Masteroppgave
Galois-teori

Anders Fjogstad
Universitetet i Stavanger
2011

Sammendrag

Problemstillingen for denne oppgaven er å sette seg inn i Galoisteorien og presentere den på en forståelig måte.
Det er kapitler som tar for seg gruppeteori og kroppsteori, før selve Galoisteorien begynner. I oppgaven tar jeg utgangspunkt i at alle kropper er underkropper av de komplekse tall $\mathbb{C}$ som er en viktig forenkling av Galoisteorien. I lærebøker blir ofte Galoisteorien presentert på en litt annen måte, hvor det er mer snakk om bl.a, endelige kropper. Det som blir kalt Galoisutvidelse i min oppgave, blir ofte kalt *normal utvidelse* i lærebøker.
Et av høydepunktet med oppgaven er slutten av kapittel 6, hvor fundamentalteoremet, også kalt Galoiskorrespondansen utledes. Den forteller at det er en 1-til-1 korrespondanse mellom underkroppene til rotkroppen til et polynom, og undergruppene av polynomets Galoisgruppe.
Dette vises i figuren under, hvor K er rotkroppen til et polynom over en kropp F, og G er Galoisgruppa.

$$\begin{array}{ccc} K & & \{id\} \\ \cup & & \cap \\ \vdots & & \vdots \\ \cup & & \cap \\ E & \leftrightarrow & H = G(K/E) \\ \cup & & \cap \\ \vdots & & \vdots \\ \cup & & \cap \\ F & & G = G(K/F) \end{array}$$

Det blir gjort klart i oppgaven at dette ikke er en metode for å løse likninger, men Galoisteorien viser hvilke polynomer som er løsbare ved rottegn, og hvordan strukturen til disse er. Alle polynom som er løsbare ved rottegn, har en løsbar Galoisgruppe, det vil si, at polynomets Galoisgruppe, har en kjede med normale undergrupper, også kalt et Abelsk tårn, hvor det er en korrespondanse mellom disse normale undergruppene, og underkropper av rotkroppen som svarer til n-te røtter.
Det er gitt korte, men også utfyllende eksempler i oppgaven, hvordan en for noen polynomer kan finne dets Galoisgruppe, og hvordan sammenhengen

mellom rotkroppen og Galoisgruppen til polynomet er.
Selv om Galoisteorien ikke er en algoritme for å løse likninger, er det blitt utformet setninger, korollarer og teoremer, både fra Galois, men også Abels arbeid, som kan hjelpe med å finne et polynoms Galoisgruppe, noe som i mange tilfeller er veldig vanskelig. Finner man et polynoms Galoisgruppe, er det lettere å bestemme om dette polynomet er løsbart ved rottegn. Dette blir beskrevet i del 7.
Husk at alle polynom til og med fjerde grad, er løsbare ved rottegn, men det er ved femtegradspolynom at det blir vanskelig. Til slutt er en grov skisse av Abels teorem tatt med, slik at dette kan sammenlignes med Galois' teorem om at det ikke finnes en generell formel for å finne røttene til et n-tegradspolynom, hvor $n \geq 5$, siden ikke alle polynom av grad $n \geq 5$ kan løses ved rottegn.
Galois' bevis er relativt enkelt når man er kommet til den delen, og det viser på en flott måte hvorfor ikke alle polynom er løsbare ved rottegn.

Innhold

1 Innledning **6**

2 Likninger **8**
2.1 Andregradslikninger 8
2.2 Tredjegradslikninger 11
2.3 Fjerdegradslikninger 15

3 Mengde- og Gruppeteori **18**
3.1 Mengder 18
3.1.1 Andre notasjoner 18
3.2 Binær operasjon 19
3.2.1 Eksempler på binære operasjoner 19
3.3 Grupper 21
3.3.1 Notasjoner og eksempler 24
3.3.2 Homomorfisme 26
3.3.3 Isomorfisme 26
3.3.4 Undergrupper 28
3.3.5 Permutasjonsgrupper 28
3.3.6 Sykliske grupper 29
3.3.7 Normale undergrupper og kvotientgrupper 29
3.4 Oppsummering 35

4 Ringer og kropper **36**
4.1 Ringer 36
4.2 Kropper 38
4.3 Ring- og kroppshomomorfisme 38
4.4 Embedding 39
4.5 Automorfisme 40
4.6 Kroppsutvidelse 41
4.7 Faktorisering av polynomer over en kropp 41
4.8 Fikskropp 42
4.9 Irredusible polynomer 42
4.9.1 Eisensteins kriterium 43
4.10 Kroppsutvidelse fortsetter 43
4.10.1 Algebraiske og transcendentale elementer 43
4.10.2 Minimalpolynomet for α over F 44
4.10.3 Enkel kroppsutvidelse 45
4.10.4 Vektorrom 47
4.10.5 Endelig kroppsutvidelse 48

4.11 Embedding fortsetter 49
4.12 Oppsummering 54

5 Biografier **56**
5.1 Niels Henrik Abel 56
5.2 Èvariste Galois 59

6 Galoisteori **62**
6.1 Rotkropp 62
6.2 Galoisgruppe 64
6.3 Fundamentalteoremet for Galoisteori 66
6.4 Oppsummering 78

7 Løsbarhet ved rottegn **79**
7.1 Abels bevis 81
7.2 Andregradspolynom 83
7.3 Tredjegradspolynom 84
7.4 Fjerdegradspolynom 85
7.5 Polynom av høyere grad 87
7.6 Andre anvendelser 90
7.7 Oppsummering 93

8 Konklusjon **94**

9 Avslutning **95**

10 Kilder **96**

11 Stikkordsregister **98**

1 Innledning

En masteroppgave er den avsluttende eksamenen av et masterprogram. I mitt tilfellet, hvor mastergraden heter, Mastergrad i realfag m/teknologi, også kalt lektorutdannelse, ga det meg et ganske fritt spillerom når det gjalt valg av tema for denne oppgaven. Fagmessig, var det aldri noen tvil om at jeg skulle skrive om matematikk, men hvilket tema, var en annen historie. Etter mye frem og tilbake, endte det til slutt med Galoisteori.

Grunnen til at jeg valgte å skrive om Galoisteori, var at dette er at helt nytt emne for meg innen tallteorien (grenen av matematikk jeg liker best), og som byr på mange utfordringer. Den største utfordringen er såklart å lære seg nye ting på egen hånd, for så å skrive om det og vise hvordan dette brukes.
I tillegg til all den nye algebraen jeg har lært meg, har jeg også måtte tenke på selve oppgaveskrivingen, at dette skal være en oppgave som skal følge en noen lunde bestemt mal, og som skal være så lettleselig som mulig.
Oppgaveskriving generelt, er noe jeg ikke har vært så mye borti på dette studiet, og dermed byr dette også på mange utfordringer.
En oppgave av denne typen, skal egentlig være en ganske rent teoretisk oppgave, men det byr også på vanskeligheter, som blant annet hvor formelt skal ting være skrevet, hvor dypt skal en gå inn i stoffet, og hvordan skal en skille ut hva som er viktig og hva som er mindre viktig.
En masteroppgave skal ha en viss størrelse, men det er lett å grave seg for langt ned i ting, så det er viktig i mange tilfeller å tenke kvalitet ovenfor kvantitet.

Oppgaven er bygget opp gradvis slik at leseren kan henge med på det som skjer, men en må ha hatt en del matematikk for å forstå det som er skrevet. Oppgaven er bygget opp på noen lunne lik måte som jeg har lært ting selv, slik at den røde tråden skal være synlig gjennom hele oppgaven. Det at oppgaven skal følge denne røde tråden har til tider ikke vært like lett, men den skal nå være god. Språket som er brukt i oppgaven er relativt lettleselig, slik at forklaringer og andre kommentarer blir så forståelige som mulig.
De kapitlene som består av mye teori, har en oppsummeringssdel på slutten, som samler opp de viktigste resultatene, viser hvilke kilder jeg har brukt, og viser sammenhengen mellom de forskjellige viktige punktene.

Starten av oppgaven er en historisk del om andre-, tredje-, og fjerdegradslikninger. Grunnen til at jeg valgte å ta med dette, var først og fremst for å vise at andre-, tredje-, og fjerdegradslikninger kan løses med en generell formel, og for å kunne sette dette litt i historisk perspektiv. Selv om andre-,

tredje-, og fjerdegradslikninger ble løst på 1500-tallet, ble ikke det faktum om at den generelle femtegradslikningen ikke kunne løses ved rottegn bestemt før ca 300 år senere.
Etter denne delen begynner jeg så smått å bygge opp oppgaven med helt enkel teori, som utvikler seg til et høyt abstrakt nivå. Jeg begynner altså med helt grunnleggende begreper og bygger gradvis på.
Oppgaven består av mye innenfor gruppeteori, derfor begynner oppgaven med helt basic ting, som å beskrive hva en gruppe er.
Omtrent midt i oppgaven ligger to korte biografier, av Galois og Abel. Grunnen til at jeg har tatt med biografien til Abel, er at han var den første som fant et skikkelig bevis for at det ikke finnes noen generell formel for å løse likninger av orden 5 eller høyere. Galois beviste det samme, men på en annen måte. Mot slutten av oppgaven vises Galois' bevis og en grov skisse av Abels bevis, slik at leseren kan sammenligne disse.
En annen grunn til at jeg har skrevet litt om Abel, er at han var på sin tid en av de største innen fagfeltet om likninger, og det er mye likheter mellom hans, og Galois' teori. I tillegg hadde ikke Norge særlig mange gode matematikere på denne tiden, og var lite annerkjent i matematikkverden, og derfor synes jeg det er viktig å være litt patriotisk og vise litt hvordan det var.

Oppgaven vil presentere Galoisteorien på fra to forskjellige vinkler; den metoden som Galois brukte, med permutasjoner av løsningene til et polynom, og den nymoderne, ved hjelp av automorfismegrupper.
Det at Galoisteorien er presentert på to måter, gir både meg som forfatter, men også deg som leser anledning til å reflektere over det en leser og se sammenhengen mellom den gamle og denne nye måten å presentere dette temaet på.

Jeg har skrevet oppgaven i Latex, og grunnen til dette, er at det gir en bedre oversikt, og et mer profesjonelt preg. Dette var i forkant, et nytt program for meg, og det har tatt litt tid å sette seg inn i det. Til utregninger har jeg brukt Maple 13 mye. Dette er et veldig bra program som gjør det mulig å regne ut det meste. Jeg har brukt programmet til forskjellige utregninger, og til å sjekke svarene mine, når jeg har regnet for hånd.

2 Likninger

Refereanse til dette kapittelet om likninger er Tignol [7], kapittel 1 - 3.

2.1 Andregradslikninger

Andregradslikninger er noe de fleste studenter møter en eller annen gang i løpet av videregående skole, og for mange er den typiske abc-formelen et sant mareritt.
Den generelle andregradslikningen skrives slik: $ax^2 + bx + c = 0$
Andregradslikninger har blitt løst i over 4000 år, derfor er det kanskje litt rart å tenke seg at den generelle formelen for å løse andregradslikninger ikke kom før rundt det 17. århundre.

Det å finne løsningen til den generelle andregradslikningen, og dermed alle andregradslikninger, kreves en del algebraisk innsikt, og under vises det hvordan man gjør.
Den generelle andregradslikningen:

$$ax^2 + bx + c = 0$$

Deler med a:

$$x^2 + \frac{bx}{a} + \frac{c}{a} = 0$$

For å få litt mer orden i uttrykket, kaller man $\left(\frac{b}{a}\right)$ for p, og $\left(\frac{c}{a}\right)$ for q.

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

Legger til $\left(\frac{p}{2}\right)^2$ på begge sider:

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

Det å kunne se at man skal legge til $\left(\frac{p}{2}\right)^2$ er trikset for å finne den generelle løsningen for andregradslikningen. Denne metoden kalles å fullføre kvadratet.

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

Dette kan vises ved å gange ut parantesene:

$$\begin{aligned}\left(x+\left(\frac{p}{2}\right)\right)^2 &= \left(x+\left(\frac{p}{2}\right)\right)\left(x+\left(\frac{p}{2}\right)\right)\\ &= x^2 + x\left(\frac{p}{2}\right) + x\left(\frac{p}{2}\right) + x\left(\frac{p}{2}\right)^2\\ &= x^2 + 2x\left(\frac{p}{2}\right) + \left(\frac{p}{2}\right)^2\\ &= x^2 + px + \left(\frac{p}{2}\right)^2\end{aligned}$$

Når dette er vist, ser man at man kan skrive:

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

som

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

Det som gjenstår nå, er å få x alene.
For å få x ut av kvadratet til venstre, må det trekkes rot. Trekker man rot på ene siden, må man også trekke rot på andre siden:

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

Flytter ledd som ikke inneholder x til høyre, og får:

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

Setter inn igjen for $p = \left(\frac{b}{a}\right)$ og $q = \left(\frac{c}{a}\right)$, og får:

$$\begin{aligned}x &= -\left(\frac{b}{2a}\right) \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \left(\frac{c}{a}\right)}\\ x &= -\left(\frac{b}{2a}\right) \pm \sqrt{\left(\frac{b^2}{4a^2}\right) - \left(\frac{c}{a}\right)}\end{aligned}$$

For å få en felles nevner, utvider man $\left(\frac{c}{a}\right)$ til $\left(\frac{4ac}{4a^2}\right)$. (Har bare ganget med 4a oppe og nede, som er det samme som å gange med 1, og det er lov)
Står da igjen med uttrykket:

$$x = -\left(\frac{b}{2a}\right) \pm \sqrt{\left(\frac{b^2}{4a^2}\right) - \left(\frac{4ac}{4a^2}\right)}$$

Trekker roten av $4a^2$ og får $2a$, som er fellesnevner.
Står igjen med den velkjente abc-formelen:

$$x = -\left(\frac{b}{2a}\right) \pm \left(\frac{\sqrt{b^2 - 4ac}}{2a}\right)$$

Denne formelen kan brukes til å løse alle andregradslikninger.

2.2 Tredjegradslikninger

Den algebraiske løsningen til likningen: $x^3 + mx = n$, ble først funnet rundt 1515 av Scipione del Ferro, en professor i matematikk i Bologna. Han publiserte aldri resultatet sitt, men metoden ble videreført til noen av studentene hans.
Etter del Ferros død, var det flere som jobbet med å løse tredjegradslikninger, blant annet Niccolo Fontana, også kalt Tartaglia. Han ble utfordret av Antonia Maria Fior, en av del Ferros tidligere elever, til en matematikkonkurranse.
Da Tartaglia hørte at Fior hadde fått løsningene til Ferro, jobbet han på spreng, og fant løsningen akkurat i tide slik at han vant konkurransen.
Nyheten om at Tartaglia hadde funnet løsningen, spredde seg, og en som fikk høre om dette var Girolamo Cardano. Cardano var en veldig allsidig forsker, som hadde gitt ut bøker på veldig mange emner, blant annet matematikk.
Cardano spurte Tartaglia om han kunne få løsningen, men Tartaglia nektet, siden han hadde selv planlagt å skrive en bok om emnet. Historien forteller at Tartaglia senere endret mening, for hvis han endring fortsatt er uklar.
Han ga Cardano løsningen til:

$$x^3 + mx = n \text{ og}$$
$$x^3 = mx + n$$

og en kort forklaring til

$$x^3 + n = mx.$$

Med moderne notasjoner, skriver vi at for å finne løsningen til:

$$x^3 + mx = n,$$

trenger vi å finne t og u, slik at:

$$t - u = n \text{ og } tu = \left(\frac{m}{3}\right)^3.$$

Da er:

$$x = \sqrt[3]{t} - \sqrt[3]{u}.$$

Løsningene til t og u blir:

$$t = \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} + \left(\frac{n}{2}\right), \text{ og}$$
$$u = \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} - \left(\frac{n}{2}\right).$$

Da kan en løsning av $x^3 + mx = n$, bli gitt med denne formelen:

$$x = \sqrt[3]{\sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} + \left(\frac{n}{2}\right)} - \sqrt[3]{\sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} - \left(\frac{n}{2}\right)}.$$

Når Cardano hadde mottatt Tartaglias løsninger, begynte han å jobbe med dette. Han fant beviser for løsningene til Tartaglia, og han løste alle andre typer tredjegradslikninger. Han publiserte resultatene sine i boka: *Ars Magna, sive de regulis algebraicis (The Great Art, or the Rules of Algebra)* Under vises Cardanos metode for hvordan en løser den generelle tredjegradslikningen.

$$x^3 + ax^2 + bx + c = 0.$$

Første steg er å endre på variabler. Setter $y = x + \left(\frac{a}{3}\right)$. Da forsvinner andregradsleddet, og vi står igjen med:

$$y^3 + py + q = 0$$

hvor:

$$p = b - \left(\frac{a^2}{3}\right) \text{ og } q = c - \left(\frac{a}{3}\right) b + 2\left(\frac{a}{3}\right)^3.$$

Dersom $y = \sqrt[3]{t} + \sqrt[3]{u}$, får vi:

$$y^3 = t + u + 3\sqrt[3]{tu}(\sqrt[3]{t} + \sqrt[3]{u})$$

og $y^3 + py + q = 0$, blir:

$$(t + u + q) + (3\sqrt[3]{tu} + p)(\sqrt[3]{t} + \sqrt[3]{u}) = 0.$$

Dette systemet har løsningen:

$$t, u = -\left(\frac{q}{2}\right) \pm \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}$$

og løsningen til $y^3 + py + q = 0$, blir:

$$y = \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\left(\frac{q}{2}\right) - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}.$$

Ved bruk av Cardanos formel, kom man av og til forbi noen rare svar. Ta eksempelet:

$$x^3 + 16 = 12x.$$

En kan se at $x = 2$ er en løsning her, men Cardanos formel gir svaret:

$$x = \sqrt[3]{(-8)} + \sqrt[3]{(-8)} = -4.$$

Det er sannsynlig at et resultat som dette fikk Cardano til å undersøke hvor mange løsninger en tredjegradslikning egentlig har. Han mente det var 3 løsninger, inklusivt de negative, som Cardano selv kalte falske, eller oppdiktede. Et annet eksempel er:

$$x^3 = 15x + 4.$$

Her kan man se at $x = 4$ må være en løsning, men Cardanos formel gir:

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

Lenge ble Cardanos formel diskutert etter at løsninger på denne formen ble oppdaget, men diskusjonen fikk til slutt et bra biprodukt, nemlig bruken av de komplekse tall.

I dag bruker man (hvertfall med programmer og lignende) denne formelen for å finne de tre røttene:

$$
\begin{aligned}
r_1 &= -\frac{a}{3} + \left(\frac{-2a^3+9ab-27c+\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)^{1/3} \\
&\quad + \left(\frac{-2a^3+9ab-27c-\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)^{1/3} \\
r_2 &= -\frac{a}{3} - \frac{1+i\sqrt{3}}{2}\left(\frac{-2a^3+9ab-27c+\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)^{1/3} \\
&\quad + \frac{-1+i\sqrt{3}}{2}\left(\frac{-2a^3+9ab-27c-\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)^{1/3} \\
r_3 &= -\frac{a}{3} + \frac{-1+i\sqrt{3}}{2}\left(\frac{-2a^3+9ab-27c+\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)^{1/3} \\
&\quad - \frac{1+i\sqrt{3}}{2}\left(\frac{-2a^3+9ab-27c-\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)^{1/3}
\end{aligned}
$$

Setter $\alpha = \left(\frac{-2a^3+9ab-27c+\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)$ og
$\beta = \left(\frac{-2a^3+9ab-27c-\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}\right)$

Kan da forenkle disse tre røttene til:

$$
\begin{aligned}
r_1 &= -\frac{a}{3} + \sqrt[3]{\alpha} + \sqrt[3]{\beta} \\
r_2 &= -\frac{a}{3} - \frac{1+i\sqrt{3}}{2}\sqrt[3]{\alpha} + \sqrt[3]{\beta} \\
r_3 &= -\frac{a}{3} + \frac{-1+i\sqrt{3}}{2}\sqrt[3]{\alpha} - \sqrt[3]{\beta}
\end{aligned}
$$

2.3 Fjerdegradslikninger

Løsninger av fjerdegradslikninger ble funnet kort tid etter løsninger av likninger av tredje grad. Det var Ludovico Ferrari, en elev av Cardano som først løste fjerdegradslikninger. Ferraris metode er ganske genial, og bygger hovedsakelig på transformering av likninger, men interessen for fjerdegradslikninger ble langt i fra like stor som for tredjegradslikninger. Grunnen til dette var at vanlige likninger representerte ei linje, andregradslikninger representerte kvadratet og tredjegradslikninger representerte kuben. De mente det var idioti å gå forbi det stadiet, siden en fjerde dimensjon ikke lå i naturen. Under ser vi på Ferraris metode for å løse fjerdegradslikninger:

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

Setter $y = x + \left(\frac{a}{4}\right)$. Da blir leddet av tredje grad kansellert og vi står igjen med:

$$y^4 + py^2 + qy + r = 0.$$

hvor:

$$\begin{aligned} p &= b - 6\left(\frac{a}{4}\right)^2, \\ q &= c - \left(\frac{a}{2}\right) b + \left(\frac{a}{2}\right)^3, \\ r &= d - \left(\frac{a}{4}\right) c + \left(\frac{a}{4}\right)^2 b - 3\left(\frac{a}{4}\right)^4. \end{aligned}$$

Ved å flytte førstegradsleddet over til høyre og fullføre kvadratet på venstre side, får vi:

$$\left(y^2 + \frac{p}{2}\right)^2 = -qy - r + \left(\frac{p}{2}\right)^2.$$

Dersom vi adderer en størrelse u til det kvadrerte uttrykket til venstre, får vi:

$$\left(y^2 + \frac{p}{2} + u\right)^2 = -qy - r + \left(\frac{p}{2}\right)^2 + 2uy^2 + pu + u^2.$$

Ideen med u, er å bestemme denne slik at høyre side også blir et kvadrat. Det kan sees på y^2 og y at dersom høyre side er et kvadrat, så er det et kvadrat av $\sqrt{2u}y - \frac{q}{2\sqrt{2u}}$. Derfor har vi:

$$-qy - r + \left(\frac{p}{2}\right)^2 + 2uy^2 + pu + u^2 = \left(\sqrt{2u}y - \frac{q}{2\sqrt{2u}}\right)^2.$$

Vi kan se at likningen holder, hvis og bare hvis:

$$-r + \left(\frac{p}{2}\right)^2 + pu + u^2 = \frac{q^2}{8u}.$$

Eller, skrevet på en annen måte:

$$8u^3 + 8pu^2 + (2p^28r)u - q^2 = 0.$$

Ved å løse denne tredjegradslikningen, kan vi se for hvilke u som passer slik at $-qy - r + \left(\frac{p}{2}\right)^2 + 2uy^2 + pu + u^2 = \left(\sqrt{2u}y - \frac{q}{2\sqrt{2u}}\right)^2$ blir rett.
Ved å sette sammen de to likningene:

$$\left(y^2 + \left(\frac{p}{2}\right) + u\right)^2 = -qy - r + \left(\frac{p}{2}\right)^2 + 2uy^2 + pu + u^2$$

og

$$-qy - r + \left(\frac{p}{2}\right)^2 + 2uy^2 + pu + u^2 = \left(\sqrt{2u}y - \frac{q}{2\sqrt{2u}}\right)^2$$

får vi :

$$\left(y^2 + \left(\frac{p}{2}\right) + u\right)^2 = \left(\sqrt{2u}y - \frac{q}{2\sqrt{2u}}\right)^2.$$

Som blir:

$$y^2 + \left(\frac{p}{2}\right) + u = \pm\sqrt{2u}y - \frac{q}{2\sqrt{2u}}.$$

For å fullføre beviset, gjenstår det å se når $u = 0$ er en rot av

$$8u^3 + 8pu^2 + (2p^28r)u - q^2 = 0.$$

Dette skjer bare når $q = 0$.
Dette fører til at løsningen av

$$x^4 + ax^3 + bx^2 + cx + d = 0,$$

blir som følger:
La p, q og r være definert som før og la u være en løsning av

$$8u^3 + 8pu^2 + (2p^2 8r)u - q^2 = 0.$$

.

Dersom $q \neq 0$, er løsningen:

$$x = \varepsilon\sqrt{\frac{u}{2}} + \varepsilon'\sqrt{-\frac{u}{2} - \frac{p}{2} - \frac{\varepsilon q}{2\sqrt{2u}}} - \frac{a}{4}.$$

Både her og under, står ε og ε for ± 1.
Dersom $q = 0$, blir løsningen:

$$x = \varepsilon\sqrt{-\frac{p}{2} + \varepsilon'\sqrt{\left(\frac{p}{2}\right)^2 - r}} - \frac{a}{4}.$$

Løsningen til de fire røttene som vi bruker i dag, er for lang til å skrive opp, men her er en link hvor løsningene vises:

http://planetmath.org/encyclopedia/QuarticFormula.html

3 Mengde- og Gruppeteori

3.1 Mengder

En mengde er en samling av objekter.
En mengde blir betegnet med en stor bokstav, f.eks: M, og objektene i mengden settes innenfor klammeparanteser: {, }.
Det finnes en mengde uten objekter, den mengden kalles *den tomme mengde*.
Vi bruker notasjonen: $\emptyset$, for den tomme mengde.
Dersom et objekt, a er inneholdt i en mengde, M, skriver vi: $a \in M$, dersom a ikke er inneholdt i M, skriver vi: $a \notin M$.

Eksempel : $M = \{1, 2, 3\}$.
Dette er en mengde som inneholder tallene 1, 2 og 3.
Vi kan også se her at: $2 \in M$, mens $4 \notin M$.

Eksempel : $M = \{\ldots -2, -1, 0, 1, 2, \ldots\}$.
Denne mengden inneholder alle heltall, også betegnet som $\mathbb{Z}$.

3.1.1 Andre notasjoner

En del andre notasjoner blir brukt fremover, og under står betydningen:
$\Rightarrow$ = Fører til (impliserer).
$\exists$ = Det eksisterer.
$\forall$ = For alle.
$\subseteq$ = Delmengde.
$F[x]$ = Polynomene med koeffisienter i kroppen F.
$\{a^n \mid n \in \mathbb{Z}\}$ = Mengden av a^n hvor $n \in \mathbb{Z}$.
E/F. En kroppsutvidelse $F \subseteq E$.
$\mathbb{N}$ = De naturlige tall.
$\mathbb{Z}$ = De hele tall.
$\mathbb{Q}$ = De rasjonelle tall.
$\mathbb{R}$ = De reelle tall.
$\mathbb{C}$ = De komplekse tall.
$\mathbb{C}^* = \mathbb{C} - \{0\}$. De komplekse tall utenom elementet 0.

En *avbildning* eller *funksjon* $f : A \to B$ er en regel som til hvert element $a \in A$ tilordner ett element $f(a) = B$.

3.2 Binær operasjon

La M være en mengde. En *binær operasjon*, $*$ i M er en regel som til alle ordna par av objekter (a, b), der $a, b \in M$, tilordner ett og kun ett objekt $a * b$ i M.
Vi sier også at operasjonen $*$ er *lukket* i M.
Det at operasjonen $*$ er *lukket i* M, betyr at dersom a, b ligger i mengden M, må også $a * b$ ligge i samme mengden M. Vi skriver:

$$a, b \in M \Rightarrow a * b \in M, \forall\, a, b \in M.$$

3.2.1 Eksempler på binære operasjoner

Under tar vi med noen av de vanligste binære operasjonene, og eksempler på hvordan de fungerer.

1. Vanlig addisjon, noteres $+$. Denne binære operasjonen er lukket i bl.a disse tallmengdene: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$.

2. Vanlig multiplikasjon, noteres $\cdot$. Denne binære operasjonen er lukket i bl.a disse tallmengdene: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$.

3. *Sammensetning av funksjoner*, noteres $\circ$. La F være mengden av alle funksjoner $f : \mathbb{R} \to \mathbb{R}$. Dersom f, g er funksjoner i F, definerer vi den sammensatte funksjonen $f \circ g$ ved:

   $$(f \circ g)(x) := f(g(x)).$$

   Da er også $(f \circ g)(x)$ definert for hele $\mathbb{R}$, dvs $f \circ g \in F$.

   Eksempel : Anta at $f(x) = x^2 - 1$ og $g(x) = x + 4$. Da er:

   $$(f \circ g)(x) = f(g(x)) = f(x + 4) = (x + 4)^2 - 1 = x^2 + 8x + 15.$$

   $\circ$ er altså en lukket binær operasjon i mengden F.

4. *Addisjon modulo* n, noteres $+_n$.

$$a +_n b := a + b \ (mod\ n).$$

Denne binær operasjonen kan defineres for alle hele tall n ≥ 2, som da blir en lukket binær operasjon i $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$.

5. I $\mathbb{Z}_n$ har vi også den lukka operasjonen *multiplikasjon modulo n*, noteres $\cdot_n$.

$$a \cdot_n b := a \cdot b \ (mod\ n).$$

Bemerkning : Når man regner *modulo n*, finner man heltallsresten etter vi har dividert med tallet n. Vi illustrerer med et eksempel:

Eksempel : $5 + 3 \equiv 2 \ (mod\ 6)$ eller $5 +_6 3 = 2$.

3.3 Grupper

Definisjon 3.1. *En mengde G sammen med en binær operasjon, $*$, i G, kalles en gruppe dersom følgende krav er oppfylt:*

1. *Operasjonen $*$ er lukket i G, dvs for alle $a, b \in G$ gjelder:*

$$a, b \in G \Rightarrow a * b \in G.$$

2. *Operajonen er assosiativ, dvs for alle $a, b, c \in G$ gjelder:*

$$(a * b) * c = a * (b * c).$$

3. *Det eksisterer et element $e \in G$ slik at for alle $a \in G$ gjelder:*

$$e * a = a * e = a.$$

   Elementet e kalles et identitetselement *i G.*

4. *For hver $a \in G$ finnes et element $b \in G$ som oppfyller:*

$$a * b = b * a = e.$$

   Elementet b kalles en invers *til a.*

En gruppe med mengde G og operasjon, $*$, noteres ofte: $(G, *)$

Setning 1. *En gruppe $(G, *)$ har ett identiteselement.*

Bevis : Vi tar utgangspunkt at det eksisterer to identitetselement: e og e', i G. Siden e er et identitetselement, må $e * e' = e'$, men siden e' også er et identitetselement, må: $e * e' = e$. Dette betyr at $e = e'$, og vi ser at identitetselementet er unikt.

Setning 2. *La G være en gruppe. Da har hvert element i G en unik invers.*

Bevis : Vi vet fra gruppebetingelsene at for et element $a \in G$ finnes et element $b \in G$ slik at:

$$a * b = b * a = e,$$

hvor e er identeitetselementet. La oss anta at det også eksisterer et element b' slik at:

$$a * b' = b' * a = e.$$

Da vil:

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'.$$

Dette betyr at $b = b'$, og vi ser at inversen er unik.

Definisjon 3.2. *En gruppe G er* abelsk *dersom binær operasjonen er kommutativ, dvs: $a * b = b * a$.*

Definisjon 3.3. *La G være en gruppe. Da er ordenen $|G|$, til gruppa G, antallet elementer i G.*

Forskjellen på en endelig og en uendelig gruppe, er bestemt av elementene i gruppa. En endelig gruppe har et endelig antall elementer, mens en uendelig gruppe ikke har det.

Eksempel : La oss se på mengdene $\mathbb{Q}^*$, $\mathbb{R}^*$ og $\mathbb{C}^*$ med vanlig multiplikasjon som binær operasjon. Minner om at * betyr at $\{0\}$ ikke er med i mengden. La oss sjekke om disse mengdene er grupper.

1. Er operasjonen lukket i disse mengdene? Ja, for dersom man tar to vilkårlige element a, b i en av disse mengdene, vil $a \cdot b$ også ligge i mengden.

2. Er operasjonen assosiativ? Ja, siden multiplikasjon er assosiativ.

3. Eksisterer det et identitetselement i mengdene? Ja, siden operasjonen er multiplikasjon, er identitetselementet 1, og 1 er inneholdt i disse tre mengdene.

4. Har hvert element en invers? Ja, for dersom man tar et vilkårlig element a i en av mengdene, vil det finnes et element b i samme mengde slik at $a \cdot b = 1$.

Disse mengdene er altså grupper, og siden de har uendelig mange elementer, er de uendelige grupper.
De er også abelske grupper, siden multiplikasjon er kommutativ.

En måte å sjekke om en mengde er en gruppe, er å sette opp en tabell for binæroperasjonen $*$. Under vises hvordan en slik tabell settes opp, og hvordan man går frem for å se om mengden er en gruppe.

Eksempel: La $G = \{1, -1, i, -i\}$ og binæroperasjonen er vanlig multiplikasjon.
Vi setter opp en tabell på denne måten:
- Vi plasserer elementene i mengden øverst og lengst til venstre. Resten av tabellen er i dette tilfellet produktet (pga multiplikasjon) av de forskjellige par av elementer i mengden.

G ·	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Sjekker gruppebetingelsene for å se om dette er en gruppe:

1. Er operasjonen lukket? Ja, siden $a \cdot b$ ligger i G for alle $a, b \in G$.

2. Er operasjonen assosiativ? Ja, siden multiplikasjon av komplekse tall er assosiativ.

3. Eksisterer det et identitetselement i mengden G? Ja, siden operasjonen er multiplikasjon, er identitetselementet 1, og $1 \in G$.

4. Har hvert element en invers? Ja. Dette er enkelt å se direkte ut i fra tabellen.

Mengden $G = \{1, -1, i, -i\}$ sammen med binær operasjonen, multiplikasjon, er altså en gruppe. Den er også endelig og abelsk, siden den har endelig mange elementer, og multiplikasjon er kommutativ.

3.3.1 Notasjoner og eksempler

Jeg minner om at største felles faktor for to elementer $a, b \in \mathbb{Z}$, noteres $gcd(a, b)$, og er det største tallet $n \in \mathbb{Z}$ som går opp i både a og b.
$gcd(4, 10) = 2$.

To elementer $a, b \in \mathbb{Z}$ er *relativt primiske* dersom $gcd = 1$.

R_n er definert som mengden av alle $x \in \mathbb{Z}_n$ som er relativt primiske med n.
$R_{12} = \{1, 5, 7, 11\}$

Eksempel : La oss vise at mengden, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, med addisjon modulo 5, $+_5$, som binær operasjon, er en gruppe.
Vi setter opp en tabell:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Sjekker gruppebetingelsene for å se om dette er en gruppe:

1. Er operasjonen lukket? Ja, siden $a +_5 b$ ligger i $\mathbb{Z}_5$ for alle $a, b \in \mathbb{Z}_5$.

2. Er operasjonen assosiativ? Ja, vet generelt at $+_n$ er assosiativ.

3. Eksisterer det et identitetselement i mengden $\mathbb{Z}_5$? Ja, siden operasjonen er addisjon, er identitetselementet 0, og $0 \in \mathbb{Z}_5$.

4. Har hvert element en invers? Ja. Dette er enkelt å se ut i fra tabellen.

Ser ut i fra dette at $(\mathbb{Z}_5)$ er en endelig gruppe. Tabellen viser også at dette er en abelsk gruppe.
Generelt er $(\mathbb{Z}_n, +_n)$ en abelsk gruppe.

Eksempel : Vi har mengden $R_{12} = \{1, 5, 7, 11\}$, som er de tallene som er relativt primiske med 12, og har multiplikasjon som binæroperasjon. Vi setter opp en tabell for R_{12}:

$R_{\cdot 12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Sjekker gruppebetingelsene for å se om dette er en gruppe:

1. Er operasjonen lukket? Ja, siden $a \cdot b$ ligger i G for alle $a, b \in G$.

2. Er operasjonen assosiativ? Ja, siden multiplikasjon er assosiativ.

3. Eksisterer det et identitetselement i mengden G? Ja, siden operasjonen er multiplikasjon, eridentitetselementet 1, og $1 \in \mathbb{R}_{12}$.

4. Har hvert element en invers? Ja. Dette er enkelt å se ut i fra tabellen.

Mengden $R_{12} = \{1, 5, 7, 11\}$ med multiplikasjon som binær operasjon er også endelig gruppe.

3.3.2 Homomorfisme

Definisjon 3.4. *La G og G' være grupper. Da er en gruppehomomorfisme en avbildning $\phi : G \to G'$ slik at for alle $a, b \in G$. gjelder:*

$$\phi(a * b) = \phi(a) * \phi(b),$$

hvor binæroperasjonen på venstre side er binæroperasjonen til G, mens den på høyre side er binæroperasjonen til G'.

Eksempel : La oss se på gruppa $(\mathbb{R}, +)$, og definerer $\phi : \mathbb{R} \to \mathbb{R} = 3x$, hvor binæroperasjonen er addisjon:

$$\phi(x + y) = 3(x + y) = 3x + 3y = \phi(a) + \phi(b).$$

Dersom vi har gruppa $(\mathbb{R}, +)$ og definerer $\phi : \mathbb{R} \to \mathbb{R} = 3x$, vil dette være en gruppehomomorfisme.
Homomorfisme er i all sin generellhet, en avbildning (funksjon) fra et algebraisk system til et annet, slik at systemets struktur bevares.
Dette gjelder for grupper, som vi ser på nå, men senere, også ringer og kropper.

Før vi definerer isomorfisme, minner jeg om noen begreper om funksjoner:

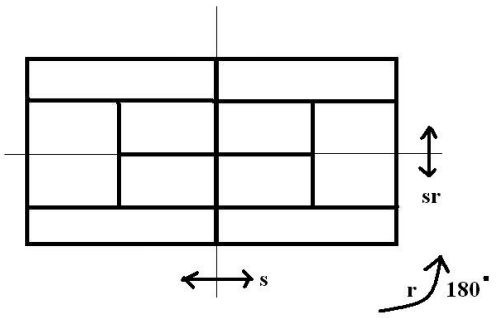
La $f : G \to G'$ være en funksjon (avbildning).
Injektiv : Dersom x og y er elementer i G, og $x \neq y$, så er $f(x) \neq f(y), \forall x, y \in G$.
Surjektiv : For et hvert element $y \in G'$, finnes $x \in G$ slik at $f(x) = y$.
Bijektiv : En funksjon er bijektiv hvis og bare hvis den er både injektiv og surjektiv.

3.3.3 Isomorfisme

Definisjon 3.5. *Dersom en gruppehomomorfisme, $\phi : G \to G'$ er bijektiv, kalles den en isomorfisme. Vi skriver da $G \cong G'$ og G, G' kalles isomorfe grupper.*

Eksempel : Gruppen av de reelle tall med addisjon $(\mathbb{R}, +)$, er isomorf med gruppen av positive reelle tall med multiplikasjon $(\mathbb{R}^+, \cdot)$, via isomorfismen: e^x.
Definer $\phi : \mathbb{R} \to \mathbb{R}^+; \phi(x) = e^x$, er bijektiv, og $\phi(x+y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$.

Eksempel :. La D_2 være symmetriene til et rektangel, dvs de transformasjonene av planet som sender rektangelet over i seg selv. Vi innser at $D_2 = \{e, r, s, rs\}$, hvor e er identitetstransformasjonen, r er rotasjon 180 grader om midtpunktet, s er speiling om vertikal symmetrilinje, og rs er $r \circ s$, som blir speiling om horisontal symmetrilinje.
Da blir D_2 sammen med operasjonen sammensetning en abelsk gruppe.
Under vises et eksempel på en slik figur:



Vis at $R_8 \cong D_2$.
$R_8 = \{1, 3, 5, 7\}$ med $\cdot_8$ som operasjon.
$D_2 = \{e, r, s, rs\}$ et rektangel.

R_8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

D_2	e	r	s	rs
e	e	r	s	rs
r	r	e	rs	s
s	s	rs	e	r
rs	rs	s	r	e

Definerer vi $\phi : R_(\to D_2$ ved $1 \mapsto e, 3 \mapsto r, 5 \mapsto s$ og $7 \mapsto rs$ ser vi fra tabellen at ϕ er en isomorfisme.

3.3.4 Undergrupper

Definisjon 3.6. *En delmengde $H < G$, kalles en* undergruppe *av G, dersom:*

1. *H er lukket under operasjonen i G.*

2. *Identitetselementet $e \in G$ ligger i H.*

3. *For hver $x \in H$ er også $x^{-1} \in H$.*

Notasjonen $H \leq G$ beskriver at H er en undergruppe av G.
Merk at i alle grupper G er $\{e\} < G$ og $G < G$.

Eksempel : $\mathbb{Q}$ med addisjon som binæroperasjon er en gruppe, og vi vet at $\mathbb{Z}$, de hele tall, er en delmengde av $\mathbb{Q}$.
Er da $\mathbb{Z}$ en undergruppe av $\mathbb{Q}$?
For å finne det ut, må vi se på definisjonen:

• Er $\mathbb{Z}$ er lukket under addisjon? Ja, for når man adderer to tall i $\mathbb{Z}$, får man et nytt element i $\mathbb{Z}$.
• Er $e \in \mathbb{Z}$? Ja. Når binæroperasjonen er addisjon, er identitetselementet 0, og vi vet at tallet 0 ligger i $\mathbb{Z}$.
• For hver $x \in H$ er også $x^{-1} \in H$. Ja, dette stemmer for $\mathbb{Z}$ når addisjon er binæroperasjonen. For hvert tall $x \in \mathbb{Z}$, er det et tall $-x \in \mathbb{Z}$,
$\mathbb{Z}$ er altså en undergruppe av $\mathbb{Q}$ ($\mathbb{Z} < \mathbb{Q}$).

3.3.5 Permutasjonsgrupper

Definisjon 3.7. *La X være en mengde. En permutasjon av X er en bijektiv avbildning,*

$$\alpha : X \to X.$$

Alle permutasjonene danner en gruppe, S_X, der binæroperasjonen er sammensetning av funksjoner.
Dersom $X = \{1, 2, \ldots, n\}$, skriver vi S_n, som har orden $n!$

Eksempel : $S_3 = \{\epsilon, (123), (132), (12), (13), (23)\}$, hvor jeg forutsetter at leseren kjenner *sykelnotasjon* for permutasjoner.

S_3 er den minste gruppa som ikke er abelsk.
De jamne permutasjonene utgjør en undergruppe A_n av orden $\frac{n!}{2}$.
Permutasjonegrupper brukes i Galoisteorien, fordi Galoisgruppa til et polynom kan oppfattes som en undergruppe av S_n.

3.3.6 Sykliske grupper

Definisjon 3.8. *La G være en gruppe, og la $a \in G$. Da er undergruppa $\{a^n \mid n \in \mathbb{Z}\}$ av G, en* syklisk undergruppe av G, generert av a*, og noteres $<a>$.*

Definisjon 3.9. *Et element, a, av en gruppe G,* genererer *G og er en* generator for *G dersom $<a> = G$. En gruppe G er* syklisk *dersom det finnes minst et element, $a \in G$ som genererer G.*

Eksempel : La oss se på $\mathbb{Z}_4$. Dette er en syklisk gruppe siden den har elementer som genererer gruppa. Disse elementene er 1 og 3.
$\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Generatorene danner gruppa på denne måten:

$$
\begin{aligned}
<1> &= \{n \cdot 1 | n \in \mathbb{Z}\} = \{1 \cdot 1, 2 \cdot 1, 3 \cdot 1, 4 \cdot 1 = 0\} = \mathbb{Z}_4, \\
<3> &= \{n \cdot 3 | n \in \mathbb{Z}\} = \{1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3 = 0\} = \mathbb{Z}_4, \\
\text{mens } <2> &= \{n \cdot 1 | n \in \mathbb{Z}\} = \{1 \cdot 2, 2 \cdot 2\} = \{0, 2\}.
\end{aligned}
$$

Eksempel : De komplekse røttene av likningen $x^n - 1 = 0$ kalles de komplekse n-te enhetsrøttene. De utgjør en gruppe av orden n, fordi hvis $\alpha^n = 1, \beta^n = 1$ er også $(\alpha\beta)^n = 1$, og $(1/\alpha)^n = 1$. Denne gruppa er *syklisk*, generert av f.eks $\omega = e^{i2\pi/n}$, som da kalles en *primitiv* n-te enhetsrot.

3.3.7 Normale undergrupper og kvotientgrupper

Definisjon 3.10. *La G være en gruppe, H en undergruppe av G, og $a \in G$.*

$$
\begin{aligned}
aH &= \{ah : h \in H\} \textit{ kalles et } \text{venstrekosett av H } i \ G, \\
Ha &= \{ha : h \in H\} \textit{ kalles et } \text{høyrekosett av H } i \ G.
\end{aligned}
$$

Dersom operasjonen i G skrives som $+$, skriver vi kosettene som $a + H$ og $H + a$.
Legg merke til at aH' hvor $a \notin H$ ikke er en undergruppe av G, bare en delmengde.

Eksempel : La $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ med operasjon $+_4$ (addisjon modulo 4), og la $H = <2> = \{0, 2\}$. Da blir venstrekosettene til H :

$$\begin{aligned} 0 +_4 H &= \{0 +_4 0, 0 +_4 2\} = \{0, 2\} = H, \\ 1 +_4 H &= \{1 +_4 0, 1 +_4 2\} = \{1, 3\} = 1 + H, \\ 2 +_4 H &= \{2 +_4 0, 2 +_4 2\} = \{2, 0\} = H, \\ 3 +_4 H &= \{3 +_4 0, 3 +_4 2\} = \{3, 1\} = 1 + H. \end{aligned}$$

Så vi får kun 2 ulike venstrekosett. Høyrekosettene blir de samme, siden $\mathbb{Z}_4$ er kommutativ.

Eksempel : Vi lar D_3 være symmetrigruppa til en regulær trekant. Da er $D_3 = <r, s> = \{e, r, r^2, s, rs, r^2 s\}$ med relasjoner $r^3 = s^2 = e, sr = r^2 s$, og lar $H = <s> = \{e, s\}$.
Vi finner lett venstre- og høyrekosettene til H i G:

$$\begin{aligned} eH = sH = H, rH = rsH = \{r, rs\}, r^2 H = r^2 sH = \{r^2, r^2 s\}. \\ He = Hs = H, Hr = Hr^2 s = \{r, r^2 s\}, Hr^2 = Hrs = \{r^2, rs\}. \end{aligned}$$

Merk at venstrekosettene er enten like eller disjunkte (ingen elementer felles), og at alle har 3 elementer. Det samme gjelder høyrekosettene. Dette er faktisk sant helt generelt, men et venstre- og høyrekosett er ikke alltid like, f.eks er $rH \neq Hr$.
Dersom G er kommutativ (abelsk), blir rH og Hr selvsagt alltid like.

Teorem 3.11. *La aH og bH være venstrekosett til en undergruppe H i G. Da gjelder:*

1. *$|aH| = |bH| = H$ når G er endelig.*
2. *Enten er $aH = bH$ eller så er $aH \cap bH = \emptyset$.*

Det samme gjelder for høyrekosett Ha og Hb.
Beviset er lett, se f.eks Lang [5] side 27.

Bemerkning : Teoremet ovenfor gir oss med en gang beviset for Lagranges teorem:

Teorem 3.12. *(Lagrange)*
Ordenen til en undergruppe H av en gruppe G, går opp i ordenen til G.

Definisjon 3.13. *La $x \in G$. Ordenen til $x, ord(x)$, er det minste heltall m ge1 slik at $x^m = e$.*

Teorem 3.14. *(Lagrange)*
La $x \in G$. Da vil $ord(x)$ gå opp i ordenen til G.

Definisjon 3.15. *La H være en undergruppe av G. H kalles en* normal *undergruppe dersom $xH = Hx$ for alle $x \in G$.*
Ekvivalent, H kalles en normal *undergruppe dersom $xHx^{-1} \subseteq H$ for alle $x \in G$.*

En normal undergruppe, H, av en gruppe G noteres: $H \triangleleft G$.
Normale undergrupper blir sentralt når vi kommer til kvotientgrupper, og senere Galoisteoriens fundamentalteorem, derfor er det viktig å forstå dette punktet.

Bemerkning : For alle grupper G er alltid den trivielle gruppa $H = \{e\}$ og $H = G$, normale undergrupper av G.
Dersom G er abelsk, er selvsagt alle undergrupper av G normal undergrupper.

Definisjon 3.16. *En gruppe G kalles* simpel *dersom den ikke har andre normale undergrupper enn $\{e\}$ og G selv.*

Simple undergrupper dukker opp senere i forbindelse med likninger som ikke er løsbare ved rottegn.

Eksempel : Den dihedrale gruppa D_4 er symmetrigruppa til et kvadrat.
$D_4 = < r, s >$, hvor $r^4 = s^2 = e, sr = r^3 s$?
$|D_4| = 8$, så en ekte undergruppe $H < D_4$ har orden 2 eller 4 ifølge Lagranges teorem.
Vi finner 5 undergrupper av orden 2: $< r^2 >, < s >, < rs >, < r^2 s >$ og $< r^3 s >$. Det er 3 undergrupper av orden 4: den sykliske gruppa $< r >$ og de to ikke sykliske gruppene $H_1 = \{e, r^2, s, r^2 s\}$ og $H_2 = \{e, r^2, rs, r^3\}$.
Ved å bruke definisjoenen finner vi etter en del regning at kun $< r^2 >$ og de 3 undergruppene av orden 4 er normal i D_4.

Teorem 3.17. *La H være en normal undergruppe av G. Da danner mengden $\{aH\}$ av venstre kosett av H en gruppe, G/H, under binæroperasjonen $(aH)(bH) = (ab)H$.*

Bevis : Se Lang [5] side 29.

Definisjon 3.18. *Gruppa G/H, i teoremet over, kalles* kvotientgruppa *til G av H.*

Elementene i kvotientgruppa G/H er altså de ulike kosettene xH så ordenen til G/H blir da $|G|/|H|$.
Identitetselement i G/H blir $eH = H$ og $(xH)^{-1} = x^{-1}H$.

Eksempel : $G = (\mathbb{Z}_6, +_6)$, og $H =< 2 >= \{0, 2, 4\}$.
Vi kan nå lett se at ordenen til $G/H = 6/3 = 2$. Vi setter opp en gruppetabell for å se hva som skjer:

$+_6$	0	2	4	1	3	5
0	0	2	4	1	3	5
2	2	4	0	3	5	1
4	4	0	2	5	1	3
1	1	3	5	2	4	0
3	3	5	1	4	0	2
5	5	1	3	0	2	4

Legg merke til at det er ting som går igjen her i tabellen: I hvert delkvadrat inngår kun elementer i de to kosettene til H, nemlig
$H = \{0, 2, 4\} = 0 +_6 H = 2 +_6 H = 4 +_6 H$ og
$\{1, 3, 5\} = 1 +_6 H = 3 +_6 H = 5 +_6 H$.

$+_6$	0	2	4	1	3	5
0	0	2	4	1	3	5
2	2	4	0	3	5	1
4	4	0	2	5	1	3
1	1	3	5	2	4	0
3	3	5	1	4	0	2
5	5	1	3	0	2	4

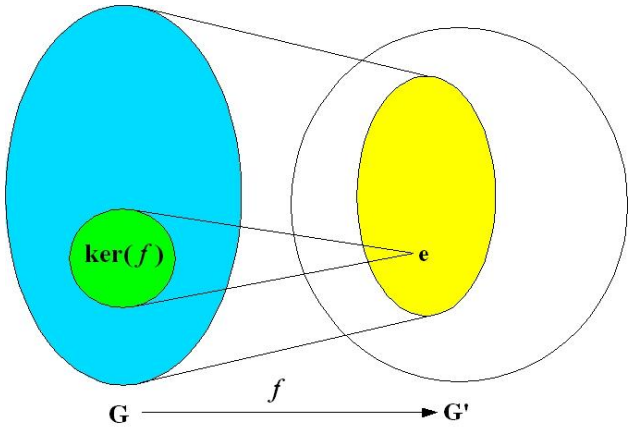
Dersom vi kaller $I = 0 +_6 H$ og $II = 1 +_6 H$, ser vi at G/H er isomorf med $\mathbb{Z}_2$, skriver $G/H \cong \mathbb{Z}_2$:

	I	II
I	I	II
II	II	I

Nyttig observasjon : La G være en gruppe, og H være en undergruppe av G, $H < G$. Anta at $|H| = |G|/2$. Da er $H \lhd G$. F.eks er A_n en normal undergruppe av S_n.

Definisjon 3.19. *La $f : G \to G'$ være en gruppehomomorfisme. Da kalles mengden $\{x \in G \mid f(x) = e'\}$,* kjernen *til f, og skrives $Ker(f)$.*

Med andre ord betyr kjernen til en homomorfisme de elementene i gruppa G som avbildes til identitetselementet i G'.
En figur illustrerer det nok bedre:



Figur 3.1. Kjernen til en homomorfisme.

Eksempel :. La $G = \{1, -1, i, -i\}$ med vanlig multiplikasjon som binæroperasjon.
Definer $\phi : \mathbb{Z} \to G$, ved $(\phi)m = i^m$.
Da er ϕ en gruppehomomorfisme. Finn kjernen til ϕ, $Ker(\phi)$.
Vi leter nå etter tall $m \in \mathbb{Z}$ slik at i^m blir identitetselementet, 1, i G:
Vet at i har orden 4, så $i^m = 1$, kun for $m = 0, \pm 4, \pm 8, \ldots =< 4 >$.
Så vi får

$$Ker(\phi) =< 4 >= \{4k \mid k \in \mathbb{Z}\}.$$

Vi ser at kjernen blir en undergruppe av $\mathbb{Z}$. Dette gjelder generelt.

Teorem 3.20. *La $\phi : G \to G'$ være en gruppehomomorfisme. Da gjelder:*

1. *$Ker(\phi)$ er en normal undergruppe av G : $Ker(\phi) \lhd G$.*

2. Anta ϕ er surjektiv. Da er $G/Ker(\phi) \cong G'$.

Eksempel : Homomorfismen $\phi : \mathbb{Z} \to G = \{1, -1, i, -i\}$ derfinert ved $\phi(m) = i^m$ er klart surjektiv, og vi så ovenfor at $ker(\phi) = < 4 >$. Så teoremet sier da at $\mathbb{Z}/ < 4 > \cong G$, og det stemmer jo:
G er syklisk av orden 4, så $G \cong \mathbb{Z}_4$, og også $\mathbb{Z}/ < 4 > = \mathbb{Z}_4$.

3.4 Oppsummering

• En mengde G, sammen med en binæroperasjon $*$ kalles en *gruppe* dersom:

1. $*$ er lukket i G.
2. $*$ er assosiativ.
3. G inneholder et identitetselement mhp $*$.
4. Hvert element i G har en invers mhp $*$.

• En delmengde L, av M, kalles en *undergruppe* av M dersom gruppeegenskapene holder for L.

• Dersom en gruppe er *kommutativ*, kalles den *Abelsk*.

• La G og G' være grupper. Da er en *gruppehomomorfisme* er en avbildning $\phi : G \to G'$ slik at for alle $a, b \in G$, gjelder: $\phi(a * b) = \phi(a) * \phi(b)$.

• Dersom en gruppehomomorfisme er bijektiv, kalles den en *isomorfisme*.

• En gruppe G er *syklisk* dersom den er generert av et element $a \in G$.

• En undergruppe $H < G$ er *normal* dersom: $xHx^{-1} \subseteq H \forall x \in G$.

• La $f : G \to G'$ være en gruppehomomorfisme. Da kalles mengden av $\{x \in G \mid f(x) = e'\}$, *kjernen* til f, $Ker(f)$.

• La H være en normal undergruppe av G. Da danner mengden $\{aH\}$ av venstre kosett av H en gruppe, G/H, under binæroperasjonen $(aH)(bH) = (ab)H$. Denne gruppa kalles *kvotientgruppa* til G av H.

Kilder i dette kapittelet har vært Fraleigh [3], kap 0 - 6, Lang [5], kap 2, og notater fra kurset Grupper og Symmetri med lærebok Armstrong [1], kap 1 - 11.

4 Ringer og kropper

4.1 Ringer

Definisjon 4.1. *En mengde, R, sammen med to lukkede binære operasjoner $+$ og $\cdot$ (kalt addisjon og multiplikasjon), kalles en* ring *dersom følgende krav er oppfylt:*

1. *R sammen med $+$ utgjør en abelsk gruppe. Identitetselementet noteres 0, og kalles nullelementet i ringen.*
2. *Multiplikasjon er assosiativ og har et identitetselement som noteres 1.*
3. *Multiplikasjon er distributiv over addisjon*

$$a \cdot (b + c) = ab + ac \text{ og } (b + c) \cdot a = ba + ca \ (\forall a, b, c \in R).$$

Kommentarer :

1. Vi antar at $1 \neq 0$.
2. Dersom multiplikasjon er kommutativ, kalles R en *kommutativ ring.*
3. De elementene $a \in R$ som har en multiplikativ invers, (dvs at det eksisterer $b \in R$ slik at $ab = ba = 1$), kalles *enheter* i R.

Eksempel : Et eksempel på en kommutativ ring, er de hele tall, $\mathbb{Z}$ sammen med operajonen $+$, vanlig addisjon.

Eksempel : $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ utgjør en endelig kommutativ ring sammen med operasjonene $+_n$ og $\cdot_n$ (addisjon og multiplikasjon modulo n).

Eksempel : De rasjonale, reelle og komplekse tall $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sammen med vanlig addisjon og multiplikasjon er ringer.

Eksempel : La F stå for $\mathbb{Q}, \mathbb{R}$ eller $\mathbb{C}$.
Alle polynomer med koeffisienter i F utgjør en ring, notert $F[x]$, kalt *polynomringen over F.*

Definisjon 4.2. *La R være en kommutativ ring, og la $a, b \in R$. Dersom $a \neq 0$ og $b \neq 0$, men $ab = 0$, kalles a og b for* nulldivisorer.

Eksempel : $\mathbb{Z}$ har ingen nulldivisorer, men dersom man har ringen $\mathbb{Z}_{12}$ som ble nevn i et tidligere eksempel, er 2, 3, 4, 6, 8, 9, 10 nulldivisorer:

$$2 \cdot_{12} 6 = 0, 3 \cdot_{12} 4 = 0, 8 \cdot_{12} 3 = 0, 9 \cdot_{12} 4 = 0, 10 \cdot_{12} 6 = 0.$$

Teorem 4.3. *La $a \in \mathbb{Z}_n$. Da er a en nulldivisor hvis og bare hvis $gcd(a, n) > 1$, og a er en enhet hvis og bare hvis $gcd(a, n) = 1$.*

Vi ser på eksempelet ovenfor at; 2, 3, 4, 6, 8, 9 og 10 er nulldivisorer av $\mathbb{Z}_{12}$, og det er akkurat de tallene som ikke er relativt primiske med 12.
Gruppen av enheter i $\mathbb{Z}_n$ utgjør gruppen R_n som nevnt i kapittel 3 og brukt i et eksempel i del 3.3.1.

Eksempel : I $\mathbb{Z}_{12}$ er det kun 1, 5, 7 og 11 som er relativt primiske med 12. Gruppa R_n er $\{1, 5, 7, 11\}$ med operasjon $\cdot_{12}$.

Korollar 4.4. *Dersom p er et primtall, har ikke $\mathbb{Z}_p$ noen 0-divisorer, og alle element $\neq 0$ er enheter.*

Dette er selvforklarende fra teorem 4.3, siden alle tall mindre enn p er relativt primiske med p.

4.2 Kropper

Definisjon 4.5. *En* kropp, *R, er en kommutativ ring, der* $(R - \{0\}, \cdot)$ *er en gruppe.*

Det vil si, en kropp er en kommutativ ring der alle element $\neq 0$ har en multiplikativ invers.

Eksempel : Tallmengdene $\mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ sammen med vanlig addisjon og multiplikasjon er kropper. For eksempel, la $z \in \mathbb{C}, z \neq 0.z = a + bi$ hvor $a, b \in \mathbb{R}$. Da vet vi at z har en multiplikativ invers i $\mathbb{C}$, nemlig

$$z^{-1} = \frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Eksempel : $\mathbb{Z}_p$ hvor p er et primtall utgjør en endelig kropp sammen med $+_p$ og $\cdot_p$ (addisjon og multiplikasjon modulo p).

Eksempel : De hele tall $\mathbb{Z}$ utgjør ingen kropp, fordi det kun er 1 og -1 som har multiplikativ invers.

4.3 Ring- og kroppshomomorfisme

Definisjon 4.6. *La R og S være ringer. En ringhomomorfisme er en avbildning* $\phi : R \to S$*, slik at for alle* $a, b \in R$ *gjelder:*

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b); \\ \phi(a \cdot b) &= \phi(a)\phi(b); \\ \phi(1) &= 1.. \end{aligned}$$

Dersom ϕ *er bijektiv, kalles den en isomorfisme.*

Eksempel : Avbildningen

$$\phi : \mathbb{Z} \to \mathbb{Z}_n$$

ved $\phi(a) = a \ (mod\, n)$ er en ringhomomorfisme.

Setning : La K være en kropp og $\phi : K \to S$, en ringhomomorfisme. Da er ϕ injektiv.

Bevis : Viser først at hvis $x \in K, x \neq 0$, så er $\phi(x) \neq 0$.
Siden K er en kropp, finnes $x^{-1} \in K$ slik at $xx^{-1} = 1$. Da blir

$$\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1) = 1, \text{ så } \phi(x) \neq 0.$$

Anta så at $x \neq y$, men anta at $\phi(x) = \phi(y)$. Da er $x - y \neq 0$, men $\phi(x - y) = \phi(x) - \phi(y) = 0$, som strider mot det vi viste først.

En homomorfisme er generelt, en avbildning fra et algebraisk system til et annet, slik at systemenes struktur bevares. Dette gjelder for grupper, ringer og kropper. Siden en kropp er en kommutativ ring, henviser jeg til definisjonen om ringhomomorfisme og ringisomorfisme, hvor de samme punktene gjelder for kroppshomo- og isomorfisme.

Bemerkning : Fra nå av, og resten av oppgaven, tar vi utgangspunkt i at alle kropper er inneholdt i de komplekse tall, $\mathbb{C}$.
$\mathbb{C}$ er en algebraisk lukket kropp, som betyr:

Definisjon 4.7. *En kropp F, er algebraisk lukket dersom hvert ikke-konstant polynom i $F[x]$, har et nullpunkt i F.*

Teorem 4.8. *(Algebraens fundamentalteorem)*
La $f(x) \in \mathbb{C}[x]$ være et polynom av grad $n \geq 1$. Da har $f(x)$ n nullpunkter $\alpha_1, \alpha_2, \ldots, \alpha_n$ i $\mathbb{C}$, og $f(x) = a(x - \alpha_1)\ldots(x - \alpha_n)$ der $a \in \mathbb{C}$.

4.4 Embedding

Definisjon 4.9. *La F og L være kropper. Med en embedding av F i L, mener vi en ringhomomorfisme*

$$\sigma : F \to L.$$

Vi bruker navnet embedding siden vi vet at σ er injektiv når F er en kropp. En embedding er med andre ord at du 'skyver venstre kropp F over i den høyre, L', og får en kopi av F inne i L.

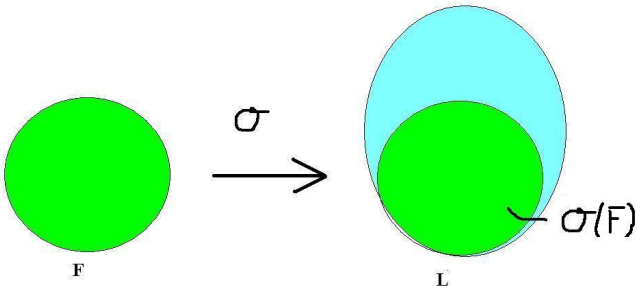
Definisjon 4.10. *La $f(x)$ være et polynom i $F[x]$. La $\sigma : F \to L$ være en embedding. Skriv:*

$$f(x) = a_n x^n + \ldots + a_0.$$

Vi definerer σf til å være polynomet

$$\sigma f(x) = \sigma(a_n)x^n + \ldots + \sigma(a_0).$$

Fra dette ser vi at dersom f, g er to polynom i $F[x]$, så er $\sigma(f+g) = \sigma f + \sigma g$ og $\sigma(fg) = (\sigma f)(\sigma g)$, dvs σ gir opphav til en homomorfisme fra $F[x]$ til $L[x]$.



Figur 4.1. Embedding. $F \to \sigma(F)$ blir en isomorfisme.

4.5 Automorfisme

Definisjon 4.11. *En* automorfisme *av en kropp F, er en isomorfisme σ: $F \to F$ av F med seg selv.*

En automorfisme er på en måte en symmetri av en kropp, og en måte å avbilde kroppen på seg selv, mens strukturen er bevart.

Setning 3. *La F være en kropp. Alle automorfismene til F danner en gruppe under sammensetning, kalt automorfismegruppa til F, $Aut(F)$.*

Bevis : Vi vet at mengden av bijektive avbildninger $F \to F$ danner en gruppe. Poenget er da at hvis σ og τ er automorfismer, er også sammensetningen $\sigma \circ \tau$ en automorfisme.

Eksempel : La oss se på de rasjonale tallene, $\mathbb{Q}$. Denne kroppen har kun *identitets automorfismen*, siden en automorfisme må avbilde elementet 1 på seg selv. Hvert rasjonalt tall kan bli dannet av elementet 1 gjennom operasjonene i en kropp, som er bevart i en automorfisme. La oss se hvordan dette fungerer. Så la $\phi : \mathbb{Q} \to \mathbb{Q}$ være en automorfisme.

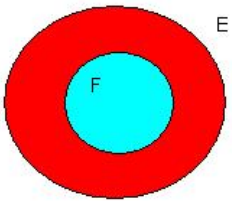
$$\phi\left(\frac{m}{n}\right) = \phi(m)\phi(n^{-1}) = \phi(m)\phi(n)^{-1}$$
$$= \phi(\underbrace{1+\ldots+1}_{\text{m}})\phi(\underbrace{1+\ldots+1}_{\text{n}})^{-1} = m\phi(1)n\phi(1)^{-1} = m \cdot n^{-1} = \frac{m}{n}.$$

dvs $\phi =$ identiteten. Så $Aut(\mathbb{Q}) \equiv \{e\}$.

4.6 Kroppsutvidelse

Definisjon 4.12. *Gitt kroppene $F, E \subseteq \mathbb{C}$, hvor $F \subseteq E$. Da kalles E en utvidelse av F, notert $F \leq E$.*

Det denne definisjonen sier, er at en kropp E, er en utvidelse av en annen kropp, F, dersom F er inneholdt i E, og operasjonene er de samme.
Man kan illustrere dette:



Figur 4.2: Her representerer den røde sirkelen kroppen E, som er en kroppsutvidelse av F

Eksempel : De reelle tall ($\mathbb{R}$) er en kroppsutvidelse av de rasjonelle tall ($\mathbb{Q}$), og de komplekse tall ($\mathbb{C}$) er en kroppsutvidelse av de reelle tall.
Vi skriver:

$$\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$$

Legg merke til at notasjonen for en uspesifisert kropp er F, og kroppsutvidelsen noteres E.

4.7 Faktorisering av polynomer over en kropp

Husk at vi er ute etter å finne nullpunkt i polynom.
La E og F være kropper, hvor E er en utvidelse av F ($F \leq E$)
Tenk deg et polynom $f(x) \in F$, slik at $f(x) = g(x)h(x)$ for $g(x), h(x) \in F[x]$, og la $\alpha \in E$.
Siden $\alpha \in E$, så er $f(\alpha) = 0$ hvis og bare hvis enten $g(\alpha)$ eller $h(\alpha) = 0$. Så, forsøket på å finne et nullpunkt i $f(x)$, er redusert til å finne et nullpunkt i en av faktorene til $f(x)$.
Da ser vi at $f(\alpha) = 0$, hvis og bare hvis enten $g(\alpha)$ eller $h(\alpha) = 0$.

Hvorfor kan vi si det? Jo, for at et produkt skal bli null, må minst en av faktorene være null.

4.8 Fikskropp

Setning 4. *La G være en gruppe av automorfismer av en kropp F. La F^G være mengden av alle elementer $x \in F$, slik at $\sigma x = x$, for alle $\sigma \in G$. Da er F^G en kropp, og kalles* fikskroppen *til G.*

Bevis : Vi skal nå bevise at F^G er en kropp.
F^G inneholder 0 og 1, og dersom $x, y \in F^G$, har vi

$$\sigma(x+y) = \sigma x + \sigma y = x + y,$$
$$\sigma(xy) = \sigma(x) + \sigma(y) = xy,$$

så $x+y$ og $xy \in F^G$. I tillegg er $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}$, så $x^{-1} \in F^G$, og dette beviser at F^G er en kropp.

Eksempel : Kompleks konjugering $\sigma : \mathbb{C} \to \mathbb{C}, \sigma(z) = \bar{z}$, er en automorfisme av $\mathbb{C}$, og $\sigma^2 = id$, så $G = \{id, \sigma\}$ er en gruppe av automorfismer av $\mathbb{C}$. Vi vet at $\bar{z} = z$ hvis og bare hvis $z \in \mathbb{R}$, så fikskroppen til G er $\mathbb{R}$.

4.9 Irredusible polynomer

Definisjon 4.13. *Et polynom $f(x) \in F[x]$ er* irredusibelt *over F, dersom $f(x)$ ikke kan skrives som et produkt $g(x)h(x)$ av to polynom $g(x)$ og $h(x)$ i $F[x]$, hvor begge er av grad lavere enn $f(x)$.*

Dersom $f(x) \in F[x]$ kan skrives som $g(x)h(x)$, kalles $f(x)$ *redusibelt* over F.

Eksempel : $f(x) = x^2 - 2$ er irredusibelt over $\mathbb{Q}$, for hvis vi kunne skrive $x^2 - 2 = (ax+b)(cx+d)$ med $a, b, c, d \in \mathbb{Q}$, ville $f(x)$ hatt rasjonale nullpunkter.

Setning 5. *La $f(x) \in F(x)$ være et polynom av grad 2 eller 3. Hvis $f(x)$ ikke har nullpunkter i F, så er $f(x)$ irredusibelt over F*

Bevis : Dette er klart, fordi hvis $f(x)$ er redusibelt over F, og har grad 2 eller 3, må en av faktorene ha grad 1, som betyr at $f(x)$ har en rot i F.

4.9.1 Eisensteins kriterium

Teorem 4.14. *La oss anta vi har følgende polynom med heltallskoeffisienter:*

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

Dersom det eksisterer et primtall, p, slik at følgende punkter stemmer

1. *p går opp i hver a_i for $i \neq n$;*

2. *p går ikke opp i a_n;*

3. *p^2 går ikke opp i a_0,*

da er $f(x)$ irredusibelt over de rasjonale tall.

Eksempel : Polynom av typen $x^n - p$ der p er et primtall, er irredusible over $\mathbb{Q}$, ved Eisenstein.

Teorem 4.15. *La F være en kropp i $\mathbb{C}$. Anta $f(x) \in F[x]$ er irredusibelt av grad n. Da har $f(x)$ n ulike røtter i $\mathbb{C}$.*

Det er en viktig forenkling av Galoisteorien når vi ser kun på underkropper av de komplekse tall $\mathbb{C}$. (tallkropper).

4.10 Kroppsutvidelse fortsetter

4.10.1 Algebraiske og transcendentale elementer

Definisjon 4.16. *Et element α i en kroppsutvidelse E av en kropp F er* algebraisk *over F dersom $f(\alpha) = 0$ for et polynom $f(x) \neq 0 \in F[x]$.*
Dersom α ikke er algebraisk over F, er α transcendent *over F.*

Eksempel : Så de komplekse tall som er *algebraiske over* $\mathbb{Q}$, er de tall $\alpha \in \mathbb{C}$ som er nullpunkt i et eller annet polynom av grad ≥ 1 med koeffisienter i $\mathbb{Q}$. Det er kjent at f.eks π og e ikke er algebraiske over $\mathbb{Q}$, de er transcendentale.

4.10.2 Minimalpolynomet for α over F

Teorem 4.17. *La E være en kroppsutvidelse av F og la $\alpha \in E$ være algebraisk over F. Da finnes det et monisk polynom, $(x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0)$, $p(x) \in F[x]$ av lavest grad, ≥ 1, slik at $p(\alpha) = 0$, og med følgende egenskaper:*

1. *p(x) er entydig bestemt.*
2. *p(x) er irredusibelt over F.*
3. *Dersom $f(x) \in F[x]$ og $f(\alpha) = 0$, er p(x) en divisor i f(x).*

Polynomet p(x) kalles minimalpolynomet *til α over F, og noteres irr(α , F). Graden til irr(α, F) kalles graden til α over F og noteres grad(α, F).*

Bevis *pkt* 1 : La graden til $p(x) = n \geq 1$, og anta at $p(x)$ er et monisk polynom av grad n med $r(\alpha) = 0$.
Dersom $r(x) \neq p(x)$, vil et konstant multiplum av $r(x) - p(x)$ være et monisk polynom av grad $< n$, med $r(\alpha) - p(\alpha) = 0 - 0 = 0$. Men dette strider mot definisjonen av $p(x)$, følgelig må $r(x) = p(x)$.

Bevis *pkt* 2 : Anta $p(x)$ er redusibelt over F, og skrive $p(x) = f(x)g(x)$, der $f(x)$ og $g(x)$ har lavere grad enn $p(x)$.
Vi kan anta at $f(x)$ og $g(x)$ er moniske. Siden $p(\alpha) = f(\alpha)g(\alpha) = 0$, må enten $f(\alpha) = 0$ eller $g(\alpha) = 0$. Men dette strider mot definisjonen av $p(x)$, følgelig er $p(x)$ irredusibelt over F.

Bevis *pkt* 3 : Sett graden til $p(x) = n \geq 1$ Siden $f(\alpha) = 0$, må graden til $f(x) \geq n$, per dfinisjon av $p(x)$. Ved polynomdivisjon kan vi skrive:

$$f(x) = p(x)q(x) + r(x),$$

der graden til $r(x) < n$ Da vil $r(\alpha) = f(\alpha) - p(\alpha)q(q(\alpha) = 0 - 0 = 0$, så dersom graden $r(x) \geq 1$, vil et konstant multiplum av $r(x)$ gi et monisk polynom av grad $< n$ med α som nullpunkt. Dette strider mot definisjonen av $p(x)$, så vi må ha $r(x) = 0$, og $f(x) = p(x)q(x)$, dvs, $f(x)$ er et multiplum av $p(x)$.

Mange av definisjonene og teoremene kan virke relativt kryptiske i sin kompakte matematiske forklaring, derfor er det viktig å lese gjennom disse og se hva de egentlig sier.

Vi har en kroppsutvidelse $F \leq E$, vi bruker: $\mathbb{Q} \leq \mathbb{R}$. α er et algebraisk element over $\mathbb{Q}$, som eksisterer i $\mathbb{R}$, og vi velger da $\sqrt{2}$.
Da eksisterer det et irredusibelt polynom $p(x) \in F[x]$ slik at $p(\alpha) = 0$. Vi velger da $p(x) = x^2 - 2$, hvor da $p(x)$ er irredusibelt over $F[x]$, men hvor $p(\alpha) = 0$.
Dersom vi da har noen polynomer $f(x) \in F[x]$, hvor $f(x) \neq 0$ og $f(\alpha) = 0$, så er $p(x)$ delelig med $f(x)$.
Når beskrivelsen over begynner å sige inn, er dette selvforklarende. Dersom vi har et polynom $f(x)$ hvor $\sqrt{2}$ er et nullpunkt, kan dette skrives som $f(x) = (x^2 - 2)g(x)$, hvor $g(x)$ er et polynom.
Da ser man lett at $f(x)$ delelig med $p(x)$:

$$\frac{f(x)}{p(x)} = \frac{(x^2 - 2)g(x)}{(x^2 - 2)} = g(x).$$

Eksempel : La $\alpha = \sqrt[n]{p}$ der p er et primtall og $n \geq 2$, la $p(x) = x^n - p, \in \mathbb{Q}[x]$. Siden vi vet at $p(x)$ er irredusibelt, er $irr(\alpha, \mathbb{Q}) = p(x)$, og $grad(\alpha, \mathbb{Q}) = n$.

4.10.3 Enkel kroppsutvidelse

Definisjon 4.18. *La $F \leq \mathbb{C}$ være en kropp, og $\alpha \in \mathbb{C}$. Den minste kroppen i $\mathbb{C}$ som inneholder F og α noteres $F(\alpha)$, og kalles en* enkel kroppsutvidelse *av F.*

Vi sier også at $F(\alpha)$ oppnås ved å *adjungere* α til F, eller at $F(\alpha)$ er *generert* av α over F.
På samme måte har vi at $F(\alpha)(\beta)$ er den minste kroppen som inneholder F og både α og β. Slike utvidelse danner et 'tårn' på denne formen:

$$F \leq F(\alpha) \leq F(\alpha)(\beta), \text{ og } F \leq F(\beta) \leq F(\alpha)(\beta).$$

Selvsagt er $F(\alpha)(\beta) = F(\beta)(\alpha)$, så vi kan skrive entydig $F(\alpha)(\beta)$ eller $F(\beta)(\alpha)$.

Eksempel : $\mathbb{Q}(\sqrt{2})$ er en enkel kroppsutvidelse av $\mathbb{Q}$.

Eksempel : $\mathbb{C}$ er en enkel kroppsutvidelse av $\mathbb{R}$, *generert av i*. Vi skriver: $\mathbb{C} = \mathbb{R}(i)$.

Det meste av kroppsteorien bygger på kroppsutvidelser og hvordan man finner de forskjellige røttene i polynomet ved å utvide kropper, så dette er et

punkt som er veldig viktig for videre lesing av denne oppgaven.

Kroppen $F(\alpha)$ er altså per definisjon den minste kroppen som inneholder F og α. Hvordan ser elementene, tallene, i $F(\alpha)$ ut? Siden en kropp er lukket under $+$, -, $\cdot$ og $/$, er det klart at $F(\alpha)$ må inneholde alle tall på formen $f(\alpha)/g(\alpha)$ der $f(x), g(x) \in F[x]$, og $g(\alpha) \neq 0$. Men mengden av slike tall utgjør en kropp, så vi har at

$$F(\alpha) = \{f(\alpha)/g(\alpha) | f(x), g(x) \in F[x], g(\alpha) \neq 0.\}$$

Et svært viktig resultat er nå at dersom α er *algebraisk* over F, kan $F(\alpha)$ beskrives mye enklere, nemlig hvert tall i $F(\alpha)$ er et polynom i α, av grad høyst graden til α:

Teorem 4.19. *La F være en kropp og α algebraisk over F. La minimalpolynomet til α over F ha grad $n \geq 1$. Da kan alle element i kroppen $F(\alpha)$ skrives på en entydig måte som $f(\alpha)$, der $f(x) \in F[x]$ er et polynom av grad $\leq n$ - 1, dvs på formen $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ der $a_0, \ldots, a_{n-1} \in F$.*

Bevis : Kroppen $F(\alpha)$ bestå per definisjon av alle uttrykk på formen $\dfrac{f(\alpha)}{g(\alpha)}$, der $f(x), g(x) \in F[x]$, og $g(\alpha) \neq 0$.
Vi skal vise at vi kan skrive $\dfrac{1}{g(\alpha)} = h(\alpha)$, for et polynom $h(x) \in F[x]$, og at $f(\alpha)h(\alpha) = t(\alpha)$ der $t(x)$ er et entydig bestemt polynom av grad $< n$.

Først, siden $g(\alpha) \neq 0$, vil minimalpolynomet $p(x)$ ikke gå opp i $g(x)$. Derfor er $p(x)$ og $g(x)$ relativt primiske, siden $p(x)$ er irredusibelt. Da vet vi det finnes polynomer $h(x), k(x)$ over F slik at $h(x)g(x) + k(x)p(x) = 1$.
Siden $p(\alpha) = 0$, får vi $h(\alpha)g(\alpha) = 1$, dvs $\dfrac{1}{g(\alpha)} = h(\alpha)$, så $\dfrac{f(\alpha)}{g(\alpha)} = f(\alpha)h(\alpha)$.

La $r(x)$ være resten ved divisjon av $f(x)g(x)$ med minimalpolynomet $p(x)$. Da er graden til $p(x) \leq n - 1$ og $\dfrac{f(\alpha)}{g(\alpha)} = f(\alpha)h(\alpha) = r(\alpha)$.
For å vise at $r(x)$ er *entydig bestemt*, anta $r(\alpha) = m(\alpha)$, der også $grad(m(x)) \leq n - 1$. Da er $r(x) - m(x)$ av grad $\leq n - 1$, og $r(\alpha) - m(\alpha) = 0$. Per definisjon av minimalpolynomet $p(x)$ må vi da ha $r(x) - m(x) = 0$, så $m(x) = r(x)$.

Eksempel : La $\alpha = \sqrt[3]{2}$. Hvordan ser elementene i $\mathbb{Q}(\alpha)$ ut? Vi vet at $irr(\alpha, \mathbb{Q} = x^3 - 2$. så α har grad 3 over $\mathbb{Q}$. I følge teorem 4.19 vil da hvert element i $\mathbb{Q}(\alpha)$ skrives entydig på form

$$a_0 + a_1\alpha + a_2\alpha^2$$

der $a_0, a_1, a_2 \in \mathbb{Q}$.

Eksempel : La $\alpha = \sqrt{2}$ og $\beta = \sqrt{3}$. Vi har utvidelsene $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\alpha)(\beta)$. α har grad 2 over $\mathbb{Q}$. Det er lett å sjekke at β har grad 2 over $\mathbb{Q}(\alpha)$ siden $x^2 - 3$ ikke har noen røtter i $\mathbb{Q}(\alpha)$. Derfor kan hvert element i $\mathbb{Q}(\alpha)(\beta$ skrives entydig som $a_o + a_1\beta$ der $a_o, a_1 \in \mathbb{Q}(\alpha)$, dvs som $a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3}$, der $a, b, c, d \in \mathbb{Q}$.

4.10.4 Vektorrom

Vektorrom kjenner leseren fra lineær algebra, hvor vi typisk har $\mathbb{R}^n$ som et vektorrom av dimensjon n over de reelle tall. De tenker vi på vektorene i $\mathbb{R}^n$ som pilereller n-tupler av reelle tall.
En helt annen svært nyttig bruk av vektorrom har vi ved en kroppsutvidelse $F \leq E$; Da kan vi nemlig se på E som et vektorrom over F. Jeg minner først om den abstrakte definisjonen av et vektorrom:

Definisjon 4.20. *La F være en kropp. Et vektorrom over F består av en abelsk gruppe, V, sammen med en skalarmultiplikasjon av elementene i F med elementene i V, slik at følgende betingelser er oppfylt for alle $a, b \in F$:*

- $a\alpha \in V$,
- $a(b\alpha) = (ab)\alpha$,
- $(a + b)\alpha = (a\alpha) + (b\alpha)$,
- $a(\alpha + \beta) = (a\alpha) + (a\beta)$,
- $1\alpha = \alpha$.

Elementene i V er vektorer, mens elementene i F er skalarer. Av disse aksiomene følger det at dersom V er et vektorrom over F, så er $0\alpha = 0, a0 = 0$ og $(-a)\alpha = a(-\alpha) = -(a\alpha)$ for alle $a \in F$ og $\alpha \in V$.

Gitt en kroppsutvidelse $F \leq E$ kan vi altså se på E som et vektorrom over F. Hvis $a \in F$ og $\alpha \in E$ er skalarmultiplikasjon $a\alpha$ der samme som den vanlige multiplikasjonen i E.

Korollar 4.21. *Graden $[F(\alpha) : F]$ til en enkel algebraisk utvidelse $F \leq F(\alpha)$, er lik graden til minimalpolynomet til α over $F, grad(\alpha, F)$:*

$$[F(\alpha) : F] = grad(\alpha, F)$$

Graden til kroppsutvidelse over en kropp er lik graden til minimalpolynomet over den samme kroppen. Kan henvise tilbake til det siste eksempelet i del 4.10.2, hvor graden til minimalpolynomet var 2, og et eksempel vi kommer til på neste side, hvor graden til $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q} = 2$.
$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = grad(\sqrt{2}, \mathbb{Q}) = 2$.

4.10.5 Endelig kroppsutvidelse

Definisjon 4.22. *Dersom en kroppsutvidelse E av en kropp F er av endelig dimensjon n som et vektorrom over F, kalles E av endelig utvidelse av grad n over F. Vi lar $[E : F]$ være graden n av E over F.*

Vi illustrerer med noen enkle eksempler:

Eksempel : Graden $[E : F] = 1$, hvis og bare hvis $E = F$.

Eksempel : $[\mathbb{C} : \mathbb{R}] = 2$. Siden $\mathbb{C} = \mathbb{R}(i)$ og $irr(i, \mathbb{R}) = x^2 + 1$.

Eksempel : $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, siden $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$..

Teorem 4.23. *En* endelig *kroppsutvidelse $F \leq E$ er algebraisk, det vil si, alle $\alpha \in E$ er algebraiske over F.*

Bevis : La $[E : F] = n$ og se på de $n + 1$ elementene $1, \alpha, \alpha^2, \ldots, \alpha^n \in E$. Siden E har dimensjon n over F, må disse være lineært avhengige over F, dvs det finnes $a_0, \ldots, a_n \in F$, ikke alle null, slik at $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$ Men dette betyr nettopp at α er algebraisk over F.

Dersom ikke alle elementer i E er algebraiske over F, kalles det en transcendent utvidelse av F.

Eksempel : Hvis vi ser på kroppsutvidelsen: $\mathbb{Q} \leq \mathbb{R}$, vet vi at dette er en transcendental utvidelse, mens $\mathbb{R} \leq \mathbb{C}$, og $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ er algebraiske utvidelser.

Teorem 4.24. *Dersom E er en endelig kroppsutvidelse av F, og K er en endelig kroppsutvidelse av E, så er K en endelig kroppsutvidelse av F, og:*

$$[K : F] = [K : E][E : F].$$

Eksempel : Hva blir $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$? Vi har f.eks $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Vi vet at $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Siden $x^2 - 3$ er irredusibelt over $\mathbb{Q}(\sqrt{2})$, er $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, så $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$ fra teorem 4.23.

Eksempel : Hva blir $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$?
Siden $p(x) = x^3 - 2$ er irredusibelt over $\mathbb{Q}$, er $p(x)$ minimalpolynomet til $\sqrt[3]{2}$ over $\mathbb{Q}$. Så $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = grad(p(x)) = 3$. Det samme gjelder også om $\sqrt[3]{2}$ står for en kompleks løsning av $x^3 - 2$.

Eksempel :Hva er $[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}]$?
Vi har f.eks $\mathbb{Q} \leq \mathbb{Q}(i) \leq \mathbb{Q}(i, \sqrt{3})$. Minimalpolynomet for i over $\mathbb{Q}$ er $x^2 + 1$, for $\sqrt{3}$ over $\mathbb{Q}(i)$ er $x^2 - 3$, siden $\sqrt{3} \notin \mathbb{Q}(i)$.
Derfor får vi fra teorem 4.24 at

$$[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

4.11 Embedding fortsetter

Setning : Dersom $p(x)$ er et irredusibelt polynom i $F[x]$, og σ er en embedding, så er σp irredusibel over σF.

Bevis : Dersom vi kan faktorisere

$$\sigma p = gh$$

over σF, da kan vi skrive

$$p = \sigma^{-1}\sigma p = (\sigma^{-1}g)(\sigma^{-1}h),$$

og p kan altså faktoriseres over F. Men dette strider mot utgangspunktet om at p er irredusibelt, og setningen holder.

Teorem 4.25. *La $f(x) \in F[x]$ og la α være algebraisk over F.- La $\sigma : F(\alpha) \to L$ være en embedding til en kropp L. Da er*

$$(\sigma f)(\sigma\alpha) = \sigma(f(\alpha)).$$

Dette følger av definisjonen av en embedding, og dersom $f(x)$ er som vist ovenfor, har vi

$$f(\alpha) = a_n\alpha^n + \ldots + a_0,$$

og

$$\sigma(f(\alpha)) = \sigma(a_n)\sigma(\alpha)^n + \ldots + \sigma(a_0).$$

Av dette følger det, at dersom α er en av røttene til f, er $\sigma(\alpha)$ en av røttene til σf.

Eksempel : La $\sigma : \mathbb{Q}(\sqrt{2}) \mapsto \mathbb{C}$ være en embedding. Hva må $\sigma(\sqrt{2})$ være?
Vi vet (se eksempel etter definisjon 4.11) at hvis $a \in \mathbb{Q}$, så må $\sigma(a) = a$.
Derfor må $\sigma(\sqrt{2})$ være en rot i $x^2 - 2$, dvs $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Hvis $\sigma(\sqrt{2}) = \sqrt{2}$, blir σ identitetsavbildningen.
At $\sigma(\sqrt{2}) = -\sqrt{2}$ faktisk gir en embedding, skal vi se i teorem 4.27 nedenfor.

Vi kommer nå til et teorem som er grunnleggende for Galoisteori; nemlig å beskrive nøyaktig hvilke embeddinger som *utvider* en gitt embedding.

Definisjon 4.26. *La $\sigma : F \to L$ være en embedding. La E være en utvidelse av F. En embedding $\tau : E \to L$ sies å være en utvidelse av σ dersom $\tau(x) = \sigma(x)$ for alle $x \in F$. Vi sier også at restriksjonen av τ til F er σ.*

Teorem 4.27. *La $\sigma : F \to L$ være en embedding. La $p(x)$ være et irredusiblet polynom i $F[x]$. La α være en rot av p, og la β være en rot av σp i L. Da eksisterer det en embedding $\tau : F(\alpha) \to L$ som er en utvidelse av σ, og slik at $\tau\alpha = \beta$. Omvendt gjelder også at hver utvidelse τ av σ til $F(\alpha)$ er slik at $\tau\alpha$ er en rot til σp.*

Kommentar : Det enkleste tilfellet får vi dersom $\sigma : F \leq \mathbb{C}$ bare er identiteten. Da sier teoremet at for hver rot β av minimalpolynomet til α over F, finnes nøyaktig en embedding $\tau : F(\alpha) \to \mathbb{C}$ som er identiteten på F (og $\tau(\alpha) = \beta$), og dette er alle embeddinger av $F(\alpha)$ som er identiteten på F.

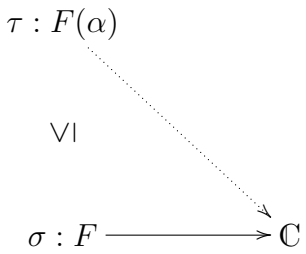
Bevis : Først, $\tau : F(\alpha) \to L$ er entydig bestemt av $\tau(\alpha)$, siden τ skal være lik den gitte σ på F. Vi vet fra teorem 4.19 at et element i $F(\alpha)$ kan skrives som et polynom $f(\alpha), f(x) \in F[x]$, og vi definerer $\tau(f(\alpha)$ som $(\sigma f)(\beta)$.

Men siden elementet $f(\alpha)$ også kan skrives $g(\alpha)$ for et annet polynom $g(x) \in F[x]$, må vi sjekke at definisjonen av τ blir uavhengig av valget av f.
Men hvis $f(\alpha) = g(\alpha)$, er $(f-g)(\alpha) = 0$. Da vet vi at minimalpolynomet $p(x)$ til α går opp i $f - g$, dvs $f - g = p(x)h(x)$. Da blir så $\sigma f - \sigma g = (\sigma p)(\sigma h)$, og dermed

$$(\sigma f)(\beta) - (\sigma g)(\beta) = (\sigma p)(\beta)(\sigma h)(\beta) = 0 \cdot (\sigma h)(\beta) = 0.$$

Dette beviser at τ blir veldefinert.
Siste del av teoremet følger av teorem 4.27.

Under ser vi en illustrasjon på teoremet.



Figur 4.3. Embeddingutvidelse. Her er $p(x) = irr(\alpha, F)$, og $(\sigma p)(\beta) = 0$.

Dersom en har en embedding $\sigma : F \to L$ eksisterer det en utvidelse av σ, kalt τ slik at $\tau : F(\alpha) \to L$ og $\tau\alpha = \beta$.

Korollar 4.28. *La p være et irredusibelt polynom over en kropp F. La α være en rot av p. La*

$$\sigma : F \to \mathbb{C}$$

være en embedding av F inn i de komplekse tall. Da er antallet ulike embeddinger av $F(\alpha)$ til $\mathbb{C}$ som utvider σ, lik graden til p.

Dersom graden til $p(x)$ er n, vet vi fra teorem 4.15 og 4.17 at $p(x)$ har n forskjellige røtter i de komplekse tall. Gitt α, kan vi utvide σ til $F(\alpha)$ på nøyaktig n ulike måter, en for hver av de n ulike røttene til $p(x)$. Dette betyr at dersom det er n røtter, er det n mulige embeddinger av $F(\alpha)$ til $\mathbb{C}$.

Korollar 4.29. *La E være en endelig utvidelse av F. La n være graden til E over F. La $\sigma : F \to \mathbb{C}$ være en embedding av F inn i de komplekse tall. Da er antallet utvidelser av σ til en embedding av E til $\mathbb{C}$ lik n.*

Det dette korollaret sier, er at dersom en har en kropp F, og en endelig utvidelse E, finnes det like mange embeddinger, av E over F som graden til $[E : F]$. Dette er et viktig poeng når vi kommer til Galoisgrupper.

Bevis : Vi kan skrive E på formen $E = F(\alpha_1, \ldots, \alpha_r)$. Se på tårnet

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \ldots \subset F(\alpha_1, \ldots, \alpha_r).$$

La $E_{r-1} = F(\alpha_1, \ldots, \alpha_{r-1})$. La $\sigma_1, \ldots, \sigma_m$ være utvidelsene av σ til E_{r-1}, der $[E_{r-1} : F] = m$. La d være graden til α_r over E_{r-1}. For hver $i = 1, \ldots, m$, kan vi finne nøyaktig d utvidelser av σ_i til E, la oss si $\sigma_{i1}, \ldots, \sigma_{id}$. Da er det klart at embeddingene $\{\sigma_{ij}\}(i = 1, \ldots, m$ og $j = 1, \ldots, d)$ er nøyaktig de ulike utvidelser σ til E (Se korollar 4.21). Dette beviser korollaret, som sier at graden til $[E : F]$, er lik antall utvidelser av embeddingen σ.

Bemerkning : La α være algebraisk over F. La $p(x)$ være det irredusible polynomet av α over F. La $\alpha_1, \ldots, \alpha_n$ være røttene til p. Da kaller vi disse røttene for *konjugerte av* α over F. For hver α_i, er det nøyaktig en embedding σ_i av $F(\alpha)$ som avbilder α på α_i, og som er identiteten på F. Denne embeddingen er entydig bestemt av $\tau(\alpha) = \alpha_i$. Merk også at hver slik embedding τ gir en *isomorfisme* mellom $F(\alpha)$ og hver $F(\alpha_i)$.

Eksempel : La oss se på polynomet $x^3 - 2$. Vi lar α være den reelle kubikkroten av 2; $\alpha = \sqrt[3]{2}$. La $1, w, w^2$ være de tre 3.-enhetsrøttene.
Det gitte polynomet er irredusibelt over $\mathbb{Q}$ og røttene er $\alpha, \omega\alpha, \omega^2\alpha$. Derfor eksisterer 3 embeddinger av $\mathbb{Q}(\alpha)$ til $\mathbb{C}$, dette er de tre embeddingene $\sigma_1, \sigma_2, \sigma_3$, slik at

$$\sigma_1\alpha = \alpha, \sigma_2\alpha = w\alpha, \sigma_3\alpha = w^2\alpha.$$

Eksempel : La $\alpha = 1 + \sqrt{2}$. Hvilke embeddinger av $\mathbb{Q}(\alpha) \to \mathbb{C}$ finnes da? (En slik embedding vet vi alltid er identiteten på $\mathbb{Q}$.) Minimalpolynomet $p(x)$ til α finner vi slik: $\alpha = 1 + \sqrt{2} \Rightarrow (\alpha - 1)^2 = 2 \Rightarrow \alpha^2 - 2\alpha - 1 = 0$, så $p(x) = x^2 - 2x - 1$. Den konjugerte til α blir da $\beta = 1 - \sqrt{2}$. Så det finnes nøyaktig 2 embeddinger av $\mathbb{Q}(\alpha)$, nemlig $\alpha \mapsto \alpha$ (dvs identiteten) og $\alpha \mapsto \beta$.

Teorem 4.30. *(Teoremet om primitivt element) La E være en endelig utvidelse av F. Da eksisterer det et element γ i E, slik at $E = F(\gamma)$.*

Eksempel : Bevis at dersom $\alpha^2 = 2$ og $\beta = \sqrt[3]{2}$, da er $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$, hvor $\gamma = \alpha + \beta$.

Finner minimalpolynomet til γ :

$$\begin{aligned} x &= \sqrt{2} + \sqrt[3]{2} \\ (x - \sqrt{2})^3 &= 2 \\ x^3 + 6x - 3x^2\sqrt{2} - 2\sqrt{2} &= 2 \\ x^3 + 6x - 2 &= 3x^2\sqrt{2} - 2\sqrt{2} \\ (x^3 + 6x - 2)^2 &= \left(3x^2\sqrt{2} - 2\sqrt{2}\right)^2 \\ x^6 + 12x^4 - 4x^3 + 36x^2 - 24x + 4 &= 18x^4 - 24x^2 + 8 \\ p(x) = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4 &= 0 \end{aligned}$$

Ifølge Maple, er dette $p(x)$ irredusibelt, og det er da minimalpolynomet til γ, som har grad 6 over $\mathbb{Q}$.
Siden $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$ og $\gamma \in \mathbb{Q}(\alpha, \beta)$, må $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$.

4.12 Oppsummering

• En *kropp* er en kommutativ ring, R, der $(R - \{0\}, \cdot)$ er en gruppe.

• La R og S være ringer. En *ringhomomorfisme* er en avbildning $\phi : R \to S$ slik at:

$$\phi(a + b) = \phi(a) + \phi(b);$$
$$\phi(a \cdot b) = \phi(a)\phi(b);$$
$$\phi(1) = 1.$$

Dersom ϕ er bijektiv, kalles den en *isomorfisme*.

• En *automorfisme* av en kropp F, er en isomorfisme σ: F $\to$ F av F på seg selv.

• En kropp E er en *utvidelse* av en kropp F, dersom $F \leq E$ og operasjonene i E og F er de samme.

• En *fikskropp* er mengden av alle elementer x i en kropp F, slik at $\sigma x = x$ for alle automorfismer σ i en gruppe av automorfismer G.

• Et polynom $f(x)$ er *irredusibelt* over en kropp, F dersom det ikke kan bli uttrykt som et produkt av to polynomer $g(x)h(x)$ i $F[x]$ hvor begge har grad lavere enn $f(x)$.

• Et polynom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ med heltallskoeffisienter er irredusibelt over $\mathbb{Q}$ dersom det finnes et primtall p slik at p ikke går opp i a_n, p^2 ikke går opp i a_0, men p går opp i alle $a_{n-1}, \ldots, a_1$.

• Et tall $\alpha \in \mathbb{C}$ kalles *algebraisk* over en kropp F dersom det finnes et *polynom* $f(x) \neq 0 \in F[x]$ slik at $f(\alpha) = 0$.

• *Minimalpolynomet* til et tall α over en kropp F er det moniske polynomet $p(x)$ av lavest grad ≥ 1 slik at $p(\alpha) = 0$. Minimalpolynomet er irredusibelt over F, og går opp i alle polynomer $\in F[x]$ med α som rot. Graden til minimalpolynomet kalles *graden* til α over $F, grad(\alpha, F)$.

• Den minste kroppen som inneholder F og $\alpha \in \mathbb{C}$, kalles en *enkel kroppsutvidelse* av F, og noteres $F(\alpha)$.

• En kroppsutvidelse $F \leq E$ kalles *endelig* dersom E har endelig dimensjon som et vektorrom over F.Dimensjonen til E over F kalles *graden* og noteres $[E : F]$.

• Graden $[F(\alpha) : F]$ til en enkel algebraisk utvidelse $F \leq F(\alpha)$, er lik graden til minimalpolynomet til α over $F, grad(\alpha, F)$:

$$[F(\alpha) : F] = grad(\alpha, F)$$

• Dersom E er en endelig kroppsutvidelse av F, og K er en endelig kroppsutvidelse av E, så er K en endelig kroppsutvidelse av F, og:

$$[K : F] = [K : E][E : F]$$

• Antallet embeddinger $\tau : F(\alpha) \to \mathbb{C}$ som er identiteten på F, er lik graden til minimalpolynomet $p(x)$ til α over F. Siden $p(x)$ er irredusibelt, har $p(x)$ *ulike* røtter $\alpha = \alpha_1, \ldots, \alpha_n$, og en embedding τ er definert ved $\tau(\alpha) = \alpha_i$.

• La $F \leq E$ være en kroppsutvidelse av grad $n : [E : F] = n$, og la $\sigma : F \to \mathbb{C}$ vaere en embedding. Da finnes nøyaktig n utvidelser av σ til en embedding $\tau : E \to \mathbb{C}$.

Kilder for dette kapittelet, er Fraleigh [3], kapittel 18 og Lang [5], kapittel 4.

5 Biografier

5.1 Niels Henrik Abel

Figur 1: Niels Henrik Abel (1802 - 1829)

Niels Henrik Abel ble født 5. august på Finnøy i Rogaland.
Han vokste opp i en familie på 8, hvor han hadde 4 brødre og en søster, hans mor, Anne Marie Simonsen, og faren, Søren Georg Abel, som var sogneprest.
Niels Henrik ble i 1815 sendt til Christiania, for å begynne på katedralskolen.
I 1817 ble matematikklæreren, Hans Peter Bader, byttet ut på grunn av brutal oppførsel, og Bernt Michael Holmboe fikk stillingen.
Holmboe var en veldig flink matematikklærer, og på grunn av hans noe spesielle læringsmetoder på den tiden, bl. a. med å gi elever individuelle oppgaver, gav det gnisten i Abel.
Holmboe merket etter kort tid at dette var en gutt med enestående matematiske evner.
Abel fikk etterhvert privatundervisning av Holmboe, og det blir sagt i ettertid at dersom Abel ikke hadde hatt Holmboe til matematikklærer, er det ikke sikkert at han hadde blitt den Niels Henrik Abel vi kjenner i dag.

Det var dårlig med realfagsstudier i Norge på den tiden, og etter at Holmboe hadde lært Abel alt han kunne, måtte Abel studere på egen hånd.
Han studerte verkene til Newton, Euler, Lagrange og Gauss.
Våren 1823, publiserte Abel sin første artikkel i Magazin for Naturvidenskabernem som var det første vitenskapelige tidsskiftet i Norge. Da var det noen av professorene ved universitetet som forstod at Abel måtte utenlands for å lære mer matematikk.
Sommeren 1823 fikk han mulighet til å reise til København. Det var under dette oppholdet han begynte arbeidet sitt med elliptiske funksjoner. Det var også her han ble kjent med Christine Kemp, som han ble forlovet med året etter.
Abel ønsket sterkt å komme seg utenlands for å lære mer, og etter et brev til kong Karl lll Johan, fikk han til slutt sitt etterlengtede stipend til utenlandsreisen.
Planen var å reise til Göttinger for å møte Gauss, men han endret planene, og reiste heller til Berlin. Han bodde i Berlin i 4 måneder før han reiste videre mot Paris.
På den tiden var Paris den store matematikkhovedstaden, hvor store navn som Cauchy, Poisson, Legendre og Fourier holdt til.
Sommeren 1826 begynte han arbeidet med en avhandling, hvor et addisjonsteorem for elliptiske integral stod i fokus. Han leverte inn avhandlingen til vitenskapsakademiet i oktober 1826, og ventet på svar.
Abel fikk ikke noe svar på avhandlingen, så rundt årskiftet 1826/1827, reiste han tilbake til Berlin, og han hadde i tillegg begynt å bli syk.
I Berlin ble han tilbudt en stilling som redaktør av Crelles Journal, men takket nei på grunn av hjemlengsel.
Abel kom tilbake til Norge i 1827, mens August Leopold Crelle jobbet med å gi ham en sikker stilling i Berlin.
I Paris hadde Abel fått tuberkolose, men fortsatte arbeidet sitt. Han jobbet med en stor avhandling om elliptiske funksjoner høsten 1827, og jobbet videre med likningsteori når denne var fullført.
Gjennom sine publikasjoner i Crelles Journal, begynte Abel å oppnå berømmelse i utlandet, men hjemme i Norge levde han under fattige kår.
I september 1828 sendte Legendre, Poisson, Lacroix og Baron de Maurice et brev til kong Karl Johan om situasjonen til Abel. Målet med brevet var å få opprettet en stilling for Abel i Stockholm. Samtidig arbeidet Crelle stadig for å få opprettet et professorstilling for Abel i Berlin.
Abel ble stadig sykere og sykere, og etter julefeiringen i 1828, var han så dårlig at han ikke klarte å returnere til Christiania.
Da Abel forstod at han ikke hadde lenge igjen, skrev han et sammendrag av beviset for Abels addisjonsteorem, som ble sendt til Crelle.

6. April 1829, døde Abel, og kun et par dager senere skrev Crelle et brev til Abel hvor han hadde sikret Abel en fast stilling og en lysende fremtid i Berlin.

Niels Henrik Abel har bidratt med mye innenfor matematikken, men det han nok er mest kjent for, er arbeidet med elliptiske funksjoner og ikke minst, beviset om at en generell likning av grad høyere enn 4, ikke kan løses ved rottegn og de fire regneartene.

5.2 Èvariste Galois

Figur 2: Èvariste Glaois (1811 - 1832)

Èvariste Galois ble født i Bourg-la-Reine, 25. oktober 1811.
Han var sønn av Nicolas-Gabriel og Adèlaïde-Marie Galois.
Han ble skikkelig interessert i matematikk som 14-åring.
Som 15-åring fant han en kopi av Adrien Marie Legendres Elements le Geometrie, som han forstod etter kun å ha lest den en gang. Han leste også de originale avhandlingene til Joseph Louis Lagrange, som sannsynligvis motiverte han til sitt videre arbeid med likninger.

Galois prøvde seg på eksamen for å komme inn på Ècole Polytechnique, det mest prestisjefulle matematikkinstituttet på den tiden, men strøk begge gangene. Første gang på grunn av manglende forklaringer til det han gjorde, andre gang på grunn av at han hoppet over mange logiske steg som ekaminatoren mente måtte være med. Galois ble utrolig sur, og det sies at han kastet kluten som ble brukt til å vaske av tavla, i hodet på eksaminatoren. Farens selvmord noen dager i forveien, kan også ha vært med på å frembringe sinnet hos Galois.
Da han etter to forsøk ikke kom inn på Ècole Polytechnique, tok han en ny eksamen for å komme inn på Ècole Normale.

På denne eksamenen stod han, og eksaminatoren kommenterte: *Denne eleven har av og til problemer med å få fram idèene sine, men er intelligent og viser en stor iver og vilje.*
Mellom de to eksamenene for å komme inn på École Polytechnique, ble hans første artikkel publisert, og han gjorde også grunnleggende oppdagelser i teorien om likninger. Han sendte inn to artikler om dette emnet, men de ble aldri publisert. Grunnen til dette er uklar.
Han fortsatte å sende inn artikler om likninger, men disse ble ikke publisert. Han fikk imedlertidig publisert noen andre artikler, i 1830, som ga grunnlag til Galois-teorien.
Galois var veldig politisk aktiv i denne tiden, og ble arrestert flere ganger. Hans lengste fengselsopphold varte i 6 måneder, for å ha hatt på seg uniform ulovlig. Under dette oppholdet, fortsatte han med å komme med matematiske idèer.
Etter kun en måned i det fri, deltok han i en duell som endte i døden. Årsaken til denne duellen er ikke helt klar, men man tror det var pga av at han var forelsket i en jente som tilhørte en annen.
Natten før duellen, skrev han brev til mange av vennene sine, som skulle bli et matematisk testament.
Dagen etter duellen, døde Galois av skadene, og hans siste ord var til broren, Alfred: *Ikke gråt Alfred. Jeg trenger alt mitt mot for å dø som 20-åring.*

Selv om Galois døde veldig ung, og hans samlede matematiske arbeid kun var på rundt 60 sider, bidro han med mye til matematikken.
Han var den første som brukte ordet 'gruppe' i matematikken, så han er en av grunnleggerne til gruppeteorien.
Han utviklet blant annet normale undergrupper og endelig kropper, men han største bidrag til matematikken er Galoisteorien, hvor han oppdaget at løsningene til et polynom er relaterte til en gruppe av permutasjoner, assosiert med røttene til polynomet, det som er kalt en Galoisgruppe av et polynom. Han fant også ut at en likning kan løses ved rottegn, dersom en kan finne en serie av undergrupper til Galoisgruppen.

Selv om Galois hadde mange idèer og teorier, fikk han ikke skrevet dem godt nok ned før sin død. Memoarene han skrev ned dagen før duellen, var kortfattet og vanskelige å lese. Heldigvis brukte Joseph Liouville (1809 - 1882) mye tid på å *dekode* Galois sine memorarer, slik at de ikke gikk til spille.

Idèen til Galois var å knytte til hver likning en gruppe av permutasjoner av røttene. Denne gruppa inneholder alle permutasjoner som bevarer alle relasjoner, røttene imellom.

Ved å bruke disse relasjonene så man vanskeligheter og problemer med likninger mye lettere, og informasjon om en likning er løselig med rotuttrykk kan bli hentet ut ved hjelp av den tilordnede gruppa.

6 Galoisteori

6.1 Rotkropp

Definisjon 6.1. *En endelig kroppsutvidelse, E, av F, kalles* rotkroppen *til et polynom, $f(x) \in F[x]$, dersom $E = F(\alpha_1 \ldots, \alpha_n)$, hvor $\alpha_1 \ldots, \alpha_n$ er alle røttene til polynomet.*

Dette vil si at rotkroppen til et polynom, $f(x) \in F[x]$. er den minste kroppsutvidelsen av F som inneholder alle røttene til polynomet.

Eksempel : Rotkroppen til x^2-2 over $\mathbb{Q}$, er per definisjon $\mathbb{Q}(\sqrt{2}, -\sqrt{2})$. Men siden $-\sqrt{2}$ er inneholdt i $\mathbb{Q}(\sqrt{2})$ (husk at $\mathbb{Q}(\sqrt{2}) = a + b\sqrt{2}$ hvor $a, b \in \mathbb{Z}$), blir rotkroppen til dette polynomet $\mathbb{Q}(\sqrt{2})$.

Eksempel : Rotkroppen til $x^2 + 1$ over $\mathbb{R}$, er $\mathbb{R}(i) = \mathbb{C}$.

Eksempel : La oss se på polynomet, $x^4 - 5x^2 + 6$ over $\mathbb{Q}$
For å løse likningen, $x^4 - 5x^2 + 6 = 0$ setter vi $x^2 = w$, og får likningen: $w^2 - 5w + 6 = 0$.
Ved å bruke andregradsformelen, finner vi ut at $w_1 = 2$ og $w_2 = 3$. Dette fører til at $x = \pm\sqrt{2}$ og $\pm\sqrt{3}$.
Rotkroppen til $x^4 - 5x + 6$ over $\mathbb{Q}$ blir da: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Eksempel : La oss se på polynomet $x^n - 1$ over $\mathbb{Q}$.
Vi løser likningen: $x^n - 1 = 0 \Rightarrow x^n = 1 \Rightarrow x = \sqrt[n]{1}$.
Likningen har n løsninger, nemlig $\omega = \left(e^{i\frac{2\pi}{n}}\right)^k, k = 0, 1, \ldots, n-1$, hvor $\omega^n = 1$. Rotkroppen til $x^n - 1$ over $\mathbb{Q}$ blir da: $\mathbb{Q}(\omega)$.
Man kan bevise at $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$ der ϕ er Eulers ϕ-funksjon ($\phi(n) =$ antall $m, 1 \leq m \leq n-1$, slik at $gcd(m, n) = 1$).

Definisjon 6.2. *En endelig kroppsutvidelse E av F, kalles en Galoisutvidelse, dersom hver embedding av E over F er en automorfisme av E.*

Teorem 6.3. *En endelig utvidelse av F er en* Galoisutvidelse *hvis og bare hvis den er rotkroppen til et polynom over F.*

Bevis : La E være en Galoisutvidelse av F. Skriv $E = F(\alpha)$. La $p(x)$ være minimalpolynomet over F. For hver rot α_i av p, eksisterer det en embedding

σ_i av E over F slik at $\sigma_i\alpha = \alpha_i$. Dette vet vi fra teorem 4.27. Siden hver embedding er en automorfisme av E, følger det at α_i er inneholdt i E. slik at

$$E = F(\alpha) = F(\alpha_1, \ldots, \alpha_n),$$

og E er rotkroppen til p. (Husk at dersom man har en Galoisutvidelse, er hver embedding av E over F en automorfisme av E).
Omvendt, la oss si at E er rotkroppen til et polynom $f(x)$ over F, med røttene $\alpha_1, \ldots, \alpha_n$. Dersom σ er en embedding av E over F, vet vi at σx_2 må være en rot av $f(x)$ (teorem 4.27). Da avbilder σ E på seg selv, og det betyr at σ er en automorfisme.

Teorem 6.4. *La E være en Galoisutvidelse av F. Dersom $p(x)$ er et irredusibelt polynom i $F[x]$, som har en rot i E, har p alle sine røtter i E.*

Bevis : La α være en av røttene til p i E, og la β være en annen rot. Da eksisterer det en embedding σ av $F(\alpha)$ på $F(\beta)$ som avbilder α på β, og er lik identiteten til F (teorem 4.27). Utvid denne embeddingen til E, da er hver embedding av E over F en automorfisme, og vi har at $\sigma\alpha \in E$, og da er også $\beta \in E$.

En viktig oppklarende sammenfatning så langt er følgende:

Bemerkning La $F(\alpha_1, \ldots, \alpha_n)$ være rotkroppen til et polynom $f(x) \in F[x]$. Da vet vi fra definisjon 6.2 at hver embedding $\sigma : F(\alpha_1, \ldots, \alpha_n) \to \mathbb{C}$ er en automorfisme av $F(\alpha_1, \ldots, \alpha_n)$.
Dessuten vet vi fra teorem 4.27, at hver slik automorfisme σ må avbilde hver rot α_i på en annen rot α_j, dvs at σ gir opphav til en *permutasjon* av de n røttene til $f(x)$, Men selvsagt vil ikke alle permutasjonene svare til en automorfisme.
Galoisgruppa (se neste definisjon) $G(F(\alpha_1, \ldots, \alpha_n)/F)$ vil altså gi en *undergruppe* av permutasjonsgruppa, S_n.

6.2 Galoisgruppe

Definisjon 6.5. *La E være en utvidelse av en kropp F. Mengden av alle automorfismer av denne utvidelsen danner en gruppe, $Aut(E/F)$.*
Dersom E/F er en Galoisutvidelse, kalles $Aut(E/F)$ Galoisgruppa *av E over F, $G(E/F)$.*

Eksempel : $G(F/F)$ er opplagt en triviell gruppe som kun har ett element, nemlig identitetsautomorfismen.

Bevis : Viser til eksempelet om automorfisme.

Eksempel : $G(\mathbb{C}/\mathbb{R})$ har to elementer, identitetsautomorfismen og den kompleks konjugerte automorfismen.

Bevis : $\mathbb{C} = \mathbb{R}(i)$, dvs $\mathbb{C}$ er rotkroppen til $x^2 + 1 \in \mathbb{R}[x]$.
Da vet vi fra tidligere at $[\mathbb{R}(i) : \mathbb{R}] = 2 = |G|$.

Det kommer mange flere eksempler på Galoisgruppen til et polynom i kapittel 7.

Før fundamentalteoremet til Galois, skal vi se kort på forskjellen mellom den klassiske og den moderne måten å presentere Galoisteorien på.

Klassisk :
La $f(x) \in F[x]$ og $f(x)$ er irredusibel over F. $f(x)$ har de ulike røttene $\alpha_1, \ldots, \alpha_n$.

Definisjon 6.6. *Galoisgruppen til $f(x)/F$, eller symmetriene til $f(x)/F$, er de permutasjonene, σ av $\alpha_1, \ldots, \alpha_n$ slik at $\sigma(\alpha_i) = \alpha_j$, som er slik at for alle polynom $P(x_1, \ldots, x_n)/F$ der $P(\alpha_1, \ldots, \alpha_n) = 0$, så skal også $P(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0$.*

Moderne :

Definisjon 6.7. *La K være rotkroppen til $f(x)$ over $F, F \leq K$. Da kalles $G(K/F)$ symmetrigruppa til $f(x)/F$, eller Galoisgruppa til $f(x)/F$.*

Vi vet nå at dersom vi har en kroppsutvidelse $F \leq K$, danner automorfismene av K over F en gruppe, notert $G(K/F)$. La oss kalle denne gruppa for G.

Dersom vi har en utvidelse av en kroppsutvidelse, $F \leq E \leq K$, danner også automorfismene av K over E en gruppe, notert $G(K/E)$. La oss kalle denne gruppa, H.
I gruppa G, holdes F i ro. I H holdes E i ro, og siden $F \leq E$ holdes F 'enda mer i ro'. Dette fører til at $H < G$.
Hvis vi går andre vei, og har en vilkårlig gruppe H som er undergruppe av $G(K/F) = G, H < G$, finnes det en mellomkropp mellom F og K, som kalles fikskroppen til H. $F \leq F^H \leq K$.

Vi kan nå spørre:
- Vil alle $H < G$ være automorfismegruppa til en eller annen $F \leq E \leq K$?
- Er alle mellomkropper fikskropp til en $H < G$?

6.3 Fundamentalteoremet for Galoisteori

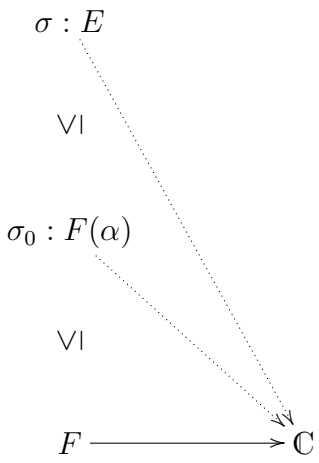
Del I :

Teorem 6.8. *La E være en Galoisutvidelse av F. La G være gruppen av automorfismer av E over F. Da er F fikskroppen til G.*

Bevis : Beviset her er i hovedsak basert på Lang [5], kap 4, §4.
Vi starter med en Galoisutvidelse $F \leq E$, og $G = G(E/F)$ er automorfismegruppa til utvidelsen.
Teoremet beskriver at da er F fikskroppen til G, og det er dette vi skal bevise. Vi starter med og la F' være fikskroppen til G. Siden vi vet fra tidligere at F' kan være større enn F, er det opplagt at $F \subset F'$. Vi skal nå vise at $F' = F$. For å gjøre dette, antar vi at F' er større enn F og utleder en selvmotsigelse.

Dersom F' er større enn F, kan vi velge et element α slik at $\alpha \notin F$, men $\alpha \in F'$. Vi lar $p(t)$ være minimalpolynomet til α over F. Legg merke til at $p(t)$ må minst ha grad 2, så vi lar α_1 være en av røttene til $p(t)$, slik at $\alpha_1 \neq \alpha$. (Polynomet må være av minst grad 2 for at vi skal ha forskjellige røtter). Fra teorem 4.27, vet vi at det eksisterer en embedding av $F(\alpha)$ over F, som sender α på α_1. Vi lar σ_0 være en slik embedding, slik at $\sigma_o(\alpha) \neq \alpha$.

Videre, bruker vi korollar 4.29, og utvider σ_0 til en embedding σ av E over $F(\alpha)$, slik at σ og σ_0 blir like på $F(\alpha)$. Da blir $\sigma(\alpha) = \sigma_0(\alpha) \neq \alpha$.
Videre, siden σ_0 lar F være i ro (fiksert), vil σ gjøre det samme, og dermed er σ en embedding av E over F. Nå bruker vi antagelsen at $F \leq E$ er en Galoisutvidelse, som medfører per definisjon at σ er en automorfisme av $F \leq E$, som vil si at $\sigma \in G$. Siden vi har valgt α i fikskroppen til G, er da $\sigma(\alpha) = \alpha$ per definisjon. Men dette strider mot at vi allerede har vist at $\sigma(\alpha) \neq \alpha$, og dermed er teoremet bevist.



Figur 6.1. F er fikskroppen til $G(E/F)$.

Teorem 6.9. *Gitt en Galoisutvidelse $F \leq K$. La $G = G(K/F)$, og la E være en mellomkropp, slik at $F \leq E \leq K$. Da gjelder:*

1. $[K : F] = |G|$.
2. *Utvidelsen $F \leq K$ er en Galoisutvidelse, og $G(K/E)$ er en undergruppe av G.*
3. *La $\mathbf{K} = \{E \mid E$ er en mellomkropp, $F \leq E \leq K\}$ og la $\mathbf{G}$ være mengden av alle undergrupper av G. Da er avbildningen $\mathbf{K} \to \mathbf{G}$ som sender mellomkroppen E til undergruppa $G(K/E)$, bijektiv.*
4. *For hver mellomkropp E er fikskroppen til $G(K/E)$ lik E, dvs inversen til avbildningen sender en undergruppe $H < G$ til fikskroppen til $H, F \leq E \leq K$.*

Bevis : Bevis til første punkt kan henvises til korollar 4.29, hvor man bruker en Galoisutvidelse istedet for en endelig utvidelse.
Fra forrige teorem vet vi at Fikskroppen til $G(K/E) = E$ dersom K er en Galoisutvidelse av E.
Hver embedding av K over E er en embedding over F, siden E er en kroppsutvidelse av F, og derfor en automorfisme av K. Av dette følger det at K er Galois over E, nettopp av definisjonen til en Galoisutvidelse (Se def. 6.2). Videre, er E fikskroppen til $G(K/E)$, som ble vist i forrige teorem. Dette viser at avbildningen, $E \mapsto G(K/E)$, er injektiv, det vil si at dersom $E \neq E'$,

fører det til at $G(K/E) \neq G(K/E')$.
Dette gjelder også andre veien. Siden E er fikskroppen til $G(K/E)$, sendes E på seg selv. Av dette blir avbildningen bijektiv:

$$E \leftrightarrow H = G(K/E).$$

Til slutt, la H være en undergruppe av G, hvor $G = G(K/F)$, og skriv $K = F(\alpha)$.
La embeddingene $\{\sigma_1, \ldots, \sigma_r\}$ være elementene i H, og la

$$f(t) = (t - \sigma_1\alpha) \ldots (t - \sigma_r\alpha).$$

For enhver σ i H, ser vi at $\{\sigma\sigma_1, \ldots, \sigma\sigma_r\}$ er en permutasjon av $\{\sigma_1, \ldots, \sigma_r\}$. Fra teorem 4.25 om embeddinger vet vi, at dersom α er en rot av f, er $\sigma(\alpha)$ en rot av σf. Fra utrykket

$$\sigma f(t) = (t - \sigma\sigma_1\alpha) \ldots (t - \sigma\sigma_r\alpha) = f(t),$$

ser vi at f har sine koeffisienter i fikskroppen K av H. Videre, $K = E(\alpha)$, og α er en rot av et polynom av grad r over E, $[K : E] \leq r$. Men K har r forskjellige embeddinger over K (de i H fra korollar 4.28). Så, $[K : E] = r$, og $H = G(K/E)$. Dette beviser teoremet.

Del II

Teorem 6.10. *La $F \leq K$ være en Galoisutvidelse med Galoisgruppe $G = G(K/F)$.*

1. *Anta E er en mellomkropp, $F \leq E \leq K$, slik at $F \leq E$ er en Galoisutvidelse.*
   Da er $G(K/E)$ en normal undergruppe av G, og $G(E/F) \cong G/G(K/F)$.

2. *Anta H er en normal undergruppe av G, $H \lhd G$, og la $E = K^H$ være fikskroppen til H, $F \leq E \leq K$.*
   Da er $F \leq E$ en Galoisutvidelse, og $G(E/F) \cong G/H$.

Bemerkning Det dette teoremet sier, er at i Galoiskorrespondansen mellom mellomkropper av $F \leq K$ og undergrupper av $G = G(K/F)$ vil faktisk normale undergrupper $H \lhd G$ svare til mellomkropper $E, F \leq E \leq K$, der utvidelsen $F \leq E$ er en Galoisutvidelse.

Og ikke bare det: Galoisgruppen til $G(E/F)$ vil da være isomorf med kvotientgruppa G/H.

Bevis Beviset er basert på Fraleigh [3], kapittel 56.
Viser først at $F \leq E$ er en Galoisutvidelse hvis og bare hvis $G(K/E)$ er en normal undergruppe av $G(K/F)$.
Husk først at den embedding av E/F alltid kan utvides til en embedding av K/F (Se teorem 4.27).
Det følger da direkte fra definisjonen av Galoisutvidelse at

$*$ $F \leq E$ er Galois $\Leftrightarrow$ for alle $\sigma \in G(K/F)$ og alle $\alpha \in E$ vil $\sigma(\alpha) \in E$.

Nå bruker vi første del av Fundamentalteoremet, som sier at E er fikskroppen til $G(K/E)$.
Dermed kan vi skrive:

$$\begin{aligned} \sigma(\alpha) \in E &\Leftrightarrow \tau(\sigma(\alpha)) = \sigma(\alpha), \forall \tau \in G(K/E) \\ &\Leftrightarrow (\sigma\tau\sigma^{-1}(\alpha) = \alpha \\ &\Leftrightarrow \sigma\tau\sigma^{-1} \in G(K/E). \end{aligned}$$

Vi ser da at høyre side av (*) kan formuleres:
For alle $\sigma \in G(K/F), \tau \in G(K/E)$, er også $\sigma\tau\sigma^{-1} \in G(K/E)$, som jo nettopp betyr at $G(K/E) \lhd G(K/F)$ pr. definisjon av normal undergruppe. (Def. 3.15)

Beviset for siste del, er Lang [5], oppgave 4, s. 113.
Vi ser på gruppehomomorfismen $\phi : G(K/F) \to G(E/F)$ som sender σ til σ restrisert til E.
Da er ϕ surjektiv, siden alle embeddinger av E over F kan utvides til K over F (teorem 4.27).
Dessuten er det lett å sjekke at $ker(\phi) = G(K/E)$.
Derfor har vi ved teorem 3.20, nettopp at $G(K/F)/G(K/E) \cong G(E/F)$.

Selv om teorien for fundamentalteoremet er gjennomgått og godt forklart, kan det fortsatt virke vanskelig å få begrep om hva fundamentalteoremet egentlig sier. Fundamentalteoremet, er beskrevet kompakt, og det kan være lurt å presentere dette fra forskjellige forfatteres tolkninger og presentasjoner. Jörg Bewersdorff beskrivelse av fundamentalteoremet [2], kap 10, er kanskje noe mer pedagogisk lagt opp, men beskriver selvfølgelig det samme.

Teorem 6.11. *La F være en kropp, og $K = F(\alpha_1, \ldots, \alpha_n)$ være rotkroppen til et polynom over F. Da er mengden av elementer i K, som forblir uendret av alle automorfismer i Galoisgruppa til polynomet, nøyaktig kroppen F.*

Dette teoremet er det samme som teorem 6.8, og forteller at F er fikskroppen til $G(K/F)$.

Teorem 6.12. *La F være en kropp, og $K = F(\alpha_1, \ldots, \alpha_n)$ være rotkroppen til et polynom over F. Da er graden til kroppsutvidelsen $F \leq K$ lik $|G(K/F)|$.*

Dette er et viktig poeng som vi har vært innom tidligere, og som brukes i noen av eksemplene, at graden til $F \leq K$ er lik antall elementer i Galoisgruppa til polynomet.

Teorem 6.13. *La F være en kropp, og $K = F(\alpha_1, \ldots, \alpha_n)$ være rotkroppen til et polynom over F. Da er mengden av elementer i K, som forblir uendret av alle automorfismer i en undergruppe, H, av Galoisgruppa til polynomet, nøyaktig kroppen F, bare dersom H er den fulle Galoisgruppa.*

Fundamentalteoremet:

Teorem 6.14. *La F være en kropp, og $K = F(\alpha_1, \ldots, \alpha_n)$ være rotkroppen til et polynom over F. Da har Galoisgruppen alle egenskapene som er listet under. I detalj gjelder disse egenskapene* mellomkroppene*, E, som er kropper slik at $F \leq E \leq K$, og enhver slik kropp er knyttet til undergruppa $G(K/E)$, som består av alle automorfismer som etterlater hvert element i E fikst.*

1. *Avbildningen som knytter undergruppen $G(K/E)$ med mellomkroppen E, etablerer en 1-til-1 korrespondanse, dvs, en bijeksjon mellom mellomkroppene og undergruppa av Galoisgruppa, G.*

2. *Graden til kroppsutvidelsen fra E til K, er lik antallet elementer i den tilknyttede undergruppen $G(K/E)$ av Galoisgruppen. Dette er antallet automorfismer som fikser hvert element i E.*

3. *Dersom en mellomkropp $E = F(y_1, \ldots, y_m)$ er oppnådd ved å adjungere røttene $y_1, \ldots, y_m$ til F, til en likning hvor koeffisientene er inneholdt i F, og hvor alle røttene ligger i $F(\alpha_1, \ldots, \alpha_n)$, da inneholder Galoisgruppen $G(E/F)$, $|G|/|G(K/E)|$ automorfismer.*

Under vises en illustrasjon på forklaringen:

$$
\begin{array}{ccc}
K & & \{id\} \\
\cup & & \cap \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cup & & \cap \\
E & \leftrightarrow & H = G(K/E) \\
\cup & & \cap \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cup & & \cap \\
F & & G = G(K/F)
\end{array}
$$

Figur 6.2. Galoiskorrespondansen

Som vi ser, så er kroppene på venstre side, og automorfismegruppene på høyre. Det er en 1-til-1-korrespondanse mellom mellomkroppene K og undergruppene av Galoisgruppa G.
La oss se på et eksempel:

Eksempel : Vi skal finne Galoisgruppen, og undergruppene av denne, samt rotkroppen og underkroppene til polynomet $f(x) = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$, som har løsningene $\pm\sqrt{2}$ og $\pm\sqrt{3}$. Rotkroppen til dette polynomet, blir $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, som vi har sett på i et eksempel under delkapittelet om rotkropp.
Når vi har en slik rotkropp, vet vi fra siste eksempelet under delkapittelet 4.10.3, at vi kan skrive alle elementer i K på følgende måte:

$$(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3},$$

hvor $a, b, c, d \in \mathbb{Q}$.

Galoisgruppen, $G = G(K/\mathbb{Q})$ kan bestemmes ved å undersøke automorfismene i K, som holder a i ro.. Siden Galoisgruppa til et polynom kun permuterer røttene til et polynom, har vi en anelse om hvordan vi skal fortsette. Husk fra delkapittelet om kroppsutvideler, at $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, så Galoisgruppen inneholder 4 elementer.
For å danne disse 4 elementene fra de to røttene har vi disse mulighetene:

- $\sqrt{2}$ kan sendes enten på seg selv, eller på $-\sqrt{2}$.
- $\sqrt{3}$ kan sendes enten på seg selv, eller på $-\sqrt{3}$.

Når $\sqrt{2}$ sendes på seg selv, blir uttrykket ovenfor uforandret, så vi ser hva som skjer når vi sender $\sqrt{2}$ på $-\sqrt{2}$, og la oss kalle denne automorfismen eller permutasjonen for σ.

$$\sigma((a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3}) = (a-b\sqrt{2})+(c-d\sqrt{2})\sqrt{3}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6},$$

og la τ sende $\sqrt{3}$ på $-\sqrt{3}$, slik at:

$$\tau((a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3}) = (a+b\sqrt{2})-(c+d\sqrt{2})\sqrt{3}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}.$$

Disse to er automorfismer av K. Det er også identitetsautomorfismen, som ikke endrer noe, og det er sammensetningen av f og g, som endrer fortegnet på begge røttene.

$$(\sigma\tau)((a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3}) = (a-b\sqrt{2})-(c-d\sqrt{2})\sqrt{3} = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}.$$

Derfor er $G = \{e, \sigma, \tau, \sigma\tau\}$, som er den ikke-sykliske gruppa av orden 4. Galoisgruppa, G, har fire undergrupper:

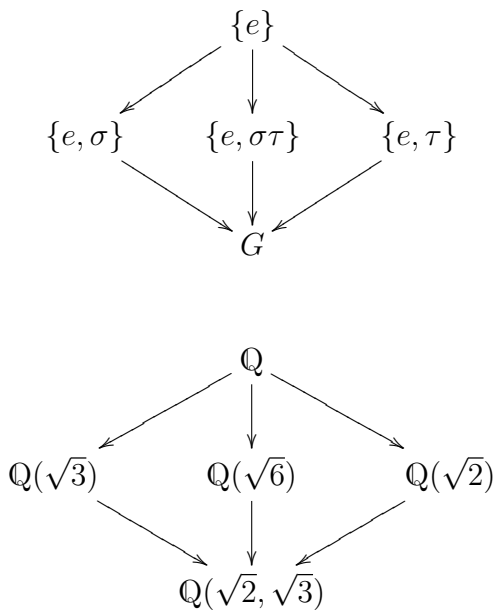
1. Den trivielle undergruppa, som kun inneholder identitetselementet. Dette tilsvarer hele F.

2. Undergruppa $\{e, \sigma\}$, som tilsvarer underkroppen $\mathbb{Q}(\sqrt{3})$, siden σ holder $\sqrt{3}$ fiksert.

3. Undergruppa $\{e, \tau\}$, som tilsvarer underkroppen $\mathbb{Q}(\sqrt{2})$, siden τ holder $\sqrt{2}$ fiksert.

4. Undergruppa $\{e, \sigma\tau\}$, som tilsvarer underkroppen $\mathbb{Q}(\sqrt{6})$, siden $\sigma\tau$ holder $\sqrt{6}$ fiksert.

Under vises en illustrasjon av eksempelet:



Figur 6.3. Eksempel 1.

Legg merke til at underkroppene av rotkroppen har grad 2 over $\mathbb{Q}$, og inneholder 2 elementer. $\mathbb{Q}$ inneholder 4 elementer, og fra den nyttige observasjonen i delkapittel 3.3.7, har vi at dersom ordenen til en undergruppe, H er halvparten av en gruppe, G, er $H \lhd G$. Dette betyr at alle undergruppene er normale. (Husk at $\{e\}$ og G også er normale undergrupper av G).

Eksempel : Vi ska nå finne alle undergrupper av Galoisgruppa, og alle underkropper av rotkroppen til følgende polynom:

$$x^4 - 5 \text{ over } \mathbb{Q}.$$

Vi vet at $x^4 - 5 = 0 \leftrightarrow x^4 = 5 \leftrightarrow x = \sqrt[4]{5}$. Vi kaller $\alpha = \sqrt[4]{5}$, så da har $x^4 - 5$ røttene $\pm\alpha, \pm\alpha i$.
Så vi lar K være rotkroppen av f over $\mathbb{Q}$: $K = \mathbb{Q}(\sqrt[4]{5}, i)$.
Da vet vi at $[K : \mathbb{Q}] = 8$, siden $\sqrt[4]{5}$ har grad 4 over $\mathbb{Q}$ og i har grad 2 over $\mathbb{Q}$.
Når graden til $[K : \mathbb{Q}] = 8$, har Galoisgruppen, G, 8 elementer.

Utskrift fra Maple:
$galois(x^4 - 5)$; "4T3", {D(4)"}, ", 8, {"(1 3)", "(1 2 3 4)"}

Hvor navnet på Galoisgruppa er: D_4 og den har 8 elementer.

Vi ser fra denne utskriften fra Maple, at Galoisgruppen er D_4.
La oss se litt videre. La f og g være automorfismene til $\mathbb{Q}(\sqrt[4]{5}, i)/\mathbb{Q}$ slik at:

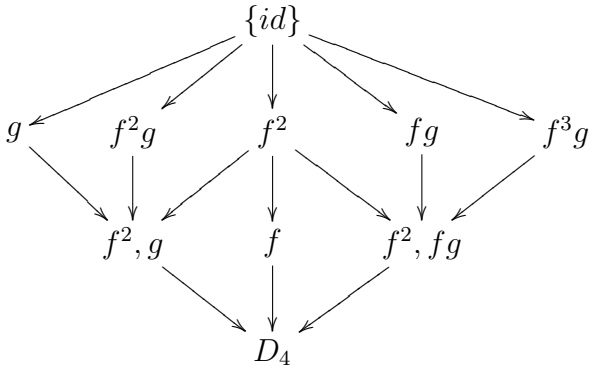
$$f(\sqrt[4]{5}) = \sqrt[4]{5}i, \;\; f(i) = i, \;\; g(\sqrt[4]{5}) = \sqrt[4]{5}, \;\; g(i) = -i.$$

La oss se på disse automorfismene i en tabell:

σ	$\{id\}$	f	f^2	f^3	g	fg	f^2g	f^3g
$\sigma(\sqrt[4]{5})$	$\sqrt[4]{5}$	$\sqrt[4]{5}i$	$-\sqrt[4]{5}$	$-\sqrt[4]{5}i$	$\sqrt[4]{5}$	$\sqrt[4]{5}i$	$-\sqrt[4]{5}$	$-\sqrt[4]{5}i$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

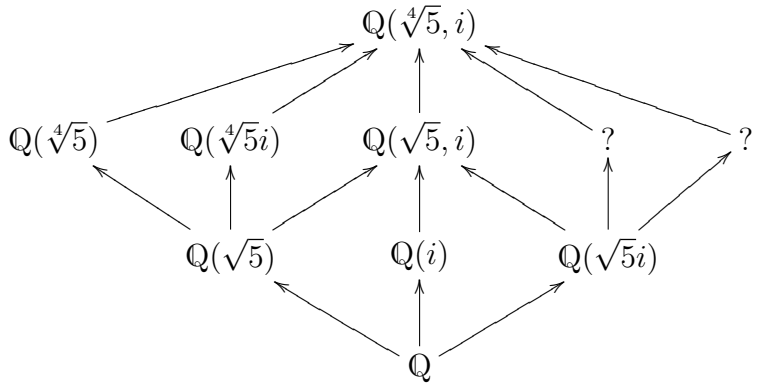
Tabell 6.1.

Vil bare minne om at $f^4, g^2 = \{id\}$, for da kommer du tilbake til utgangspunktet.
La oss nå bruke Galoiskorrespondansen, og se på de forskjellige underkroppene mellom $\mathbb{Q}(\sqrt[4]{5}, i)$ og $\mathbb{Q}$.



Figur 6.4a. Eksempel 2.

Først setter vi inn automorfismene, som vist i figuren over. Da kan man se samsvaret, eller korrespondansen, mellom undergruppene av automorfismegruppa, og underkroppene av rotkroppen.



Figur 6.4b. Eksempel 2.

Som vi har vært innom tidligere i oppgaven, er det en korrespondanse mellom de to figurene ovenfor.
Den første består av automorfismegruppa, altså polynomets Galoisgruppe, og dens undergrupper. Som man ser, så er det forskjellig orden på de forskjellige nivåene.
Siden vi i dette tilfellet snakker om D_4, er det 8 undergrupper av Galoisgruppen, og på samme måte er det 8 underkropper av rotkroppen.
I slutten av eksempelet sjekker vi om det finnes noen normale undergrupper.

La oss først se på permutasjonene, eller automorfismene, som er vist i den øverste av disse to figurene:
Siden vi har D_4, er det 8 automorfismer: $\{\{id\}, r, r^2, r^3, s, rs, r^2s, r^3s\}$.
Undergrupper av en gruppe av orden 8, må ifølge Lagrange ha en orden som går opp i 8, derfor er de forskjellige automorfismene satt opp slik de er, så at det er lett å se sammenhengen, mellom ordenen til de forskjellige automorfismene (permutasjonene) og underkroppene av rotkroppen.
På samme måte er underkroppene satt opp på denne måten, hvor man har de forskjellige underkroppene med lik orden, på den samme horisontale linjen.
For å vise dette litt klarer, kan vi bruke noen eksempler:
Alle speilinger har orden 2, slik at $s^2 = \{id\}$, og rotasjonene har orden 4, slik at $r^4 = \{id\}$ og $(r^2)^2 = \{id\}$.

Underkroppene har også en slik fordeling, basert på orden, som vi har nevnt tidligere. $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}] = 8$.
$[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(i)] = 4$.
$[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5}] = 2$.

Figuren over har 2 spørsmålstegn. Dette er på grunn av at de to resterende underkroppene ikke er så enkle å finne. Det vi vet, er at disse har orden 4 over $\mathbb{Q}$. Vi kan også se på den øverste av disse to figurene, at den ene av disse underkroppene holdes fikst av rs, men ikke av r^2, mens den andre holdes fikst av r^3s, men ikke av r^2. Vi har vært innom dette tidligere, men repeterer det nå.

La oss finne den første ukjente av de to, og kalle den α. Vi begynner med å skrive opp de generelle elementene til $\mathbb{Q}(\sqrt[4]{5}, i)$ over $\mathbb{Q}$.

$$\alpha = a + b\sqrt[4]{5} + c\sqrt{5} + d\sqrt[4]{5^2} + ei + f\sqrt[4]{5}i + g\sqrt{5}i + h\sqrt[4]{5^3}i$$

Siden denne underkroppen holdes fikst av rs ser vi hva som skjer når $rs(\alpha) = \alpha$.

$$rs(\alpha) = a + b\sqrt[4]{5}i - c\sqrt{5} + d\sqrt[4]{5^2}i - ei + f\sqrt[4]{5} + g\sqrt{5}i + h\sqrt[4]{5^3}$$

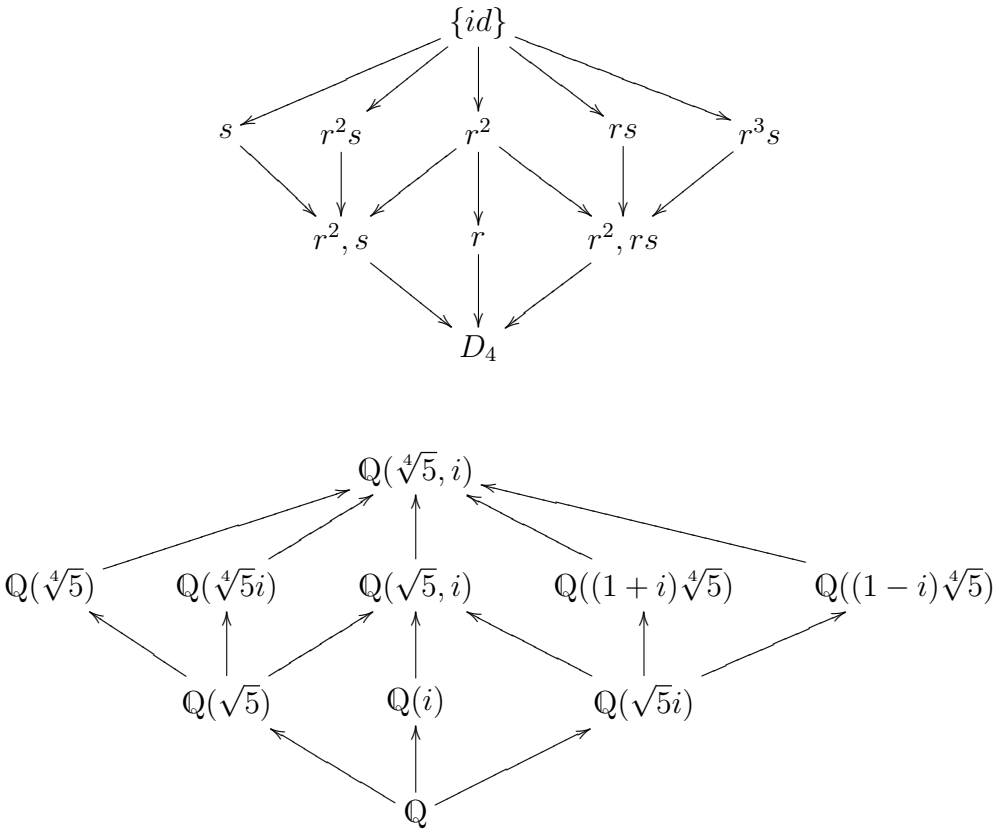
Man kan se at det blir slik ved å følge tabellen i starten av dette eksempelet. Da ser vi at dette skjer for følgende koeffisisenter: $b = f, c = -c, e0 - e, d = -h$.
Vi kan derfor skrive uttrykket slik:

$$\alpha = a + b(\sqrt[4]{5} + \sqrt[4]{5}i) + d(\sqrt[4]{5^3} - \sqrt[4]{5^3}i) + g\sqrt[4]{5}i.$$

De resterende koeffisientene kan hvilke som helst rasjonale tall, så for å gjøre det enkelt, velger vi $b = 0$, og de andre koeffisientene til 0. Da står vi igjen med:

$$\alpha = \sqrt[4]{5} + \sqrt[4]{5}i = (1 + i)\sqrt[4]{5}.$$

$r^2(\alpha) = -\alpha$, så α er fikst av rs, men ikke av r^2, som betyr at kroppen $\mathbb{Q}$ er i fikskroppen til rs, men ikke i fikskroppen til r^2, så $\mathbb{Q}$ må være fikskroppen til rs.
Differansen $\beta = \sqrt[4]{5} - \sqrt[4]{5}i$ er fikst av r^3s, men ikke av r^2, så fikskroppen til r^3s er $(1 - i)\sqrt[4]{5}$. Nå kan vi fylle ut diagrammet.
Vi tar med både diagrammet av undergrupper av Galoisgruppa, og det andre diagrammet som viser underkropper av rotkroppen til polynomet, slik at en enklere kan ser Galoiskorrespondansen, og hva den egentlig sier.



Figur 6.4c. Eksempel 2.

Henviser til eksempelet i 3.3.7 som omhandlet D_4.
Nå spørr vi: Er noen av undergruppene normale?
Fra eksempelet med D_4 fant vi ut at det er 3 undergrupper av orden 4. Disse er $< r^2, s >, < r >$ og $< r^2, rs >$ fra figuren. Husker fra nyttig observasjon at dersom $|H| = |G|/2$, er $H \lhd G$. Så disse er 3 er hvertfall normale undergrupper. Finnes det flere?
Ja, vi fant ut at det er 4 normale undergrupper av D_4, og den siste viser seg å være $< r^2 >$ på figuren.
Så vi har 4 normale undergrupper.

6.4 Oppsummering

• *Rotkroppen* til et polynom $f(x) \in F[x]$ er den minste kroppen som inneholder F og alle røttene til polynomet.

• En endelig kroppsutvidelse $F \leq E$ kalles en *Galoisutvidelse* dersom hver embedding av E over F er en automorfisme av E..

• La E være en kroppsutvidelse av F. Mengden av alle automorfismer av denne utvidelsen danner en gruppe, som noteres: $Aut(E/F)$. Dersom E/F er en Galoisutvidelse, kalles $Aut(E/F)$ *Galoisgruppen* av E over F, og noteres $G(E/F)$.

• Galois fundamentalteorem beskriver at det er en 1-til-1-korrespondanse mellom underkroppene til rotkroppen et polynom, og undergruppene til polynomets Galoisgruppe.

$$
\begin{array}{ccc}
K & & \{id\} \\
\cup & & \cap \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cup & & \cap \\
E & \leftrightarrow & H = G(K/E) \\
\cup & & \cap \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cup & & \cap \\
F & & G = G(K/F)
\end{array}
$$

Kilder som er brukt i dette kapittelet, er Fraleigh [3], kapittel 50 - 56, Lang [5], Kapittel 4, og Bewersdorff [2], kapittel 10.

7 Løsbarhet ved rottegn

Hvilke polynom som er løsbare ved rottegn, var noe Abel lurte på, men ikke fant ut i sitt korte liv. Galois derimot fant ut av dette, og gjennom sitt arbeid så han en sammenheng mellom polynomene som er løsbare ved rottegn. Vi begynner derfor med å forklare hva løsbarhet ved rottegn er, og når en gruppe er løsbar.

Definisjon 7.1. *La $F \leq F(\alpha)$ være en enkel algebraisk utvidelse. Da kalles* $F(\alpha)$ enkel radikal *over F dersom α er rot i likning av typen $x^n - a \in F[x], a \neq 0$, dvs, $\alpha^n = a \in F$.*

Eksempel : La $\alpha^2 = 2$, og $1+\sqrt{2} \in \mathbb{Q}(\alpha)$, og $\beta^3 = 1+\sqrt{2} \Rightarrow \beta = \sqrt[3]{1+\sqrt{2}}$. Da er $\mathbb{Q}(\alpha)$ en *enkel radikal* over $\mathbb{Q}$, og $\mathbb{Q}(\alpha)(\beta)$ er en *enkel radikal* over $\mathbb{Q}(\alpha)$. Elementene i $\mathbb{Q}(\alpha)(\beta)$ kan skrives på formen:

$$a_0 + a_1\beta + a_2\beta^2, \text{ der } a_0, a_1, a_2 \in \mathbb{Q}(\alpha).$$

Definisjon 7.2. *En utvidelse $F \leq K$ kalles* radikal *dersom det finnes en kjede av utvidelser*

$$F = F_0 \leq F_1 \leq F_2 \leq \ldots \leq F_r = K$$

der $F_i \leq F_{i+1}$ er en enkel radikal *utvidelse.*

Definisjon 7.3. *Gitt polynom $f(x) \in F[x]$. Da sier vi at $f(x)$ er* løsbar ved rottegn over F *dersom rotkroppen, E, til $f(x)$ over F er inneholdt i en radikal utvidelse K over F:*

$$F \leq E \leq K.$$

Definisjon 7.4. *Ei gruppe G kaller* løsbar *dersom det finnes en kjede av undergrupper*

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_n = G$$

slik at $G_{i-1} \lhd G_i$ for $i = 1, \ldots, n$ og alle kvotientgruppene G_i/G_{i-1} er abelske. En slik kjede kalles et abelsk tårn *for G.*

Teorem 7.5. *Enhver undergruppe H av en endelig løsbar gruppe G er løsbar.*

Bevis : Se e-bok Stewart [3], kapittel 14.1.

Eksempel : Alle abelske grupper er løsbare. Et viktig faktum er at S_3 og S_4 er løsbare, men S_n er ikke løsbar for $n \geq 5$.
Et abelsk tårn for S_3 er

$$\{\epsilon\} < A_3 < S_3$$

og for S_4

$$\{\epsilon\} < V < A_4 < S_4$$

der $V = \{\epsilon, (12)(34), (13)(24), (14)(23)\}$ er abelsk og normal i A_4 (Siden V er den eneste undergruppa av A_4 av orden 4).
Kvotientene er alle abelske grupper:

$$S_3/A_3 \cong \mathbb{Z}_2, A_3/\{e\} \cong A_3 \cong \mathbb{Z}_3.$$
$$S_4/A_4 \cong \mathbb{Z}_2, A_4/V \cong \mathbb{Z}_3, V/\{e\} \cong V \cong \mathbb{Z}_2 \text{ x } \mathbb{Z}_2.$$

Du kan 'lese av' fra Galoisgruppa til et polynom (dvs Galoisgruppa til rotkroppen til polynomet) om polynomet er løsbart ved rottegn.

Her kommer en av de store oppdagelsene til Galois. Han fant ut det Abel lenge prøvde å finne svaret på, nemlig når er en likning løsbar ved rottegn. Følgende teorem beskriver akkurat dette:

Teorem 7.6. *En likning er løsbar ved rottegn, hvis og bare hvis dens Galoisgruppe er løsbar.*

Bevis : Jeg følger beviset til Lang [5], side 116 - 117.
Lar R være rotkroppen til et polynom $f(x) \in F[x]$.
Skal vise at hvis $f(x)$ er løsbart ved rottegn over F, så vil Galoisgruppen til $f(x), G(R/F)$, være løsbar.
Vi antar alltid at R er inneholdt i en radikal utvidelse $F \subseteq K : F \subseteq R \subseteq K$.
Da har K en kjede av enkle radikale utvidelser

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_i \subseteq F_{i+1} \subseteq \ldots \subseteq F_r = K$$

der $F_{i+1} = F_i(\alpha_i)$ med $\alpha_i^{n_i} = a_i \in F_i$, for $i = 0, 1, \ldots, r-1$. Nå gjør Lang to antakelser:

1. $F \subseteq K$ er Galoisutvidelse.
2. F inneholder nok enhetsrøtter til at hver utvidelse $F_i \subseteq F_{i+1}$ blir en Galoisutvidelse, dvs at F_{i+1} er rotkroppen til polynomet $x^{n_i} - a_i \in F_i[x]$.

(Den første antakelsen gjøres også av Fraleigh [3], i del X, kapittel 56).

Jeg skal først vise at Galoisgruppa $G(K/F)$ blir løsbar.

Se på

$$F \subseteq F_i \subseteq F_{i+1} \subseteq K.$$

Siden vi antar at $F \subseteq K$ er Galois, vil også $F_i \subseteq K$ og $F_{i+1} \subseteq K$ være Galois, og vi får Galoisgruppene

$$\{e\} < G(K/F_{i+1}) < G(K/F_i) < G(K/F).$$

Siden $F_i \subseteq F_{i+1}$ er Galois, vet vi fra fundamentalteoremet, del II, at $G_{i+1} \lhd G_i$, og at $G(F_{i+1}/F_i) \cong G_i/G_{i+1}$.
Men i Lang side 116, punkt (2), blir det bevist at Galoisgruppen til $F_i \subseteq F_{i+1}$ er abelsk. Dermed vil Galoisgruppene $G(K/F_i)$ være en kjede av normale undergrupper med abelske kvotienter, som nettopp betyr at $G(K/F)$ er løsbar.
Til slutt, vi har $F \subseteq R \subseteq K$, der $F \subseteq R$ er Galois. Da vet vi igjen fra fundamentalteoremet del II, at $G(K/R) \lhd G(K/F)$ og at $G(R/F)$ er kvotientgruppa. Siden $G(K/F)$ er løsbar, følger det at $G(R/F)$ er løsbar, se Stewart, e-bok [3], teorem 14.4.

Både Galois og Abel beviste at den generelle likningen av grad ≥ 5 ikke kunne løses ved rottegn. Galois sa det elegant ved å vise at S_n ikke er en løsbar gruppe for $n \geq 5$, mens Abel brukte lange og kompliserte utregninger.

Under vises to eksempler på Abels arbeid.
Først en grov skisse av hans bevis for at den generelle likningen av grad høyere enn 4 ikke kan løses ved rottegn, og til slutt, et teorem om når en likning er løsbar ved rottegn.

7.1 Abels bevis

Henviser til Pesic [5], s. 155 - 169 for Abels bevis.
Beviset er langt og komplisert, men vi tar det groveste.

Vi antar at den generelle femtegradslikningen

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

kan løses ved rottegn. La røttene vaere x_1, x_2, x_3, x_4, x_5 og diskriminanten

$$D = [(x_1 - x_2)(x_1 - x_3)\dots(x_4 - x_5)]^2.$$

Vi antar at røttene er ulike.

Etter svært lange, kompliserte utregninger og argumentasjoner, kommer Abel til slutt fram til at dersom likningen kan løses ved rottegn, så må følgende gjelde:

$$\frac{1}{5}(x_1 + \omega^4 x_2 + \omega^3 x_3 + \omega^2 x_4 + \omega x_5) = (p + p_1\sqrt{D})^{\frac{1}{5}}$$

hvor ω er en primitiv 5-te enhetsrot, og p, p_1 er bestemte rasjonale funksjoner av koeffisientene a, b, c, d, e.
Venstresiden har 120 mulige verdier: 5 mulige for x_1, så 4 mulige for x_2 osv, dvs, $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ verdier. Men høyresiden har bare 10 mulige verdier: To verdier for kvadratroten, og for hver av disse, 5 verdier for 5.-te roten.
Da har vi en selvmotsigelse, og antakelsen i begynnelsen av beviset stemmer ikke.
Beviset er da fullført.

Abels teorem: (Tignol [7], kap 14.)

Teorem 7.7. *La P være et polynom av grad n over en kropp F, med røtter $x_1, \ldots, x_n$ i en kroppsutvidelse av F. Dersom det eksisterer rasjonale funksjoner $\theta_2, \ldots \theta_n \in F[x]$ slik at*

$$r_i = \theta_i(r_1) \text{ for } i = 2, \ldots, n.$$

og

$$\theta_i(\theta_j(r_1)) = \theta_j(\theta_i(r_1)) \text{ for alle } i, j$$

er likningen $P(X) = 0$, løsbar ved rottegn over F.

Vi har vært innom permutasjoner i kapittel 3, men vi får bruk for det her, i allefall permutasjonsgruppene S_n og A_n. Minner om at S_n er mengden av alle permutasjoner av $\{1, 2, \ldots, n\}$.

Teorem 7.8. *De jamne permutasjonene i S_n utgjør en undergruppe av S_n, notert A_n og er kalt den* alternerende gruppa. *A_n har orden $n!/2$.*

Vi skal nå se litt på noen eksempler på forskjellige polynom, noen som er løsbare ved rottegn, og noen som ikke er det.
Vi begynner med andre-, tredje-, og fjerdegradspolynom, som vi vet er løsbare ved rottegn (se kapittel 2).
Det vil bli utregninger av Galoisgrupper til de forskjellige polynom, både på teoretisk plan, men også litt med Maple.
Der hvor jeg har brukt Maple, og viser utskriften, har jeg markert hva som er Galoisgruppa, og hva ordenen er.

7.2 Andregradspolynom

Som en kjapp repetisjon, minner vi om at det generelle andregradspolynomet ser slik ut: $ax^2 + bx + c$. For å løse en andregradslikning, over hvilken som helst kropp, bruker vi formelen:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

hvor $D = b^2 - 4ac$, kalles diskriminanten.

Et polynom av andre grad har to røtter, og har enten Galoisgruppa A_2 eller S_2. Galoisgruppa blir A_2 dersom diskriminanten er et kvadrat. Grunnen til dette er at dersom diskriminanten er et kvadrat, løser man opp rottegnet, og svaret blir et tall i $\mathbb{Q}$ som ikke er irredusibelt, siden vi som regel ser på polynomer over $\mathbb{Q}$. Dersom diskriminanten ikke er et kvadrat, er Galoisgruppa S_2.
A_2 inneholder kun et element, identitetspermutasjonen, mens S_2 inneholder 2.
I tillegg til identitetspermutasjonen, σ_0, er det en permutasjon σ_1 som permuterer de to løsningene.
La oss se på tabellen og et eksempel.

Eksempel :

$$x^2 - 6x + 1 = 0 \text{ over } \mathbb{Q}.$$
$$x = 3 \pm 2\sqrt{2}$$

Siden $\sqrt{2} \notin \mathbb{Q}$, ser vi at rotkroppen til dette polynomet er $\mathbb{Q}(\sqrt{2})$. Minner om at $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
Siden σ_1 permuterer de to løsningene, kan den skrives som $\sigma_1(a + b\sqrt{2}) = a - b\sqrt{2}$.
Her blir Galoisgruppa S_2.

	σ_0	σ_1
σ_0	σ_0	σ_1
σ_1	σ_1	σ_0

$=$

	σ_0	σ_1
σ_0	$a + b\sqrt{2}$	$a - b\sqrt{2}$
σ_1	$a - b\sqrt{2}$	$a + b\sqrt{2}$

Eksempel :

$$x^2 + 2x - 1 \text{ over } \mathbb{Q}$$
Diskriminanten er: $b^2 - 4ac = 4 - (-4) = 8$.

8 er ikke et kvadrat, og Galoisgruppa blir S_2

7.3 Tredjegradspolynom

Når det gjelder irredusible polynomer av tredje grad, er det to muligheter. Enten inneholder Galoisgruppa alle de seks permutasjonene av de tre røttene, S_3, eller så inneholder den tre permutasjoner som permuterer løsningene syklisk, A_3.
La $K = F(\alpha_1, \alpha_2, \alpha_3)$ være rotkroppen til f. La G være Galoisgruppa av K over F. Vi antar at f er irredusibel. Da er G representert som en undergruppe av den symmetriske gruppa S_3. Siden K inneholder $F(\alpha)$ for alle røtter α av f, følger det at $[K : F]$ er delelig med 3, og ordenen til G er enten 3 eller 6.

Definisjon 7.9. *Anta $f(x) \in \mathbb{Q}[x]$ har røttene $\alpha_1, \ldots, \alpha_n$. Da er* diskriminanten *til $f(x), D$ gitt ved*

$$D = [\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)]^2.$$

Teorem 7.10. *Gruppa G er isomorf med S_3 hvis og bare hvis diskriminanten ikke er et kvadrat i F. Dersom diskriminanten er et kvadrat i F, har K grad 3 over F.*

Diskriminanten til tredjegradslikningen er:

$$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Eksempel : $x^3 + x^2 - 2x - 1 = 0$.
$D = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd = 4 - (-32) - (-4) - 27 + 36 = 49 = 7^2$

Diskriminanten er et kvadrat, og det betyr at Galoisgruppa til dette polynomet er A_3.

Eksempel : $x^3 + x - 6 = 0$. (Legg merke til at det ikke er noen b med her.)
$D = -4ac^3 - 27a^2d^2 = -4 - (27 \cdot 6) = -166$

Diskriminanten er ikke et kvadrat, og det betyr at Galoisgruppa til dette polynomet er S_3.

7.4 Fjerdegradspolynom

Irredusible polynomer av fjerde grad, kan ha Galoisgrupper med 4, 8, 12 eller 24 permutasjoner, som er: V, C_4, D_4, A_4 og S_4. (Bewersdorff [2], kap 9, Tignol [7], kap 14).
C_4 er en syklisk gruppe med orden 4, mens D_4 er den dihedrale gruppa.

Eksempel :

$$x^4 - 2 = 0 \text{ over } \mathbb{Q}$$
$$x^4 = 2$$
$$x = \sqrt[4]{2} = \alpha$$

Fjerderot gir fire løsninger, og vi vet at løsningene er $\pm\alpha, \pm\alpha i$.
Rotkroppen til polynomet finner vi ved å adjungere α og i til $\mathbb{Q}$. Rotkroppen til polynomet blir da: $K = \mathbb{Q}(\sqrt[4]{2}, i)$.
For å finne graden til utvidelsen husker vi: $[K : \mathbb{Q}]$.
Vi skriver det opp på denne måten:

$$\begin{aligned}[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \\ &= 2 \cdot 4 = 8.\end{aligned}$$

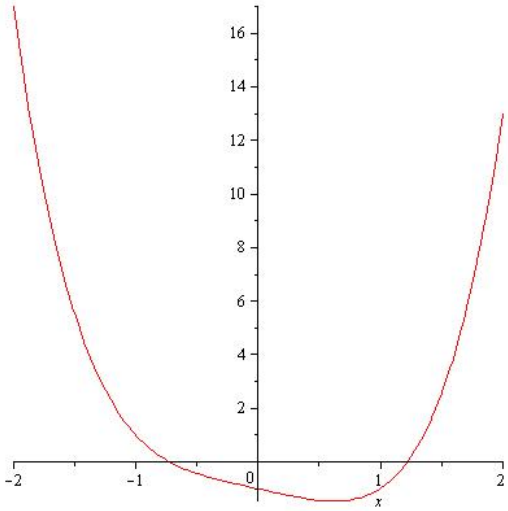
Graden til utvidelsen er 8, det betyr at antall elementer i Galoisgruppa er 8, og Galoisgruppa er D_4.

Det er ikke alltid like lett å finne røttene til et fjerdegradspolynom, men det er det som er utgangspunktet for å finne Galoisgruppa. Heldigvis finnes det en generell formel for å finne røttene til et fjerdegradspolynom, men den er komplisert, og det tar tid å finne røttene. Maple, er et bra program en kan bruke, og det har en egen Galoisfunksjon. Denne skal jeg vise i neste eksempel.
Vi avslutter dette delkapittelet med å se på et fjerdegradspolynom som er litt vanskeligere å løse.

Eksempel :

$$x^4 - x - 1 = 0 \text{ over } \mathbb{Q}.$$

For å kunne finne løsningene, må en sjekke likningen, og se hvordan den oppfører seg for forskjellige x-verdier, altså se på grafen.
Ved å tegne en graf, kan en se hvor mange reelle røtter likningen har, og hvor disse ligger.



Figur 7.1. Eksempel.

Som vi ser, har denne likningen to reelle røtter, og må da ha to komplekse røtter.
Fra her er det vanskelig å bestemme løsningene eksakt, så vi bruker Maple.
Utskrift:
$irreduc(x^4 - x - 1)$; true
$galois(x^4 - x - 1)$; "4T5", {"$\mathbf{S_4}$"}, ", **24**, {"(1 4)", "(2 4)", "(3 4)"}
Polynomet er irredusibelt over $\mathbb{Q}$ og har Galoisgruppe S_4.

Generelt:
$x^4 \pm x \pm 1$, har orden 24.
$x^4 \pm 2x + 1$, har orden 24.
$x^4 \pm 3x \pm 1$, har orden 24.
$x^4 \pm 4x + 1$, har orden 24.
$\Rightarrow x^4 \pm (2j+1)x \pm 1$ orden 24, for $j = 0, \ldots, n$, og
$x^4 \pm (2j)x \pm 1$ har orden 24, for $j = 3, \ldots, n$.

Vi har også:
$x^4 \pm (2j+1)x^3 \pm 1$ orden 24, for $j = 0, \ldots, n$, og
$x^4 \pm (2j)x^3 \pm 1$ har orden 24, for $j = 3, \ldots, n$.

Løser noen oppgaver i Maple:

Eksempel :

$$x^4 + 1 \text{ har Galoisgruppe } C_4$$

Eksempel :

$$x^4 - 2 \text{ Har Galoisgruppe, } D_4$$

Eksempel :

$$x^4 - 8x + 12 \text{ har Galoisgruppe } A_4$$

7.5 Polynom av høyere grad

Irredusible polynomer av femte grad, kan ha Galoisgruppe med 5, 10, 20, 60 eller 120 elementer, Bewersdorff [2], kap 9. Grupper med 5, 10 eller 20 elementer er løsbare (f.eks C_5, D_5 og F_5, Frobenius' gruppe), mens grupper med 60 eller 120 elementer, ikke er løsbare med rottegn (f.eks A_5 og S_5).
Siden det ikke finnes en generell formel for å finne røtter av polynomer av høyere grad enn 4, er det ikke alltid like lett å finne røttene til et slikt polynom. I de enkle tilfellene kan en bruke noen metoder, men til de vanskelige polynomene, må man nesten bruke Maple, eller et lignende program.
Vi kan se på ett av disse enkle tilfellene som et eksempel:

Eksempel :

$$x^5 - 2 = 0 \text{ over } \mathbb{Q}$$
$$x^5 = 2$$
$$x = \sqrt[5]{2}$$

Her er det kun en reell løsning, og 4 komplekse løsninger.

La $\alpha = \sqrt[5]{2}$, og la $\omega = e^{i\frac{2\pi}{5}}$. ($\omega^5 = 1$). Da har $x^5 - 2 = 0$ følgende løsninger:

$$\alpha, \alpha\omega, \alpha\omega^2, \alpha\omega^3, \alpha\omega^4, \text{ hvor } \omega \text{ har grad 4.}$$

Da ser vi at rotkroppen er $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\sqrt[5]{2}, \omega)$.
Denne kroppsutvidelsen har da grad 20, siden $\mathbb{Q}(\sqrt[5]{2})$ har grad 5 over $\mathbb{Q}$ og $\mathbb{Q}(\omega)$ har grad 4 over $\mathbb{Q}$.
$4 \cdot 5 = 20$, og Galoisgruppa til dette polynomet blir:

Utskrift fra Maple:
$galois(x^5 - 2)$; "5T3", {"5:4", "$\mathbf{F_5}$"}, ", **20**, {"(1 2 3 4 5)", "(1 2 4 3)"}

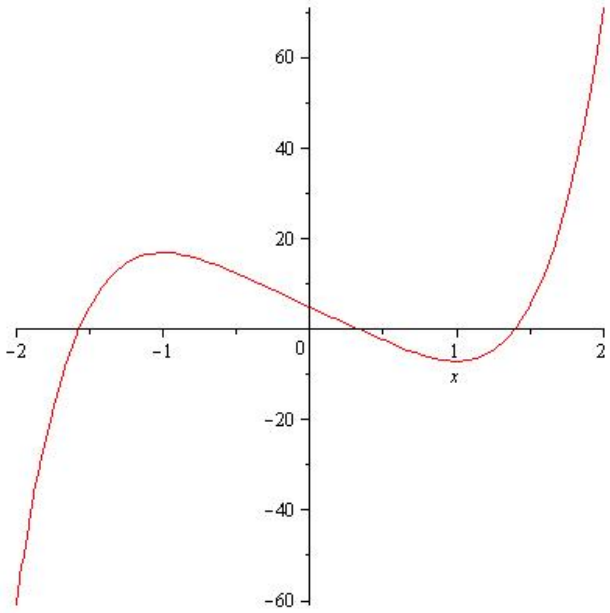
Galoisgruppen er Frobenius' gruppe, F_5, med orden 20.

Vi løser et til eksempel teoretisk, før vi tar noen eksempler i Maple.

Eksempel :

$$3x^5 - 15x + 5 \text{ over } \mathbb{Q}.$$

Ved å bruke Eisensteins kriterium (4.9.1), ser vi at polynomet er irredusibelt over $\mathbb{Q}$.
Vi bruker Maple til å plotte grafen til polynomet:



Figur 7.2. Eksempel.

Vi vet at rotkroppen til polynomet er $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$, hvor det er tre reelle røtter og to komplekse.
Vi vet også fra tidligere at alle Galoisgrupper av femtegradspolynom er en undergruppe av S_5, så $G(K/\mathbb{Q})$ må være isomorf med en undergruppe av S_5.
Siden α_1 er et nullpunkt i det irredusible polynomet av grad 5 over $\mathbb{Q}$ vet vi fra korollar 4.21, at $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 5$, og derfor må $[K : \mathbb{Q}]$ være delelig med 5.
Avbildningen $\mathbb{C} \to \mathbb{C}$ sender $a + bi$ til $a - bi$ siden vi har to komplekse røtter.
Av dette kan vi konkludere med at $G(K/\mathbb{Q})$ inneholder en 2-sykel.
Men siden den eneste undergruppen av S_5 som inneholder en 2-sykel og en 5-sykel, er S_5 selv, (se oppgave 27 i kapittel 27 i Gallian [4]) kan vi konkludere med at $G(K/\mathbb{Q}) \cong S_5$.
Siden S_5 ikke er løsbar ved rottegn, er ikke polynomet løsbart ved rottegn.

La oss prøve to oppgaver fra Ian Stewarts bok. (e-bok [3])

Eksempel : Finn rotkroppen og Galoisgruppa til $f(x) = x^6 - 7$ over $\mathbb{Q}$.
Vet at $f(x)$ er irredusibel over $\mathbb{Q}$ (Eisenstein), så $\alpha = \sqrt[6]{7} \in \mathbb{R}$ har grad 6 over $\mathbb{Q}$. Røttene til $f(x)$ blir da $\alpha, \alpha\omega, \ldots, \alpha\omega^5$ der $\omega (= e^{i2\pi/6})$ er en primitiv 6. enhetsrot.
Hva er graden til ω? Vet at $\omega^3 = -1$, og $x^3 + 1 = (x+1)(x^2 - x + 1)$ der $x^2 - x + 1$ er irredusibel over $\mathbb{Q}$, så graden til ω er 2 over $\mathbb{Q}$. Dermed blir rotkroppen til $f(x)$ lik $F = \mathbb{Q}(\alpha, \omega)$ som har grad $6 \cdot 2 = 12$ over $\mathbb{Q}$. Galoisgruppen til F blir D_6:

Utskrift fra Maple:
$galois(x^6 - 7)$; "6T3",{"**D$_6$**", S(3)[x]2"}, ", **12**, {"(1 2 3 4 5 6)", "(5 6)(1 4)(2 3)"}

Det som er interessant fra denne utskriften. er det som er uthevet. Det forteller Galoisgruppa, og den er D_6, som har orden 12.

Eksempel :

$$x^6 - 2x^3 - 1 \text{ over } \mathbb{Q}.$$

Dette er et polynom i x^3, så vi setter $u = x^3$, dvs $u^2 - 2u - 1 = 0$, med røtter $a = 1 + \sqrt{2}, b = 1 - \sqrt{2}$. Vi kan faktorisere $f(x) = (x^3 - a)(x^3 - b)$. Merk at $ab = -1$, dvs, $b = -\frac{1}{a}$. Så hvis vi lar $\alpha^3 = a$, blir røttene i $f(x)$: $\alpha, \alpha\omega, \alpha\omega^2, -1/\alpha, -\omega/\alpha, -\omega^2/\alpha$ derω er en primitiv 3. enhetsrot. Vi har $x^3 - 1 = (x-1)(x^2 + x + 1)$ der $x^2 + x + 1$ er irredusibelt over $\mathbb{Q}$, så ω har grad 2. Dermed blir rotkroppen til $f(x)$, lik $F = \mathbb{Q}(\sqrt{2}, \alpha, \omega)$ som får grad $2 \cdot 3 \cdot 2 = 12$ over $\mathbb{Q}$.
Polynomet har Galoisgruppen D_6.

Utskrift fra Maple:
$galois(x^6 - 7)$; "6T3",{"**D$_6$**", S(3)[x]2"}, ", **12**, {"(1 2 3 4 5 6)", "(5 6)(1 4)(2 3)"}

Under er noen eksempler som er gjort i Maple:

Eksempel :

$x^6 - 5x^4 + 3x^3 - 1$ har Galoisgruppe S_6, med 720 elementer. Dette polynomet er ikke løsbart ved rottegn.

Eksempel :

$x^6 - 3x^2 - 6$ har Galoisgruppe D_6, med 12 elementer. Dette polynomet er løsbart ved rottegn.

7.6 Andre anvendelser

Selv om Galoisteorien ikke er en metode forå løse likninger, forteller den hvilke polynom som er løsbare ved rottegn og ikke. Ved hjelp av Galoisgruppen til polynomet er det ikke så vanskelig å finne ut om et polynom er løsbart ved rottegn eller ikke. Problemet er å finne Galoisgruppen til et polynom. Selv om dette ikke er enkelt, finnes det videreutviklinger både fra Galois' og Abels arbeid som kan hjelpe med dette.

Galois skrev selv: (Tignol [7], kap 14, s. 240)
Dersom du gir meg en likning som du selv har valgt ut, og du vil vite om den er løsbar ved rottegn eller ikke, kan jeg ikke gjøre annet enn å forklare deg nøye at at det er mulig å svare på spørsmålet, uten å ville gi meg selv eller noen andre oppgaven med å gjøre det. Utregningene er upraktiske.

Generelt:
$x^n - 1$, hvor n er et primtall, er løselig ved rottegn.
$x^{2n} + 2$ for $n = 2, \ldots$ har Galoisgruppe D_{2n}.
$x^5 - x \pm 1$, har orden 120, og er ikke løselige ved rottegn.
$x^5 \pm x^2 \pm 1$, har orden 120, og er ikke løselige ved rottegn.
$x^5 \pm x^3 \pm 1$, har orden 120, og er ikke løselige ved rottegn.

$x^j \pm x \pm 1$,har Galoisgruppen S_j for $j \leq 2$, men for $j \neq 8$, er det kun $x^8 \pm x - 1$ som har Galoisgruppe S_8. I tillegg har vi spesialtilfellet med $x^5 - x \pm 1$, som ikke er løsbar ved rottegn, mens dersom vi har $x^5 + x \pm 1$ er likningen ikke irredusibel.

Det er faktisk kun 5 løsbare femtegradslikninger av formen $x^5 + ax^2 + b$. Disse er:

$$x^5 - 2s^3x^2 - \frac{s^5}{5}$$
$$x^5 - 100s^3x^2 - 1000s^5$$
$$x^5 - 5s^3x^2 - 3s^5$$
$$x^5 - 5s^3x^2 + 15s^5$$
$$x^5 - 25s^3x^2 - 300s^5$$

hvor s er en skalar.
Hvem som oppdaget dette er ukjent, men blant anne Paxtor Young var blant en av de som fant mange løsbare femtegradslikninger på slutten av 1800-tallet.
Kilde: http://en.wikipedia.org/wiki/Quintic_function.

Dersom vi har: $x^5 + x^4 + x^3 + x^2 + x + 1$, kan dette polynomet knyttes til S_5 dersom man erstatter ett av plusstegnene med et minustegn.
Dette fungerer faktisk for alle polynom av denne formen så lenge den høyeste graden er et oddetall.
Dersom man erstatter alle plusstegnene med minustegn, kan alle polynom på denne formen knyttes til den fulle Galoisgruppa. (Tenker selvfølgelig fra $n = 2$ og oppover.)

Galoisgruppen til et polynom på formen $x^{p-1} + x^{p-2} + \ldots + 1$ er en syklisk gruppe av orden $p - 1$ når p er et primtall.

Abel jobbet mye med liknigner, og prøvde å finne ut hvilke som var løsbare ved rottegn. Under står et av korollarene hans som er en videreutvikling fra et av hans teoremer. (Teoremene og korollaret er hentet fra Tignol [7], kap 14.)

Korollar 7.11. *La P være et irredusibelt polynom av grad p over en kropp F, hvor p er et primtall. Likningen $P(X) = 0$ er løsbar ved rottegn over F hvis og bare hvis alle røttene i P, kan bli uttrykt over F fra hvilke som helst to av dem.*

Korollar 7.12. *La P være et irredusibelt polynom av grad p hvor p er et primtall. Dersom antallet reelle røtter i P er minst 2, men mindre enn p er ikke polynomet løsbart ved rottegn over $\mathbb{Q}$.*

Bevis : La $r_1, \ldots r_p$ være røttene til P, og anta at $r_1, r_2 \in \mathbb{R}$, og $r_p \notin \mathbb{R}$. Da er $\mathbb{Q}(r_1, r_2) \subset \mathbb{R}$, og $r_p \notin \mathbb{Q}(r_1, r_2)$. Fra korollar 9.3, kan vi da se at $P(x) = 0$ ikke er løsbar ved rottegn over $\mathbb{Q}$.

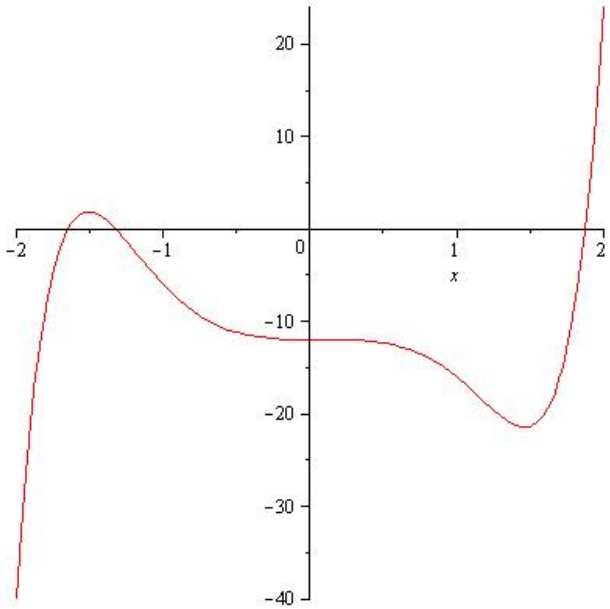
Det var Leopold Kroenecker som oppdaget dette ved å bruke Abels arbeid på dette området.

Korollar 7.13. *La P være et irredusibelt monisk polynom av grad p over $\mathbb{Q}$. La $p \equiv 1 \ (mod\ 4)$. Dersom diskriminanten til P er negativ er ikke $P(X) = 0$ løsbar ved rottegn.*

Eksempel :

$$x^7 - 2x^5 - 4x^3 + x^2 - 12 \text{ over } \mathbb{Q}.$$

Plotter denne i Maple, eller på kalkultor, og får denne kurven:



Figur 7.3. Eksempel.

Ser at funksjonen har 3 reelle røtter, og vet da at Galoisgruppen S_7, siden 7 er et primtall.

Utskrift fra Maple:
$galois(x^7 - 2 * x^5 - 4 * x^3 + x^2 - 12)$; "7T7", {"$\mathbf{S_7}$"}, ", **5040**, {"(1 7)", "(2 7)", "(3 7)", "(4 7)", "(5 7)", "(6 7)"}

7.7 Oppsummering

• Et generelt polynom av n-te grad har Galoisgruppe S_n.

Polynom av andre, tredje og fjerde grad kan alltid løses ved rottegn, og Galoisgruppen til slike polynom er kjent:

- Irredusible andregradspolynom har alltid S_2 som Galoisgruppe.
- Irredusible tredjegradspolynom har enten A_3 eller S_3 som Galoisgruppe. Det som bestemmer dette, er om diskriminanten er et kvadrat eller ikke.
- Irredusible fjerdegradspolynom har enten V, C_4, D_4, A_4 eller S_4 som Galoisgruppe.

• La $F \leq F(\alpha)$ være en enkel algebraisk utvidelse. Da kalles $F(\alpha)$ *enkel radikal* over F dersom α er rot i likning av typen $x^n - a \in F[x], a \neq 0$, dvs, $\alpha^n = a \in F$.

• En utvidelse $F \leq K$ kalles radikal dersom det finnes en kjede av utvidelser

$$F = F_0 \leq F_1 \leq F_2 \leq \ldots \leq F_r = K$$

der $F_i \leq F_{i+1}$ er en *enkel radikal* utvidelse.

• Gitt polynom $f(x) \in F[x]$. Da sier vi at $f(x)$ er *løsbar ved rottegn over* F dersom rotkroppen, E, til $f(x)$ over F er inneholdt i en radikal utvidelse K over F:

$$F \leq E \leq K$$

• Ei gruppe G kaller *løsbar* dersom det finnes en kjede av undergrupper

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_n = G$$

slik at $G_{i-1} \lhd G_i$ for $i = 1, \ldots, n$ og alle kvotientgruppene G_i/G_{i-1} er abelske. En slik kjede kalles et abelsk tårn for G.

• Enhver undergruppe H av en endelig løsbar gruppe G er løsbar.

• En likning er løsbar ved rottegn, hvis og bare hvis dens Galoisgruppe er løsbar.

Kilder som er brukt i dette kapittelet, er Lang [5], kapittel 4, Bewersdorff [2], kapittel 9, Gallian [4], kapittel 33, Tignol [7], kapittel 14 og e-bok Stewart [3], kapittel 14.

8 Konklusjon

Konklusjonen med denne oppgaven er at Galoisteorien, selv om dette ikke er en metode eller algoritme en bruker for å løse likninger, forteller hvilke polynom som er løsbare ved rottegn gjennom den flotte, og nærmest vakre korrespondansen mellom underkropper av rotkroppen til et polynom og undergrupper av polynomets Galoisgruppe.
Galoisteorien svarer på det Abel, men sikkert mange andre også lurte på; hvilke likninger av høyere grad enn 4 er løsbare ved rottegn, når det var kjent at det ikke fantes en formel for å løse disse.
Galoisteorien har også bidratt til matematikken på andre måter. Ved å se på denne teorien fra andre sider i nyere tid, har det oppstått en moderne presentasjon av Galoisteorien, som ikke bare er mer elegant, men som også skaper relasjoner mellom mange forskjellige matematiske emner.
Selv om selve Galoisteorien ikke blir brukt så mye i dagens matematikk, er det mange som hevder at dette er noe av den peneste matematikken som er oppdaget, og den var, i tillegg til Abels teori, med på å løse et problem som hadde stått uløst i flere hundre år. Galoisteorien går til og med videre og forteller om strukturen til et polynom som er løsbart ved rottegn. At en så ung matematikere, kan komme frem til så flott teori, tross i hans turbulente liv, er helt fantastisk, og absolutt verdt å skrive en masteroppgave om.
Igjen, selv om Galoisteorien ikke er den viktigste matematikken sett gjennom praktiske øyne, gir den en flott samenheng mellom forskjellige matematiske grener, og har mye viktig matematisk historie.

9 Avslutning

En avslutning, ofte kalt en oppsummering, skal hovedsaklig bestå i korte trekk hva oppgaven har handlet om, mine synspunkter og hva jeg har lært.

I en hver oppgave hører det til å ta med en historisk del. I denne oppgaven omfatter denne historiske delen et kapittel om likninger, og en kort biografi av Abel og Galois.
Videre er dette en oppgave som bygges opp gradvis gjennom kapitler om grupper, ringer, kropper, Galoisteori, og bruk av Galoisteorien. Et av høydepunktene i oppgaven er slutten av kapittel 6 som beskriver Galois' fundamentalteorem, også kalt Galoiskorrespondansen.
Fundamentalteoremet beskriver, som sagt i konklusjonen, en korrespondanse mellom underkropper av rotkroppen til et polynom og undergrupper av polynomets Galoisgruppe.
Videre i oppgaven er det beskrevet mange flotte poeng, og fine teoremer, som er utviklet etter Galois' og Abels arbeid.
Det viktigste poenget med Galoisteorien er at den beskriver hvilke polynom som er løsbare ved rottegn, og hvorfor det ikke finnes en generell formel for å løse likninger av orden høyere enn 4, et problem som stod uløst i mange hundre år.

Mine egne erfaringer med å jobbe med et slikt nytt tema, har vært mange. Jeg har fått utfordre meg selv til å lære nye ting, kunnet sette meg inn i beviser på en helt ny måte, og i tillegg merket hvor utrolig spesifikk og nøyaktig en må være når en fører bevis.
Oppgaven har også krevd av meg at jeg må velge ut det som er viktig, og hva som kan forkastes. Selv om denne oppgaven er en masteroppgave som krever at en går dypt inn i et tema, er det også viktig å vite når en graver for dypt. Det har selvfølgelig oppstått problemer underveis, som blant annet forståelse av teori (hvor alt dette har vært på engelsk), hvordan en skriver definisjoner og teoremer, og hvordan en fører bevis. Heldigvis har jeg hatt en god veileder som har hjulpet meg med de problemene jeg har hatt.

I tillegg til å ha lært meg mye ny og spennende matematikk, har jeg også lært meg Latex. Dette programmet har jeg skrevet hele oppgaven i, og dette gir et profesjonelt preg over oppgaven. Latex er også et program som er nyttig å ta med seg videre, hvor dette garantert kommer til nytte i læreryrket.

10 Kilder

Bøker

[1] Armstrong M. A.. *Groups and Symmetry.* Springer, 1988.

[2] Bewersdorff, Jörg. *Galois Theory for Beginners.A Historical Perspective. 2nd edition.* Friedr. Vieweg & Sohn Verlag, 2004.

[3] Fraleigh, John B. *A First Course in Abstract Algebra. 7th edition.* International Edition. Pearson Education, Inc, 2003.

[4] Gallian, Joseph A. *Contemporary Abstract Algebra. 2nd edition.* D. C. Health and Company. 1990..

[5] Lang, Serge. *Algebraic Structures.* Addison Wesley, Massachusetts, 1968.

[6] Pesic, Peter. *Abel's Proof - An Essay on the Sources and Meaning of Mathematical Unsolvability.* Massachusetts Institute of Technology, 2003.

[7] Tignol, Jean-Pierre. *Galois Theory of algebraic equations.* World Scientific Publishing Co. Pte. Ltd, 2001.

E-bøker

[1] Baker, Andrew. *An Introduction to Galois Theory.*

[2] Milne, J. S. *Fields and Galois Theory.* Version 4.21.

[3] Stewart, Ian. *Galois Theory 3rd edition.* Chapman & Hall/CRC.

Internett

Algebra :
http://no.wikipedia.org/wiki/Niels_Henrik_Abel
http://en.wikipedia.org/wiki/%C3%89variste_Galois
http://en.wikipedia.org/wiki/Galois_group
http://en.wikipedia.org/wiki/Fundamental_theorem_of_Galois_theory
http://hubpages.com/hub/Abels-Proof–A-Gentle-Introduction-to-the-Sublime-Beauty-of-Mathematics
http://fermatslasttheorem.blogspot.com/2008/10/abels-impossibility-proof.html
http://www.latex-community.org/forum/viewtopic.php?f=46&t=5269

Latex :
http://en.wikibooks.org/wiki/LaTeX/Tables
http://web.ift.uib.no/Fysisk/Teori/KURS/TeX/sym1.html
http://newton.ex.ac.uk/research/qsystems/people/sque/symbols/
http://www.artofproblemsolving.com/Wiki/index.php/LaTeX:Symbols
http://www.proofwiki.org/wiki/Symbols:Z
http://www.ctex.org/documents/packages/math/dsdoc.pdf
http://mactex-wiki.tug.org/wiki/index.php?title=Graphics_inclusion
http://termvakt.uio.no/LaTeX
http://godplaysdice.blogspot.com/2009/02/latex-equation-labels.html
http://www.andy-roberts.net/misc/latex/latextutorial10.html
http://w2.syronex.com/jmr/tex/latex-symbols
http://lahelper.sourceforge.net/mini_latex_tutorial.html
http://w2.syronex.com/jmr/tex/texsym.old.html
http://www.maths.tcd.ie/ dwilkins/LaTeXPrimer/WhiteSpace.html
http://www.ursoswald.ch/LaTeXGraphics/picture/picture.html
http://en.wikibooks.org/wiki/LaTeX/Creating_Graphics
http://crab.rutgers.edu/~karel/latex/class3/class3.html
http://en.wikibooks.org/wiki/LaTeX/Bibliography_Management
http://www.complang.tuwien.ac.at/anton/latex/ltx-58.html

Personer

[1] Magnar Dale

Andre kilder

[1] Notater i Grupper og Symmetri.

[2] Tofteby, Tanja. Galois teori. Artikkel.

[3] 92lalgsol6.pdf. Oppgaver og løsninger til Galoisgrupper.

[4] galsol.pdf. Oppgaver og løsninger til Galoisgrupper.

[5] galoisex.pdf. Keith Conrad. SOME EXAMPLES OF THE GALOIS CORRESPONDENCE.

11 Stikkordsregister

Abel, Niels Henrik, 56
Abels bevis, 81
Abels teorem, 82
Abelsk tårn, 79
Addisjon, 19
    modulo n, 19, 20
Algebraisk element, 43
Algebraisk utvidelse, 48
Automorfisme, 40
    gruppe, 40
Avbildning, 18

Bewersdorff, Jörg, 69
Bijektiv, 26

Diskriminant, 83, 84

Eisenstein, 43
Embedding, 39, 49
    utvidelse, 52
Enhet, 37
Eulers phi-funksjon, 62

Faktorisering, 41
Ferrari, Ludovico, 14
Fikskropp, 42, 66
Fundamentalteoremet for Galoisteori, 66
    del I, 66
    del II, 68
    eksempel, 71, 73
Funksjon, 18
Funksjoner
    sammensetning av, 19

Galois, 59
    bevis, 80
    Évariste, 59
    gruppe, 64, 83, 84, 85, 87
    teori, 62

fundamentalteoremet, 66
utvidelse, 62
Generator, 29
Gruppe
abelsk, 22
definisjon, 21
dihedral
D_2, 27
D_3, 30
D_4, 31, 75
eksempel, 24
endelig, 22
homomorfisme, 26
isomorfisme, 26
kvotient, 32
løsbar, 79
permutasjons-, 28
simpel, 31
syklisk, 29
tabell, 23
uendelig, 22
under-, 28
normal, 31

Homomorfisme
gruppe, 26
ring, 38

Identitetselement, 21
Injektiv, 26
Invers, 21, 22
Isomorfisme
gruppe, 26
ring, 38

Kjerne (Kernel), 33
Kosett, 29
høyre, 29
venstre, 29
Kroenecker, Leopold, 91
Kropp

algebraisk lukket, 39
definisjon, 38
fiks, 42, 66
homomorfisme, 38
isomorfisme, 38
mellom, 67
rot, 62
utvidelse, 41, 43
endelig, 48
enkel, 45
grad, 52

Lagrange, 31
Likninger, 8
andre grad, 8
fjerde grad, 15
løsbar, 80
tredje grad, 11
Løsbar
gruppe, 79
polynom, 79
likning, 80

Mengde, 18
del, 28
eksempler, 18
tomme, 18
Minimalpolynom, 44
grad, 44, 48
Multiplikasjon, 19
modulo n, 20

n-te enhetsrot, 29
primitiv, 29
Notasjoner, 18, 24
Nulldivisor, 37

Operasjon
binær, 19
eksempler, 19, 20
Oppsummering

grupper, 35
ring, kropp, 54
galoisteori, 78
løsbarhet ved rottegn, 93

Permutasjoner, 82
Polynom
andregrads, 83
av grad $n \geq 5$, 87
fjerdegrads, 85
irredusible, 42
løsbart, 79
minimal, 44
monisk, 44
tredjegrads, 84
Primitivt element, 53

Radikal utvidelse, 79
enkel, 79
Relativt primiske elementer, 24
Ring
definisjon, 36
homomorfisme, 38
isomorfisme, 38
kommutativ, 36
Rotkropp, 62

Største felles faktor, 24
Surjektiv, 26

Transcendentale element, 43

Undergruppe, 28
Normale, 31

Vektorrom, 47