots, e_n$ är de elementära symmetriska polynomen av variablerna $x_1, x_2, \dots, x_n$. Då kan termerna i $p(e_1, e_2 \dots, e_n)$ skrivas som $T_i = c_i {e_1}^{v_1}, {e_2}^{v_2}, \dots, {e_n}^{v_n}$ där inte alla c_i är noll.

Vi väljer nu ut de T_i med högst grad i förhållande till $e_1, e_2, \dots, e_n$, det vill säga de termer där summan $v_1 + v_2 + \cdots + v_n$ är som störst, låt denna summa vara h_1. Om det endast finns en sådan term, betecknar vi denna T. Finns det fler sådana termer väljer vi ut de termer med högst grad i förhållande till $e_2 \dots, e_n$, det vill säga de termer där summan $v_2 + \cdots + v_n$ är som störst, låt denna summa vara h_2. v_1 är då entydigt bestämt enligt $v_1 = h_1 - h_2$. Om det endast finns en sådan term, betecknar vi denna T. Annars fortsätter vi på samma sätt r gånger tills vi har hittat termen T och där då $v_1, v_2, \dots, v_n$ är entydigt bestämda av de entydiga $h_1, h_2, \dots, h_r$ enligt $h_r = v_r + v_{r+1} + \cdots + v_n$ och $v_i = h_i - h_{i+1}$ för $i = 1,2, \dots, r-1$. För $h_{r+1}, h_{r+2}, \dots, h_n$ definierar vi också dessa enligt $h_s = v_s + v_{s+1} + \cdots + v_n$ där $s = r+1, r+2, \dots, n$.

Vi ser nu att $T = ce_1{}^{v_1}e_2{}^{v_2} \dots e_n{}^{v_n} = c_i(x_1 + x_2 + \cdots + x_n)^{v_1}(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n)^{v_2} \dots (x_1x_2 \dots x_n)^{v_n}$ för något $c \in K \neq 0$. Vid en utveckling av denna term kommer således potensprodukten $x_1^{h_1}x_2^{h_2} \dots x_n^{h_n}$ förekomma som term med koefficienten $c \neq 0$. Dock kan ingen annan T_i ge upphov till denna potensprodukt tack vare det sättet som vi valde ut T. Därmed har vi visar att om vi har ett polynom $p(e_1, e_2, \dots, e_n) \neq 0$ över talkroppen K där $e_1, e_2, \dots, e_n$ är de elementära symmetriska polynomen av variablerna $x_1, x_2, \dots, x_n$ ger utvecklingen av polynomet i $x_1, x_2, \dots, x_n$ att $p(x_1, x_2, \dots, x_n) \neq 0$. Således har vi visat att $p(e_1, e_2 \dots, e_n) = \sum a_{k_1,k_2,\dots,k_r}e_1^{k_1}e_2^{k_2} \dots e_r^{k_r} = 0$ om och endast om alla $a_{k_1,k_2,\dots,k_r} = 0$. Därmed är de elementära symmetriska polynomen oberoende och framställningen av polynom i de elementära symmetriska polynomen är därför entydig.

Vi har alltså visat både existensen och entydigheten. Alltså är satsen bevisad.

Sats 2.2.4: Låt K vara en talkropp eller $\mathbb{Z}$ och låt $q(x)$ vara ett polynom över K med nollställena $a_1, \dots, a_n$. Låt $p(x_1, \dots, x_n)$ vara ett symmetriskt polynom över K. Då är $p(a_1, \dots, a_n)$ ett polynom över K i qs koefficienter.

Bevis: Enligt Sats 2.1.2 är $q(x) = q_n(x - a_1)(x - a_2) \dots (x - a_n)$ för något $q_n \in K$. Utvecklar vi dessa parenteser får vi $q(x) = q_n(x^n - (a_1 + \cdots + a_n)x^{n-1} + (a_1a_2 + \cdots + a_{n-1}a_n)x^{n-2} - \cdots \pm a_1 \dots a_n)$ och vi ser här att koefficienterna i parenteserna är de elementära symmetriska polynomen av $a_1, \dots, a_n$, det vill säga att $q(x) = q_nx^n - q_ne_1(a_1, \dots, a_n)\square^{n-1} + q_ne_2(a_1, \dots, a_n)x^{n-2} - \cdots \pm q_ne_n(a_1, \dots, a_n)$.

Eftersom $p(x_1, \dots, x_n)$ är ett symmetriskt polynom över K så kan $p(x_1, \dots, x_n)$ enligt Huvudsatsen för symmetriska polynom (Sats 2.2.3) skrivas som ett polynom över K av de elementära symmetriska polynomen. Alltså är $p(x_1, \dots, x_n) = p_e(e_1(x_1, \dots, x_n), \dots, e_n(x_1, \dots, x_n))$. Insättning av nollställena för $q(x)$ ger $p(a_1, \dots, a_n) = p_e\big(e_1(a_1, \dots, a_n), \dots, e_n(a_1, \dots, a_n)\big)$. Eftersom koefficienterna till $q(x)$ är multiplar över K av de elementära symmetriska polynomen av $a_1, \dots, a_n$ betyder det att vi kan skriva $p(a_1, \dots, a_n)$ som ett polynom över K i koefficienterna för $q(x)$, vilket skulle visas.

Sats 2.2.5: Låt $p(x)$ vara ett irreducibelt polynom över talkroppen K och låt L vara sönderfallskroppen för något polynom $q(x)$ över talkroppen K. Antag vidare att $p(x)$ är reducibelt över L. Då har alla irreducibla faktorer i $p(x)$ över L samma grad. Om $p(x)$ har ett nollställe i L så ligger alla dess nollställen i L.

Bevis: Låt $q(x)$ vara ett polynom av graden n med nollställena $a_1, \dots, a_n$ så att $L = K(a_1, \dots, a_n)$. Låt $K[a_1, \dots, a_n]$ vara mängden av polynom i $a_1, \dots, a_n$ med

koefficienter i K och låt polynomet $g(x) = x^m + r_1(a_1, \dots, a_n)x^{m-1} + \cdots + r_m(a_1, \dots, a_n)$ över L vara en irreducibel faktor i $p(x)$ över L.

Eftersom $g(x)$ är irreducibelt över L så måste även $g^\sigma(x) = x^m + r_1(a_{\sigma(1)}, \dots, a_{\sigma(n)})x^{m-1} + \cdots + r_m(a_{\sigma(1)}, \dots, a_{\sigma(n)})$ vara irreducibelt över L för varje permutation σ av $1,2, \dots, n$. Ty om vi betraktar $g(x) = g(x, a_1, \dots, a_n) = x^m + r_1(a_1, \dots, a_n)x^{m-1} + \cdots + r_m(a_1, \dots, a_n)$ och antar att $g^\sigma(x) = g\big(x, a_{\sigma(1)}, \dots, a_{\sigma(n)}\big)$ är reducibelt över $L(a_1, \dots, a_n)$ så att det finns två polynom g_1 och g_2 i x över $L(a_1, \dots, a_n)$ så att $g^\sigma(x) = g\big(x, a_{\sigma(1)}, \dots, a_{\sigma(n)}\big) = g_1(x, a_1, \dots, a_n)g_2(x, a_1, \dots, a_n)$ så skulle $g(x) = g(x, a_1, \dots, a_n) = g_1\big(x, a_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n)}\big)g_2\big(x, a_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n)}\big)$ och således också reducibelt i $L(a_1, \dots, a_n)$. Men eftersom $L(a_1, \dots, a_n) = L$ så gäller detta även över L.

Sätt $P(x) = \prod_\sigma g^\sigma(x)$ där produkten sker över alla permutationer σ. Eftersom produkten sker över alla permutationer av $1,2, \dots, n$ så måste $P(x)$ vara symmetriskt i nollställena $a_1, \dots, a_n$. Men om vi utvecklar $P(x) = \prod_\sigma g^\sigma(x) = \prod_\sigma(x^m + r_1(a_{\sigma(1)}, \dots, a_{\sigma(n)})x^{m-1} + \cdots + r_m(a_{\sigma(1)}, \dots, a_{\sigma(n)})) = x^M + R_1(a_1, \dots, a_n)x^{M-1} + \cdots + R_m(a_1, \dots, a_n)$ där $R_i(a_1, \dots, a_n)$ är polynom i $a_1, \dots, a_n$ över K så ser vi att även $R_i(a_1, \dots, a_n)$ måste vara symmetriska i $a_1, \dots, a_n$. Därmed är koefficienterna i $P(x)$ symmetriska polynom i nollställena $a_1, \dots, a_n$ med koefficienter i K. Eftersom $q(x)$ har koefficienter i K så måste $P(x)$ enligt Sats 2.2.4 också kunna skrivas som ett polynom med koefficienter i K.

Eftersom $g(x)$ är en irreducibel faktor till både $p(x)$ och $P(x)$ i L och $p(x)$ är irreducibelt i K så måste $p(x)|P(x)$ i K och därmed $p(x)|P(x)$ i L eftersom $L \supseteq K$. Men eftersom polynomen g^σ är irreducibla över K och detta kan ske på ett entydigt sätt enligt Aritmetikens fundamentalsats för polynom över talkroppen K (Sats 1.2.12) så måste $p(x)$ vara en produkt av vissa g^σ. Alltså har alla irreducibla faktorer i $p(x)$ över L samma grad eftersom alla g^σ har samma grad.

Om $p(x)$ har ett nollställe i L så vet vi enligt Faktorsatsen (Sats 1.2.13) att $p(x)$ har en irreducibel faktor av grad 1 över L. Men eftersom alla irreducibla faktorer i $p(x)$ över L har samma grad så måste $p(x)$ kunna faktoriseras i polynom över L med grad 1. Därmed måste alla nollställen till $p(x)$ ligga i L. Alltså är satsen bevisad.

Vi ska även visa några egenskaper hos polynomet $p(x) = x^n - a$, vilket spelar en viss roll i beviset för Abels sats.

Sats 2.2.6: Polynomet $p(x) = x^n - a$ där $a \in \mathbb{C}, n \in \mathbb{N}, n \geq 1$ har n stycken nollställen som kan skrivas på formen $\sqrt[n]{r}\, e^{\frac{i\varphi + 2\pi ik}{n}} \in \mathbb{C}$ där $k = 0,1, \dots, n-1$ och $a = re^{i\varphi}$ för något $r, \varphi \in \mathbb{R}, r, \varphi \geq 0$.

Bevis: Låt oss börja med att betrakta $p(z) = z^n - 1$. Enligt Sats 2.1.2 har $p(z)$ exakt n nollställen i $\mathbb{C}$. Alltså kan dessa nollställen skrivas på den polära formen $r_1 e^{i\varphi_1}$ där $r_1, \varphi_1 \in \mathbb{R}, r_1, \varphi_1 \geq 0$.

Alltså måste $p\left(r_1 e^{i\varphi_1}\right) = (r_1 e^{i\varphi_1})^n - 1 = 0$ det vill säga att $(r_1 e^{i\varphi_1})^n = 1 \Leftrightarrow {r_1}^n e^{ni\varphi_1} = 1^k$ för $k = 0,1,\dots,n-1$ och enligt Eulers identitet är då ${r_1}^n e^{ni\varphi_1} = ((e^{\pi i})^2)^k$. Således är ${r_1}^n e^{ni\varphi_1} = e^{2\pi ik}$ och därmed måste ${r_1}^n = 1$ och $ni\varphi_1 = 2\pi ik \Leftrightarrow \varphi_1 = 2\pi k/n$. Alltså kan alla nollställen till $p(z) = z^n - 1$ skriva på formen $e^{2\pi ik/n}$ där $k = 0,1,\dots,n-1$.

Eftersom $(e^{2\pi ik/n})^n = 1$ för $k = 0,1,\dots,n-1$ och $a = re^{i\varphi}$ så måste $(\sqrt[n]{r}\, e^{\frac{i\varphi+2\pi ik}{n}})^n = (\sqrt[n]{r} e^{\frac{i\varphi}{n}} e^{\frac{2\pi ik}{n}})^n = (\sqrt[n]{r} e^{\frac{i\varphi}{n}})^n (e^{\frac{2\pi ik}{n}})^n = re^{i\varphi} = a$ för $k = 0,1,\dots,n-1$. Alltså måste $p\left(\sqrt[n]{r}\, e^{\frac{i\varphi+2\pi ik}{n}}\right) = (\sqrt[n]{r}\, e^{\frac{i\varphi+2\pi ik}{n}})^n - a = a - a = 0$ för $k = 0,1,\dots,n-1$ och därmed är dessa nollställen till $p(x)$, vilket skulle visas.

Sats 2.2.7: Låt n vara ett primtal, K vara en talkropp och $a \in K$ vara ett tal som inte uppfyller att $k^n = a$ för något $k \in K$. Då är polynomet $p(x) = x^n - a$ irreducibelt över K.

Bevis: Låt oss börja med $n = 2$. Därmed är $p(x) = x^2 - a$ för något $a \in K$ där $\sqrt{a} \notin K$ och $\sqrt{a}$ är någon av lösningarna ekvationen $x^2 - a = 0$. Dock ser vi att $p(x) = x^2 - a = (x - \sqrt{a})(x + \sqrt{a})$ och eftersom denna faktorisering är entydig enligt exempelvis Divisionsalgoritmen (Sats 1.2.6) så är en faktorisering ej möjlig över K. Därmed är $p(x) = x^2 - a$ irreducibelt över K och satsen gäller för $n = 2$.

Övriga primtal är udda så låt oss nu anta att $p(x) = x^n - a$ för något $a \in K$ där n är ett udda primtal och där det inte existerar något $b \in K$ så att $b^n = a$.

Enligt Sats 2.2.6 så har $p(x)$ nollställena $\sqrt[n]{r}\, e^{\frac{i\varphi+2\pi ik}{n}}$ där $j = 0,1,\dots,n-1$. Låt $c = \sqrt[n]{r}\, e^{\frac{i\varphi}{n}}$ och $d_j = e^{2\pi ij/n}$ för $j = 0,1,\dots,n-1$ så att $p(x)$ har nollställena cd_j.

Antag nu att $p(x)$ är reducibelt över K och att det därmed finns $g(x)$ och $q(x)$ över K med graden ≥ 1 så att $p(x) = x^n - a = q(x)g(x)$ och högstagradskofficienterna för $g(x)$ och $q(x)$ är 1. Då måste även nollställen till $q(x)$ vara vissa av nollställen i $p(x)$. Därmed är den konstanta termen $q_0 \in K$ lika med en produkt $\pm c^m D_{j,m}$ där $1 \leq m < n$, $\deg q(x) = m$ och $D_{j,m}$ är produkten av m stycken olika d_j. Detta ger att ${q_0}^n = (\pm c^m D_{j,m})^n = \pm (c^m)^n (D_{j,m})^n = \pm (c^n)^m = \pm a^m$.

Eftersom $n \nmid m$ och n är ett primtal så kan inte n och m ha några gemensamma heltalsdelare vilket innebär att $n_0 n + m_0 m = 1$ för något $n_0, m_0 \in \mathbb{Z}$ enligt Sats

1.2.10. Därmed måste $a = a^1 = a^{n_0 n + m_0 m} = a^{n_0 n}(a^m)^{m_0} = a^{n_0 n}(\pm {q_0}^n)^{m_0} = a^{n_0 n}(\pm q_0)^{n m_0} = (a^{n_0}(\pm q_0)^{m_0})^n$. Eftersom $a, q_0 \in K$ så måste även $a^{n_0}(\pm q_0)^{m_0} \in K$. Men att $a = (a^{n_0}(\pm q_0)^{m_0})^n$ är dock en motsägelse eftersom det inte existerar något $b \in K$ så att $b^n = a$ enligt förutsättningen. Alltså leder antagandet att $p(x)$ är reducibelt över K till en motsägelse och därmed är $p(x)$ är irreducibelt över K även för udda primtal. Alltså är satsen bevisad.

Sats 2.2.8: Om talkroppen K är sluten under komplexkonjugering, det vill säga att $\bar{a} \in K$ om $a \in K$, så gäller att om b är en radikal över K så är även $\bar{b}$ det.

Bevis: Låt b vara en radikal över K. Därmed så måste $b^n \in K$ för något $n \in \mathbb{N}$. Eftersom K är sluten under komplexkonjugering så måste därför även $\overline{b^n} \in K$. Men $\overline{b^n} = \bar{b}^n$ och därmed måste $\bar{b}$ vara en radikal över K, vilket skulle visas.

Med hjälp av dessa satser kan vi nu bevisa Niels Henrik Abels sats från 1824 som säger att det finns vissa restriktioner för att femtegradsekvationen ska vara lösbar med radikaler.

Sats 2.2.9 (Abels sats): Låt $p(x)$ vara ett irreducibelt femtegradspolynom över den reella talkroppen $K \subset \mathbb{R}$. För att ekvationen $p(x) = 0$ ska vara lösbar med radikaler måste antingen endast ett eller samtliga av polynomets nollställen vara reella.

Bevis: Vi vet enligt Sats 2.1.6 att ett reellt femtegradspolynom antingen har ett, tre eller fem reella nollställen eftersom alla dess komplexa (icke-reella) nollställen kommer i par. Abels sats säger alltså att om det finns irreducibla femtegradspolynom som är lösbara med radikaler så har de exakt ett eller fem reella nollställen. Därmed kan det inte finnas irreducibla femtegradspolynom med tre reella nollställen som är lösbara med radikaler.

Om den algebraiska ekvationen $p(x) = 0$ är lösbar med radikaler och $p(x)$ är irreducibelt över talkroppen K så är sönderfallkroppen $L \supset K$ en ändlig radikal utvidgning av K. Eftersom denna radikala utvidgning är ändlig så kan den konstrueras genom succesiva ändliga radikala utvidgningar där varje utvidgning har primtalsgrad. Om exempelvis $[K(\beta): K] = 6$ för den radikala utvidgningen $K(\beta)$ över K så kan vi dela upp denna i de två radikala utvidgningarna $K(\beta^2, \beta) \supseteq K(\beta^2) \supseteq K$ där $[K(\beta^2): K] = 3$ och $[K(\beta^2, \beta): K(\beta^2)] = 2$ eller i de två radikala utvidgningarna $K(\beta^3, \beta) \supseteq K(\beta^3) \supseteq K$ där $[K(\beta^3): K] = 2$ och $[K(\beta^3, \beta): K(\beta^2)] = 3$. I serien av utvidgningar från K till L finns därmed ett steg $L_1 \supset K_2$ av primtalsgrad där $p(x)$ är irreducibelt över K_2 men reducibelt över L_1 så att $L \supseteq L_1 \supset K_2 \supseteq K$. Enligt Sats 1.2.21 så gäller att $5 | [L_1: K_2]$ eftersom $p(x)$ är femtegradspolynom men eftersom vi vet att $[L_1: K_2]$ är ett primtal så måste $[L_1: K_2] = 5$.

Låt oss nu betrakta femtegradsekvationen $x^5 - 1 = 0$. Enligt Sats 2.2.6 så kan lösningarna skrivas på formen $e^{2\pi ij/5} \in \mathbb{C}$ där $j = 0,1,\dots,4$. Vi ser alltså att $e^{2\pi i/5}$ är en radikal över $\mathbb{Q}$ och därmed även en radikal över $K \supseteq \mathbb{Q}$. Låt därför $e^{2\pi i/5}$ vara en av de radikaler som vi adjungerar i någon radikal utvidgning från K till L. Vi undrar nu om adjungeringen av $e^{2\pi i/5}$ påverkar huruvida $p(x)$ är reducibelt eller inte. Eftersom $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ så ser vi att $\deg_K e^{2\pi i/5} \leq 4$. Således kan vi anta att om $e^{2\pi i/5} \in L_1$ så är $e^{2\pi i/5}$ redan ett element i K_2. Ty om $e^{2\pi i/5} \in L_1$ och $\deg_K e^{2\pi i/5} \leq 4$ innebär detta att $[L_1 : K_2] \nmid \deg_K e^{2\pi i/5}$ och därmed måste $e^{2\pi i/5} \in K_2$ enligt Sats 1.2.21. Alltså kan vi adjungera $e^{2\pi i/5}$ på ett sådant sätt att $e^{2\pi i/5} \in K_2$ och att $p(x)$ ändå är irreducibelt över K_2.

Eftersom $p(x)$ är ett reellt polynom vet vi enligt Sats 2.1.6 att icke-reella lösningar alltid kommer i par med sina komplexkonjugat. Dock finns det talkroppar som inte innehåller komplexkonjugaten av alla sina element. Eftersom L_1 är en ändlig radikal utvidgning av K så skapar vi denna genom radikala utvidgningar enligt $K \subset K\left(e^{2\pi i/5}\right) \subset K\left(e^{2\pi i/5}, a_1\right) \subset K\left(e^{2\pi i/5}, a_1, \bar{a}_1\right) \subset \cdots \subset K\left(e^{2\pi i/5}, a_1, \bar{a}_1, \dots, a_l, \bar{a}_l\right) = L_1$ där $\bar{a}_1$ är komplexkonjugatet till a_1, vilket vi kan göra enligt Sats 2.2.8.

Låt b vara den radikal över K_2 så att $L_1 = K_2(b)$ och låt oss nu betrakta polynomet $x^5 - b^5$. Vi vet då att $b^5 \in K_2$, att $b \notin K_2$ och att $x^5 - b^5$ är ett polynom över K_2. Eftersom dess lösningar kan skrivas på formen $be^{2\pi ij/5}$ för $j = 0,1,2,3,4$ enligt Sats 2.2.6 så måste $be^{2\pi ij/5} \in K_2(b)$ och därför sönderfaller polynomet $x^5 - b^5$ över L_1. Enligt Sats 2.2.5 har därför alla irreducibla faktorer av $p(x)$ över L_1 samma grad. Eftersom $\deg p(x) = 5$ och alla faktorer ska ha samma grad är detta bara möjligt om dessa har grad 1 eller 5. Enligt antagandet är dock $p(x)$ reducibelt i L_1 och därmed måste graden av de irreducibla faktorerna till $p(x)$ över L_1 vara 1. Men då ligger alla nollställen till $p(x)$ i L_1 och således måste $L_1 = L$.

Låt oss återigen betrakta polynomet $x^5 - b^5$. Enligt Sats 2.2.7 är detta polynom irreducibelt över K_2 men vi vet sedan tidigare att det sönderfaller i $L = K_2(b)$. Talen b^0, b^1, b^2, b^3, b^4 bildar alltså en bas för L över K_2. Detta innebär att alla tal $l \in L$ kan skrivas som $l = \kappa_0 + \kappa_1 b + \kappa_2 b^2 + \kappa_3 b^3 + \kappa_4 b^4$ där $\kappa_i \in K_2$.

Enligt Sats 2.1.7 vet vi att det finns minst en reell lösning x_0 till ekvationen $p(x) = 0$. Eftersom $x_0 \in L$ så kan vi skriva denna som $x_0 = \kappa_0 + \kappa_1 b + \kappa_2 b^2 + \kappa_3 b^3 + \kappa_4 b^4$ där $\kappa_i \in K_2$. Vi ska nu visa att samtliga rötter x_j till $p(x) = 0$ ges av $x_j = \kappa_0 + \kappa_1 e^{2\pi i/5^j} b + \kappa_2 e^{2\pi i/5^{2j}} b^2 + \kappa_3 e^{2\pi i/5^{3j}} b^3 + \kappa_4 e^{2\pi i/5^{4j}} b^4 = \sum_{i=0}^{4} \kappa_i (\varepsilon^j b)^i$ för $j = 0,1,2,3,4$ där $\varepsilon = e^{2\pi i/5}$.

Notera att $b, \varepsilon b, \varepsilon^2 b, \varepsilon^3 b, \varepsilon^4 b$ är nollställena till polynomet $x^5 - b^5$ enligt Sats 2.2.6. Sätt $q(x) = \prod_{j=0}^{4}(x - x_j) = (x - x_0)(x - x_1)(x - x_2)(x - x_3)(x - x_4)$.

Koefficienterna i $q(x)$ är symmetriska polynom i $\varepsilon^j b$ med koefficienter i K_2 och enligt Sats 2.2.4 kan därför $q(x)$ skrivas som ett polynom över K_2. Men $p(x)$ och $q(x)$ har det gemensamma nollstället x_0 och eftersom $p(x)$ är irreducibelt över K_2 så måste $p(x) = q(x)$. Alltså har vi visat att om $p(x)$ är lösbart med radikaler så ges samtliga rötter x_j till $p(x) = 0$ av $x_j = \sum_{i=0}^{4} \kappa_i (\varepsilon^j b)^i$ för $j = 0,1,2,3,4$ där $\varepsilon = e^{2\pi i/5}$.

Eftersom vi konstruerar L som en radikal utvidgning av K genom att adjungera radikaler ihop med deras konjugat innebär detta att utvidgningen till K_2 sker på ett av två sätt, antingen att $K_2 = K\left(e^{2\pi i/5}, a_1, \bar{a}_1, \dots, a_l\right)$ och därmed att $b = a_l$ eller att $K_2 = K\left(e^{2\pi i/5}, a_1, \bar{a}_1, \dots, a_l, \bar{a}_l\right)$ och då att $b = \bar{a}_l$.

Om $b = a_l$ måste vi skilja på om b^5 är reellt eller inte, vilket ger ytterligare möjliga utfall. Om b^5 är reellt kan vi anta att $b = \sqrt[5]{b^5}$, alltså den reella femteroten, och därmed är alltså även b^2, b^3, b^4 reella. Eftersom x_0 är reell så måste $x_0 = \overline{x_0} \Leftrightarrow \kappa_0 + \kappa_1 b + \kappa_2 b^2 + \kappa_3 b^3 + \kappa_4 b^4 = \overline{\kappa_0} + \overline{\kappa_1} b + \overline{\kappa_2} b^2 + \overline{\kappa_3} b^3 + \overline{\kappa_4} b^4$. Eftersom b^0, b^1, b^2, b^3, b^4 är en bas för L över K_2 så måste koefficienterna vara parvis lika enligt definitionen för baser (Definition 1.1.6), det vill säga att $\kappa_i = \overline{\kappa_i}$ för alla $i = 0,1,2,3,4$. Därmed är alltså alla koefficienterna κ_i reella. Vi ser då att $x_4 = \sum_{i=0}^{4} \kappa_i (\varepsilon^4 b)^i = \sum_{i=0}^{4} \kappa_i (\varepsilon (e^{2\pi i/5})^3 b)^i = \sum_{i=0}^{4} \kappa_i (\varepsilon e^{6\pi i/5} b)^i = \sum_{i=0}^{4} \kappa_i (\varepsilon e^{\pi i/5} b)^i = \sum_{i=0}^{4} \kappa_i (-\varepsilon b)^i = \sum_{i=0}^{4} \kappa_i (\bar{\varepsilon} b)^i = \overline{x_1}$. Eftersom $p(x)$ är irreducibelt över K_2 så kan det inte ha multipla nollställen enligt Sats 2.1.5 och därmed måste x_4 och x_1 vara icke-reella. På samma sätt kan vi se att $x_3 = \overline{x_2}$ och att dessa också är icke-reella. Om b^5 är reellt har alltså $p(x)$ ett reellt och fyra icke-reella nollställen.

Om $b = a_l$ och b^5 istället inte är reellt så kan heller inte b vara reellt. Däremot måste $b^5\overline{b^5}$ vara reellt så låt c vara den reella femteroten till $b^5\overline{b^5}$. Om nu $p(x)$ är reducibelt över $K_2(c)$ så är därmed c^0, c^1, c^2, c^3, c^4 en bas för L över K_2 och då visade vi nyss att $p(x)$ har ett reellt och fyra icke-reella nollställen. Om $p(x)$ däremot är irreducibelt över $K_2(c)$ så resonerar vi som ovan fast med utvidgningen $L = K_2(b, c)$ över $K_2(c)$ istället för $L = K_2(b)$ över K_2. Eftersom $c^5 = b^5\overline{b^5} \Leftrightarrow c^5 = b^5\bar{b}^5 \Leftrightarrow \frac{b^5\bar{b}^5}{c^5} = 1 \Leftrightarrow \left(\frac{b\bar{b}}{c}\right)^5 = 1$ kan $\frac{b\bar{b}}{c}$ enligt Sats 2.2.6 skrivas som $\varepsilon^j = e^{2\pi i j/5}$ för $j = 0,1,2,3,4$ och därmed är $\bar{b} = \frac{c\varepsilon^j}{b}$ för något j. Men eftersom x_0 är reell så är $x_0 = \overline{x_0}$ och därmed är $\sum_{i=0}^{4} \kappa_i b^i = \sum_{i=0}^{4} \overline{\kappa_i b^i} = \sum_{i=0}^{4} \overline{\kappa_i}\bar{b}^i = \sum_{i=0}^{4} \overline{\kappa_i} \left(\frac{c\varepsilon^j}{b}\right)^i = \sum_{i=0}^{4} \overline{\kappa_i}\, c^i \varepsilon^{ji}/b^i$. Betraktar vi sidorna i denna likhet ser vi att $\sum_{i=0}^{4} \kappa_i b^i = \sum_{i=0}^{4} \overline{\kappa_i}\, c^i \varepsilon^{ji}/b^i \Leftrightarrow b^5 \sum_{i=0}^{4} \kappa_i b^i = b^5 \sum_{i=0}^{4} \overline{\kappa_i}\, c^i \varepsilon^{ji}/b^i \Leftrightarrow b^5 \sum_{i=0}^{4} \kappa_i b^i = \sum_{i=0}^{4} \overline{\kappa_i} c^i \varepsilon^{ji} b^{5-i}$ och utvecklar vi dessa summor ser vi att $\kappa_0 = \overline{\kappa_0}$ samt att $\overline{\kappa_i} = \kappa_{5-i} b^5 c^{-i} \varepsilon^{-ji}$ för $i = 1,2,3,4$. Därmed är $\overline{x_j} = \overline{\sum_{i=0}^{4} \kappa_i (\varepsilon^j b)^i} = \sum_{i=0}^{4} \overline{\kappa_i}\overline{\varepsilon^{ij}}\bar{b}^i = \sum_{i=0}^{4} \overline{\kappa_i} \varepsilon^{-ij} (\frac{c\varepsilon^j}{b})^i = \kappa_0 + \sum_{i=1}^{4} \overline{\kappa_i} \varepsilon^{-ji} (\frac{c\varepsilon^j}{b})^i =$

$\kappa_0 + \sum_{i=1}^{4}(\kappa_{5-i}b^5c^{-i}\varepsilon^{-ji})\varepsilon^{-ji}(\frac{c\varepsilon^j}{b})^i = \kappa_0 + \sum_{i=1}^{4}\kappa_{5-i}b^{5-i}\varepsilon^{-ji} = \kappa_0 + \sum_{i=1}^{4}\kappa_{5-i}b^{5-i}\varepsilon^{j(5-i)} = \kappa_0 + \sum_{i=1}^{4}\kappa_i b^i\varepsilon^{ji} = \sum_{i=0}^{4}\kappa_i b^i\varepsilon^{ji} = x_j$ och således är alla rötter reella.

Om $b = \bar{a}_l$ så är alltså $p(x)$ irreducibelt över $K_2 = K\left(e^{2\pi i/5}, a_1, \bar{a}_1, \dots, a_l\right) = K_1(a_l)$. Här kan b^5 inte vara reellt ty då skulle $b^5 = \overline{b^5} = \bar{b}^5 \Leftrightarrow \bar{a}_l{}^5 = a_l{}^5$ och isåfall skulle $\bar{a}_l$ kunna skrivas som $e^{2\pi ij/5}a_l$ för något $j = 0,1,2,3,4$ och därmed skulle $\bar{a}_l \in K_2$ eftersom $e^{2\pi ij/5}, a_l \in K_2$. Däremot är $b\bar{b}$ reellt. Eftersom b är en radikal över K_1 så måste $b^5 \in K_1$ och eftersom K_1 är slutet under komplexkonjugering så är $\overline{b^5} = \bar{b}^5 \in K_1$. Således gäller att det reella talet $b^5\bar{b}^5 \in K_1$ och därmed att $b\bar{b}$ är en reell radikal över K_1. Om $p(x)$ sönderfaller över $K_1(b\bar{b})$ så har vi redan visat att $p(x)$ då har ett reellt och fyra icke-reella nollställen. Om $p(x)$ däremot inte sönderfaller över $K_1(b\bar{b})$ så har vi dock visat enligt ett argumentet i förra stycket att alla rötter är reella.

Vi har alltså visat att om $p(x) = 0$ är lösbar med radikaler så måste antingen endast ett eller samtliga av polynomets nollställen vara reella, vilket skulle visas.

Det är möjligt att på ett liknande sätt visa att denna sats även gäller generellt för polynom av udda primtalsgrad, det vill säga att ett irreducibelt polynom av udda primtalsgrad endast har samtliga nollställen som är lösbara med radikaler om endast ett eller samtliga nollställen är reella, vilket vi dock inte ska visa här.

Enligt Abels sats (Sats 2.2.9) så är en femtegradsekvation där ett reellt irreducibelt femtegradspolynom med tre reella (och två icke-reella) nollställen är lika med noll inte lösbart med radikaler. Nu behöver vi alltså visa att det existerar ett sådant polynom.

Att avgöra om ett polynom är irreducibelt över en viss talkropp kan vara omständligt. Dock finns det enkla sätt att avgöra om vissa heltalspolynom är irreducibla över $\mathbb{Q}$ eller inte.

Sats 2.2.10 (Gauss lemma): Om ett polynom med koefficienter i $\mathbb{Z}$ är irreducibelt över $\mathbb{Z}$ så är det även irreducibelt över $\mathbb{Q}$.

Bevis: Låt $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ där $a_0, \dots, a_n \in \mathbb{Z}$ vara ett polynom med koefficienter i $\mathbb{Z}$ och antag att det är reducibelt i $\mathbb{Q}$, det vill säga att $p(x) = q(x)g(x)$ för några polynom $q(x)$ och $g(x)$ över $\mathbb{Q}$ med grad större än noll.

Därmed är $p(x) = q(x)g(x) = (q_0 + q_1x + \cdots + q_mx^m)(g_0 + g_1x + \cdots + g_ox^o)$ där $q_i, g_j \in \mathbb{Q}$, $m, o > 0$ och $m + o = n$. Låt oss nu bryta ut alla nämnare ur parenteserna så att alla koefficienter i parenteserna är heltal och sedan även alla

gemensamma faktorer. Efter förkortning har vi då $p(x) = \frac{e}{f}(b_0 + b_1x + \cdots + b_mx^m)(c_0 + c_1x + \cdots + c_ox^o)$ där $e, f, b_i, c_j \in \mathbb{Z}$ och $d(e,f) = d(b_0, b_1, \ldots, b_m) = d(c_0, c_1, \ldots, c_o) = 1$ där $d(e,f) \in \mathbb{Z}$ är det största möjliga heltal där $\frac{e}{d(e,f)}, \frac{f}{d(e,f)} \in \mathbb{Z}$ och $d(b_0, b_1, \ldots, b_m)$, $d(c_0, c_1, \ldots, c_o)$ är motsvarande för $b_0, b_1, \ldots, b_m$ och $c_0, c_1, \ldots, c_o$. Eftersom $b_0, b_1, \ldots, b_m$ inte har några gemensamma faktorer är minst en av dem ej delbar med f, låt den första i summan vara b_i. På samma sätt måste minst en av $c_0, c_1, \ldots, c_o$ ej vara delbara med f, låt den första i summan vara c_j.

Skulle vi nu utveckla $p(x)$ igen får vi att koefficienter $a_{i+j} = \frac{e}{f}(b_0c_{i+j} + \cdots + b_ic_j + \cdots + b_{i+j}c_0)$. Här ser vi att alla termer till vänster om b_ic_j är delbara med f eftersom b_i var den första som inte var delbar med f. Vi ser även att alla termer till höger om b_ic_j är delbara med f eftersom c_j var den första som inte var delbar med f. b_ic_j är dock inte delbar med f så eftersom alla andra termer är det innebär detta att summan i parentesen inte är delbar med f. Men då blir inte a_{i+j} ett heltal, vilket skulle vara en motsägelse mot att $p(x)$ är ett polynom över $\mathbb{Z}$. Alltså måste $f = 1$. Därmed har vi visat att $p(x) = e(b_0 + b_1x + \cdots + b_mx^m)(c_0 + c_1x + \cdots + c_ox^o)$ där $e, b_i, c_j \in \mathbb{Z}$ och därmed att $p(x)$ även är reducibelt över $\mathbb{Z}$.

Alltså har vi visat ett heltalspolynom som är reducibelt över $\mathbb{Q}$ även måste vara reducibelt över $\mathbb{Z}$. Därmed måste även ett heltalspolynom som är irreducibelt över $\mathbb{Z}$ även vara irreducibelt över $\mathbb{Q}$, vilket skulle visas.

Sats 2.2.11 (Eisensteins kriterium): Låt $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ där $a_0, \ldots, a_n \in \mathbb{Z}$ vara ett polynom med koefficienter i $\mathbb{Z}$ och antag att det finns ett primtal p så att p delar $a_0, \ldots, a_{n-1}$ men $p \nmid a_n$ samt att $p^2 \nmid a_0$. Då är $p(x)$ irreducibelt över $\mathbb{Q}$.

Bevis: Låt oss anta att $p(x)$ är reducibelt över $\mathbb{Z}$, det vill säga att $p(x) = (b_0 + b_1x + \cdots + b_mx^m)(c_0 + c_1x + \cdots + c_ox^o)$ för $b_0, b_1, \ldots, b_m, c_0, c_1, \ldots, c_o \in \mathbb{Z}$ och $m, o > 0$ och $m + o = n$.

Vi ser att $a_0 = b_0c_0$ och eftersom a_0 är delbart med p men inte med p^2 så måste p även dela antingen b_0 eller c_0, låt denna vara b_0. Eftersom p inte delar $a_n = b_mc_o$ så delar p varken b_m eller c_o. Låt även b_i vara den första koefficient i vänsterparentesen som inte är delbar med p så måste $0 < i \leq m$.

Utveckling av parenteserna ger att $a_i = b_0c_i + \cdots + b_ic_0$ men eftersom $b_0, b_1, \ldots, b_{i-1}$ är delbara med p men varken b_i eller c_0 är det så är inte heller summan det. Eftersom $m < n$ är detta en motsägelse mot att a_i är delbar med p enligt grundantagandet. Alltså måste antagandet att $p(x)$ är reducibelt över $\mathbb{Z}$ vara felaktigt och därmed måste $p(x)$ vara irreducibelt över $\mathbb{Z}$.

Eftersom $p(x)$ är irreducibelt över $\mathbb{Z}$ måste enligt Gauss lemma (Sats 2.2.10) även $p(x)$ vara irreducibelt över $\mathbb{Q}$, vilket skulle visas.

Nu är vi redo att bevisa att det inte går att konstruera en generell lösningsformel för femtegradsekvationen.

Sats 2.2.12: Den algebraiska femtegradsekvationen $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ är ej lösbar med radikaler för alla $a, b, c, d, e \in \mathbb{C}$.

Bevis: Betrakta polynomet $p(x) = x^5 - 6x + 3$. Enligt Eisensteins kriterium (Sats 2.2.11) är $p(x)$ irreducibelt över $\mathbb{Q}$. Genom en teckenstudie av funktionen $f(x) = p(x)$ ser vi dock att $p(x)$ har tre reella nollställen, exempelvis eftersom $p(-2) = -17$, $p(-0) = 3$, $p(1) = -2$ och $p(2) = 23$. Enligt Abels sats (Sats 2.2.9) är alltså ekvationen $x^5 - 6x + 3 = 0$ ej lösbar med radikaler.

Eftersom vi hittat en femtegradsekvation som inte är lösbar med radikaler innebär detta att femtegradsekvationen generellt inte är lösbar med radikaler, vilket skulle visas.

Enligt vår diskussion om lösningsformler för algebraiska ekvationer i delkapitel 1.3 innebär detta att det inte går det att konstruera en generell algebraisk lösningsformel för femtegradsekvationen. Det är möjligt att visa att ekvationer av högre grad än fem inte heller generellt är lösbara med radikaler, vilket kallas Abel-Ruffini-satsen (Paolo Ruffini gav ett inkomplett bevis för detta 1799 men ett fullständigt bevis för detta gavs som vi skrev tidigare först av Abel). Alltså är det endast ekvationerna av grad ett till fyra som det går att konstruera generella lösningsformler för.

Avslutning

I denna uppsats har vi använt en version av Niels Henrik Abels bevis från 1824 för att bevisa att femtegradsekvationen inte generellt är lösbar med radikaler. Detta bevis är som vi sett något omständligt men samtidigt vackert på det sättet att det endast använder generella egenskaper hos polynom, en följd av huvudsatsen för symmetriska polynom samt ett par enkla exempel på femtegradsekvationer. Idag är det vanligare att dessa resultat bevisas med hjälp av den gruppteori som först utvecklades av Évariste Galois (se exempelvis Christofferson [1]), som var ungefär samtida med Abel.

Att en ekvation inte är lösbar med radikaler innebär dock inte att den inte är lösbar. Med Newton–Raphsons metod (se exempelvis Nagell [5]) eller en variant av denna är det exempelvis möjligt att approximera en lösning till en femtegradsekvation med godtycklig noggrannhet, vilket gör att femtegradsekvationen sedan kan faktoriseras till en approximativ fjärdegradsekvation med övriga nollställen, vilken är lösbar med Ferraris metod eller genom upprepad användning av Newton–Raphsons metod. Idag finns även sätt att generellt avgöra om en femtegradsekvation är lösbar med radikaler eller inte och dessutom algebraiska metoder för att lösa alla femtegradsekvationer som är lösbara med radikaler (se Lazard [4]), något som tyvärr inte fick plats i denna uppsats. Möjligtvis kan detta vara ett ämne för ytterligare en uppsats?

Referenser

[1] Christofferson, Stig (1975). *Grupper, ringar, kroppar*. Lund: LiberLäromedel/ Gleerup.

[2] Hartman, Sven G. (2012). *Det pedagogiska kulturarvet: traditioner och idéer i svensk undervisningshistoria*. 2., [rev] utg. Stockholm: Natur & kultur.

[3] Hellström, Lennart (2002). Elementär algebra. 2. uppl. Lund: Studentlitteratur.

[4] Lazard, Daniel (2002). Solving Quintics by Radicals. I Laudal, Olav Arnfinn & Piene, Ragni (red.) (2004). *The legacy of Niels Henrik Abel: the Abel Bicentennial, Oslo, [June 3-8] 2002*. Berlin: Springer.

[5] Nagell, Trygve (1949). *Lärobok i algebra*. Stockholm: Almqvist & Wisells.

[6] Thompson, Jan (1996). *Matematiken i historien*. Lund: Studentlitteratur.

[7] Skolverket (2015). *Läroplan för grundskolan, förskoleklassen och fritidshemmet 2011: reviderad 2015*. 2. uppl. Stockholm: Skolverket. Tillgänglig på Internet: http://www.skolverket.se/publikationer?id=2575 [2016-05-20].

[8] Skolverket (2017). Ämnesplan i matematik för gymnasieskolan 2011: reviderad 2017. 2. uppl. Stockholm: Skolverket. Tillgänglig på Internet: https://www.skolverket.se/laroplaner-amnen-och-kurser/gymnasieutbildning/gymnasieskola/mat/subject.pdf?subjectCode=MAT&tos=gy&lang=sv [2017-10-10].

[9] Skolöverstyrelsen (1955). *Undervisningsplan för rikets folkskolor den 22 januari 1955* [Elektronisk resurs]. 3. tr. [med tillägg och ändringar] (1958). Stockholm: Norstedt. Tillgänglig på Internet: http://hdl.handle.net/2077/51176 [2017-10-10].