Forelesninger over

GALOIS-TEORI

AV

KARL EGIL AUBERT

MATEMATISK INSTITUTT
Blindern 1958

75NMO6573

Forelesninger over

Galois-teori

av

Karl Egil Aubert

Matematisk Institutt

Blindern 1958

INNHOLD

§ 1. Grupper

1. Gruppedefinisjonen 1
2. Undergruppe, homomorfi og kvotientgruppe 3
3. Sykliske grupper 6
4. Eksempler på kvotientgrupper 7
5. Grupper med operatorer. Isomorfisatsene 7
6. Satsene til Schreier og Jordan-Hölder for grupper med operatorer 10

§ 2. Kommutative ringer og idealer

7. Ringdefinisjonen 15
8. Ideal, kongruens, restklassering, homomorfi 17
9. Generering av idealer. Snitt og union av idealer 19
10. Primidealer og maksimale idealer 20
11. Hovedidealringer. Euklidske ringer 24
12. Produktoppspaltning i Euklidske ringer 25
13. Polynomringer 27

§ 3. Kropper

14. Kropper, primkropper og kroppers karakteristikk 29
15. Utvidelse av kropper 31
16. Enkle kropputvidelser. Algebraiske og transendente utvidelser 32
17. Utvidelseskropper betraktet som vektorrom over grunnkroppen 37
18. Et par anvendelser på algebraiske tall og konstruksjonsproblemer (kubens fordobling) 39
19. Rotkroppen til en algebraisk likning 42

§ 4. Galois-teori

20. Den Galoiske gruppen til en rotkropp 43
21. Separable og inseparable polynomer 46
22. Rotkropper og Galois-grupper for separable polynomer 48
23. Symmetriske polynomer 51

24. Hovedsatsen i den Galoiske teorien 52
25. Endelige kropper 55
26. Enhetsrötter og sirkeldelingskropper 58
27. Konstruksjon av regulære n-kanter 59
28. Endelige separable utvidelser er enkle 61
29. Galoiske utvidelser og mer om separable og normale utvidelser 63

§ 5. Anvendelser av Galois-teori på algebraiske likninger

30. Problemstilling 67
31. Rene likninger og deres Galois-grupper 68
32. Hovedsatsen om lösbarhet av algebraiske likninger 70
33. Ulösbarheten av den generelle n'te-gradslikning for $n \geq 5$ 74
34. Lösbarhet og ulösbarhet av spesielle algebraiske likninger med rasjonale koeffisienter 77

Forord.

Den Galoiske teorien skulle av flere grunner egne seg utmerket til hovedfagspensum i algebra. Samtidig som den gir en innföring i praktisk talt alle de fundamentale begrepene i algebraen, viser den i höy grad nytten av de innförte begreper ved lösningen av vanskelige konkrete problemer. Vi sikter her först og fremst til lösbarhets-problemer i teorien for algebraiske likninger, men også til problemer i forbindelse med konstruksjoner med passer og linjal. Det finnes i dag ingen annen tilfredsstillende behandling av disse problemer enn ved den abstrakte algebras begrepsdannelse.

Vi har vanligvis ikke tatt med andre ting fra det generelle grunnlaget i algebraen enn det som trengs for å utvikle den Galoiske teorien. Blant unntagelsene er f.eks. den viktige Schreiers sats som vi straks viser et par anvendelser av. Ellers skulle innholds-fortegnelsen gi klar beskjed om innholdet.

K.E. Aubert.

§ 1. Grupper.

1. Gruppedefinisjonen. Studieobjektet i algebraen er först og fremst de såkalte algebraiske strukturer (eller algebraiske systemer). Med en algebraisk struktur forstår en (noe upresist) en mengde E hvori det er definert et visst antall operasjoner som oppfyller visse regneregler (aksiomer). Ettersom vi velger forskjellige aksiomer for de operasjoner vi betrakter får vi forskjellige typer av algebraiske strukturer. Blant de viktigste av disse er grupper, ringer, kropper og vektorrom. Disse spiller alle en fundamental rolle i algebraen spesielt også for den Galoiske teorien. Vi skal her begynne med det mest grunnleggende begrepet, nemlig gruppebegrepet.

La G være en mengde hvori det er definert en binær operasjon. Det vil si at vi til et ordnet par av elementer (a,b); a og $b \in G$ har tilordnet et entydig bestemt element $c \in G$ som vi skriver $c = ab$. Den binære operasjonen som vi her har skrevet som en multiplikasjon er derfor ikke noe annet enn en avbildning av produktmengden $G \times G$ inn i G.[1] Hvis den gitte operasjonen er assosiativ, det vil si $a(bc) = (ab)c$ sier vi at G danner en semigruppe (m.h.p. denne operasjonen). Hvis G i tillegg til å være en semigruppe oppfyller följende aksiomer sier vi at G er en gruppe.

A. Det eksisterer minst ett element $e \in G$ med den egenskap at $ea = a$ for alle $a \in G$ og slik at det til ethvert element $b \in G$ eksisterer minst ett element $b^{-1} \in G$ som oppfyller betingelsen $b^{-1}b = e$.

Vi sier her at e er et venstresidig enhetselement i G og at b^{-1} er en venstreinvers til b (m.h.p. e). Den gruppedefinisjonen vi her har gitt er tilsynelatende "svakere" enn den definisjonen en oftest finner i läreböker.[2] Vanligvis krever en også at e skal være et höyresidig enhetselement som er entydig bestemt og at elementet b^{-1} også skal være en höyre-invers til b, d.v.s. $bb^{-1} = e$. Följende sats viser at disse tingene er en konsekvens av aksiomene ovenfor.

Sats 1. I en gruppe er et venstresidig enhetselement også et höyresidig enhetselement og er entydig bestemt. Videre er en venstresidig invers a^{-1} til a også en höyresidig invers til a og er entydig

1) Når det gjelder enkle mengdeteoretiske definisjoner og betegnelser henviser vi til [2].

2) Formuleringen A er imidlertid identisk med konjunksjonen av betingelsene 3 og 4 i van der Waerdens definisjon [5] side 19.

bestemt.

Bevis: På grunn av assosiativiteten trenger vi ikke å sette parenteser og vi får av aksiom A at $a^{-1}aa^{-1} = ea^{-1} = a^{-1}$. Multipliserer vi denne likningen fra venstre med den venstre-inverse til a^{-1} får vi $aaa^{-1} = e$ eller $aa^{-1} = e$ som viser at a^{-1} også er höyre-invers til a. Av dette følger forövrig at a er den inverse til a^{-1}. Vi får videre at $ae = aa^{-1}a = ea = a$ slik at e også blir et höyre-sidig enhetselement. Om e_1 og e_2 er to enhetselementer får vi $e_1 = e_1 \cdot e_2 = e_2$ som viser at enhetselementet e er entydig bestemt. Endelig viser multiplikasjon fra höyre med a^{-1} i likningen $ba = e$ at den inverse er entydig bestemt.

Følgende sats viser at gruppebegrepet også kan defineres ved lösbarhet av lineære likninger.

Sats 2. En semigruppe G er en gruppe hvis og bare hvis likningene $ax = b$ og $ya = b$ er lösbare i x og y når a og b er faste vilkårlige elementer i G. (Disse likningene får derfor automatisk entydige lösninger.)

Bevis: La G være en gruppe. Da vil de to likningene ha henholdsvis $x = a^{-1}b$ og $y = ba^{-1}$ som lösninger. La omvendt G være en semigruppe hvor de gitte likninger er lösbare. Da vil spesielt likningen $xc = c$ for et gitt $c \in G$ være lösbar. Vi betegner en lösning av denne likningen med e slik at $ec = c$. For et vilkårlig element $a \in G$ kan vi videre finne en x slik at $cx = a$ og det gir $ea = ecx = cx = a$ som viser at e er et venstresidig enhetselement. Resten av betingelsen A er nå en direkte følge av lösbarheten av $xa = e$. Entydigheten av x i $ax = b$ følger ved å multiplisere $ax_1 = ax_2 (= b)$ fra venstre med a^{-1}. På samme måte har $ya = b$ bare en lösning.

Hvis en semigruppe består av et endelig antall elementer sies den å være endelig og vi har en semigruppe med forkortningsregel dersom $ax = bx \Rightarrow a = b$ og $xa = xb \Rightarrow a = b$.

Sats 3. En endelig semigruppe S med forkortningsregel er en gruppe.

Bevis: La $a \in S$ og betrakt avbildningen φ_a definert ved at $\varphi_a(x) = ax$. Forkortningsregelen sier nettopp at φ_a er en-entydig. Siden S er endelig og derfor ikke kan avbildes en-entydig på en ekte del av seg selv må $\varphi_a(S) = S$, men det betyr at for et vilkårlig element $b \in S$ kan vi finne et x slik at $\varphi_a(x) = b$, men dette betyr at $ax = b$ er lösbar. På samme måte blir $xa = b$ lösbar og G

er derfor en gruppe ifölge Sats 2.

En gruppe sies å være kommutativ (eller abelsk) dersom $ab = ba$ for alle $a, b \in G$.

2. Undergruppe, homomorfi og kvotientgruppe. En undermengde H av en gruppe G sies å være en undergruppe av G dersom den danner en gruppe med hensyn på den operasjonen som allerede er definert i G. Forat H skal være en undergruppe av G er åpenbart nödvendig og tilstrekkelig at om a og b hörer til H så gjör også ab og a^{-1} (og b^{-1}) det. For av dette följer at $e = aa^{-1} \in H$. Vi kan slå de to betingelsene sammen og den får da formen $a \in H \,\&\, b \in H \Rightarrow ab^{-1} \in H$. Av dette följer nemlig ved å sette $a = b$ at $a \in H \Rightarrow a \cdot a^{-1} = e \in H$ og av dette igjen $ea^{-1} = a^{-1} \in H$.

Den fundamentale egenskapen ved undergrupper er at de på en naturlig måte bevirker en oppdeling av G i ekvivalensklasser. Vi får forövrig som vi skal se i det ikke-kommutative tilfellet to oppdelinger. La H være en undergruppe av G og la a være et fast element i G. Mengden av alle elementer i G av formen ah hvor $h \in H$ betegner vi med aH og kaller en venstre-restklasse modulo H. Vi påstår nå at to slike mengder aH og bH enten er identiske eller vil ha et tomt snitt. Er nemlig $aH \cap bH \neq \emptyset$ har vi $ah_1 = ah_2$ for passende $h_1, h_2 \in H$. For en vilkårlig $h \in H$ får vi da $ah = bh_2h_1^{-1}h \in bH$ og altså $aH \subseteq bH$. På grunn av symmetrien får vi $aH = bH$. Venstre-restklassene aH danner derfor en oppdeling av G i klasser som par-vis ikke har noe element felles. Den tilsvarende kvotientmengden (se [2]) betegner vi med G/H. Et element i G/H er altså en venstre-restklasse aH. En analog betraktning over mengdene av formen Ha leder til begrepene höyre-restklasse og höyre-kvotientmengde. Det vi forelöpig har vist kan også formuleres på följende måte:

Sats 4. Hvis vi med hensyn på en undergruppe H av G skriver $a \equiv_V b \pmod{H}$ og $a \equiv_h b \pmod{H}$ når henholdsvis $a^{-1}b \in H$ og $ab^{-1} \in H$ vil $\equiv_V$ og $\equiv_h$ definere to ekvivalensrelasjoner i G.

Följende enkle konsekvens av Sats 4 var allerede kjent av Lagrange.

Korollar: Hvis en endelig gruppe med n elementer har en undergruppe med m elementer er m en divisor i n.

Vi er nå interessert i hvilken betingelse H må oppfylle forat de to ekvivalensrelasjonene $\equiv_V$ og $\equiv_h$ også skal være kongruens-

relasjoner, det vil si at vi f.eks. for $\equiv_h$ har at

$x \equiv_h y (\mathrm{mod}\ H)$ medfører $xz \equiv_h yz$ og $zx \equiv_h zy (\mathrm{mod}\ H)$ for alle $z \in G$.

Vi nöyer oss i det følgende med å betrakte relasjonen $\equiv_h$. Behandlingen av $\equiv_v$ er helt analog og förer til nöyaktig samme (symmetriske) betingelse på H. Vi noterer först at $\equiv_h$ automatisk er en kongruensrelasjon med hensyn på multiplikasjon fra höyre side uten å pålegge H noen ekstra betingelse. For $x \equiv_h y \iff xy^{-1} \in H \iff xz(yz)^{-1} \in H$ $\iff xz \equiv_h yz (\mathrm{mod}\ H)$. Anta så at $\equiv_h$ er en kongruensrelasjon m.h.p. multiplikasjon fra venstre. Da følger av $x \in H$, d.v.s. av $x \equiv_h e (\mathrm{mod}\ H)$ at $yxy^{-1} \equiv_h e (\mathrm{mod}\ H)$ eller $yxy^{-1} \in H$. Siden x er vilkårlig valgt i H har vi derfor $yHy^{-1} \subseteq H$ for alle $y \in G$. Ved å erstatte y med y^{-1} får vi $y^{-1}Hy \subseteq H$. Skal $\equiv_h$ være en kongruensrelasjon må derfor H oppfylle betingelsen $yHy^{-1} = H$ (eller den dermed ekvivalente betingelse $yHy^{-1} \subseteq H$) for alle y. En slik undergruppe av G kaller vi en <u>invariant</u> (eller normal) undergruppe. (Dette begrepet ble innfört allerede av Galois.) Er på den annen side H invariant blir $\equiv_h$ også en venstre-kongruens for $x \equiv_h y (\mathrm{mod}\ H)$ betyr at $xy^{-1} \in H$ og $ax(ay)^{-1} = axy^{-1}a^{-1} \in H$. Vi har dermed bevist:

<u>Sats 5. Den nödvendige og tilstrekkelige betingelse for at ekvivalensrelasjonene $\equiv_v$ og $\equiv_h$ definert med hensyn på en undergruppe H skal være kongruensrelasjoner er at H er en invariant undergruppe av G.</u>

Når H er invariant er $yH = Hy$ slik at vi ikke får noen distinksjon mellom höyre- og venstre-restklasser. Vi skal nå se at det ikke finnes andre kongruensrelasjoner i G enn de som fremkommer av invariante undergrupper på den måten som er beskrevet ovenfor. La $\equiv$ være en vilkårlig kongruensrelasjon i G. Da vil for det förste de elementer $x \in G$ som er slik at $x \equiv e$ danne en invariant undergruppe H_e av G. For $x \equiv e$ og $y \equiv e$ medfører $xy \equiv e$; $x \equiv e \Rightarrow xx^{-1} \equiv x^{-1}$ d.v.s. $x^{-1} \equiv e$ og $x \equiv e$ medfører $yxy^{-1} \equiv e$. For det annet vil restklassene modulo H_e falle sammen med restklassene m.h.p. $\equiv$. For $x \equiv y \iff xy^{-1} \equiv e \iff xy^{-1} \in H_e \iff x \equiv y (\mathrm{mod}\ H_e)$. At vi hermed har en en-entydig korrespondanse mellom kongruensrelasjoner og invariante undergrupper i G er klart siden to forskjellige invariante undergrupper gir opphav til to forskjellige kongruensrelasjoner. Vi formulerer dette som

<u>Sats 6. Det finnes ikke andre kongruensrelasjoner i G enn de som fremkommer av invariante undergrupper. Det er derfor en-entydig korrespondanse mellom invariante undergrupper og kongruensrelasjoner i G.</u>

Hvis $\equiv$ er en kongruensrelasjon slik at $a_1 \equiv b_1$ og $a_2 \equiv b_2$ får vi $a_1a_2 \equiv b_1a_2 \equiv b_1b_2$ og altså $a_1a_2 \equiv b_1b_2$. Dette viser at den restklassen som produktet a_1a_2 ligger i ikke endres om vi erstatter a_1 og a_2 med to andre elementer b_1 og b_2 som ligger i de samme restklasser. Med andre ord kan vi entydig definere produktet av de to restklassene som a_1 og a_2 hörer til som den restklassen som produktet a_1a_2 hörer til. Om H er en invariant undergruppe av G kan vi direkte se dette slik: $aH \cdot bH = a(Hb) \cdot H = a(bH) \cdot H = ab \cdot H$. Vi skal vise at den operasjonen vi hermed får definert i kvotientmengden G/H gjör G/H til en gruppe. Dette kan lett sees direkte, men er også en konsekvens av följende to ting: 1) Den kanoniske avbildningen $\varphi : a \to aH$ av G på G/H er en homomorfi og 2) at det homomorfe billedet av en gruppe er en gruppe og at en avbildning f av en gruppe inn i en mengde hvor det er definert en binær operasjon (som vi også skriver som en multiplikasjon) er en <u>homomorfi</u> betyr at $f(ab) = f(a) \cdot f(b)$. At avbildningen φ ovenfor tilfredsstiller denne likningen betyr bare at $abH = aH \cdot bH$ som er selve definisjonen av multiplikasjonen av restklassene. En <u>isomorfi</u> er en homomorfi som er en-entydig.

<u>Sats 7. Det homomorfe billedet av en gruppe er en gruppe.</u>

<u>Bevis</u>: Hvis G er en gruppe og φ er en homomorfi av G inn i en mengde med en binær multiplikasjon er det $\varphi(G) = G'$ som er det homomorfe billedet av G. La $\varphi(x)$, $\varphi(y)$ og $\varphi(z)$ være tre elementer i G'. Av assosiativiteten i G: $x(yz) = (xy)z$ följer $\varphi(x(yz)) = \varphi((xy)z)$ eller $\varphi(x)(\varphi(y) \cdot \varphi(z)) = (\varphi(x)\varphi(y)) \cdot \varphi(z)$ som viser assosiativiteten i G'. Videre vil $\varphi(e)$ være et enhetselement i G' hvis e er enhetselementet i G, for $ex = x$ gir $\varphi(e) \cdot \varphi(x) = \varphi(x)$ hvor $\varphi(x)$ kan velges vilkårlig i G'. Endelig er $\varphi(x^{-1})$ den inverse til $\varphi(x)$ idet $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e)$.

Av at G er en gruppe og at $a \to aH$ er en homomorfi följer dermed at G/H er en gruppe under den restklassemultiplikasjonen vi har definert ovenfor. Omvendt er enhver homomorfi $\varphi : G \to G'$ entydig bestemt ved en invariant undergruppe i G nemlig mengden $\varphi^{-1}(\{e'\}) = H_\varphi$ av de elementer i G som avbildes på enhetselementet e' i G'. $\varphi^{-1}(\{e'\})$ kalles <u>kjernen</u> i homomorfien φ. At $\varphi^{-1}(\{e'\})$ danner en invariant undergruppe i G ser en lett: 1) $\varphi(x) = e'$ og $\varphi(y) = e'$ medförer $\varphi(xy^{-1}) = \varphi(x)(\varphi(y))^{-1} = e'e' = e'$ og 2) $\varphi(x) = e'$ medförer $\varphi(yxy^{-1}) = \varphi(y)e'(\varphi(y))^{-1} = e'$. Videre er φ bestemt av $\varphi^{-1}(\{e'\})$ i den forstand at $\varphi(x) = \varphi(y) \iff \varphi(x)(\varphi(y))^{-1} = e' \iff$

$\Leftrightarrow \varphi(xy^{-1}) = e' \Leftrightarrow xy^{-1} \in \varphi^{-1}(\{e'\}) = H_\varphi$. Dette fører til at korrespondansen $\varphi(a) \leftrightarrow aH_\varphi$ blir en-entydig og det følger umiddelbart av regelen for multiplikasjon av restklasser samt av at φ er en homomorfi at denne korrespondansen gir en isomorfi mellom G' og G/H. Vi har dermed bevist:

Sats 8. Hvis H er en invariant undergruppe av G er den kanoniske avbildningen $G \to G/H$ gitt ved $a \to aH$ en homomorfi med H som kjerne. Omvendt vil enhver homomorfi være av denne typen. For om φ er en homomorfi av G på G' med H_φ som kjerne vil G' og G/H være isomorfe.

3. Sykliske grupper. La A være en vilkårlig undermengde av gruppen G. Snittet av alle de undergrupper av G som inneholder A vil igjen være en undergruppe $H(A)$ av G og $H(A)$ vil tydeligvis være den entydig bestemte minste undergruppe av G som inneholder A. En sier at undermengden A genererer undergruppen $H(A)$. $H(A)$ består nöyaktig av de elementer i G som lar seg skrive som et endelig produkt $a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ hvor $a_i \in A$ og n_i er et helt positivt eller negativt tall. (Om $-n$ er negativ betyr a^{-n} elementet $(a^{-1})^n$ og $a^0 = e$ hvor e er enhetselementet i G.) Spesielt enkelt blir det når A reduserer seg til ett element $A = \{a\}$. Da vil $H(A)$ bestå av mengden av alle positive og negative eksponenter av a. Generelt sier en at en gruppe G som kan genereres utfra ett av sine elementer, altså $G = H(\{a\})$ for passende $a \in G$, er en syklisk gruppe. En syklisk gruppe er alltid kommutativ og det finnes to typer av dem: Hvis $G = H(\{a\})$ er uendelig betyr det at alle potensene a^n er forskjellige og G blir isomorf med den additive gruppen Z av de hele rasjonale tall. Hvis G er endelig er den av formen $G = \{e, a, a^2, \ldots, a^{m-1}\}$ hvor n er det minste hele tall slik at $a^n = e$. Denne gruppen er isomorf med restklassegruppen modulo m beskrevet i eksempel 1 nedenfor. En liten sats som vi får bruk for senere er følgende:

Sats 9. En undergruppe av en syklisk gruppe er selv syklisk.

Bevis: La G være en syklisk gruppe med generator a og H en undergruppe av G. La videre p være det minste hele tall > 0 slik at $a^p \in H$. Vi påstår at a^p genererer H. Anta at $b = a^n \in H$. Vi kan tydeligvis anta at $n > 0$ (for om a^n er en positiv potens av a^p - slik som vi skal se er tilfellet - så vil a^{-n} være lik den tilsvarende negative potens av a^p). Vi skriver $n = qp+r$ med $0 \leq r < p$

og får $a^n = (a^p)^q \cdot a^r$ eller $a^r = a^n(a^{-p})^q \in H$ siden a^{-p} og $a^n \in H$. På grunn av minimalegenskapen til p er derfor $r = 0$ og $a^n = (a^p)^q$.

4. Eksempler på kvotientgrupper. 1) La Z betegne gruppen av de hele rasjonale tall med addisjon som gruppeoperasjon og la m være et helt tall > 0. Den uendelige sykliske gruppen $(m) = mZ$ generert av m består av alle hele positive og negative multipla av m. Undergruppen mZ leder til en kongruensrelasjon $a \equiv b \pmod{mZ}$ i Z som ikke er noe annet enn den vanlige tallteoretiske kongruensrelasjonen som vi skriver $a \equiv b \pmod{m}$. For $a \equiv b \pmod{mZ}$ betyr jo at $a - b \in mZ$, d.v.s. $m \mid (a - b)$. Kvotientgruppen Z/mZ kan på vanlig måte representeres ved tallene $0, 1, 2, \ldots, m-1$ hvor en adderer dem modulo m. Denne endelige sykliske gruppen generert av 1 er restklassegruppen modulo m.

2) La så C^* betegne gruppen av de komplekse tall $\neq 0$ med multiplikasjon som gruppeoperasjon. C^* har spesielt to viktige undergrupper - nemlig gruppen R_+^* bestående av de reelle tall > 0 og gruppen T bestående av de komplekse tall med tallverdi lik 1. La oss først se på kongruensen $a \equiv b \pmod{R_+^*}$. : $ab^{-1} \in R_+^*$. Siden ethvert komplekst tall kan skrives entydig på formen $re^{i\varphi}$ med $r > 0$, $0 \leq \varphi < 2\pi$ får vi hvis vi setter $a = r_1 \cdot e^{i\varphi_1}$ og $b = r_2 e^{i\varphi_2}$ at $ab^{-1} = \frac{r_1}{r_2} e^{i(\varphi_1 - \varphi_2)}$. Vi får derfor $a \equiv b \pmod{R_+^*}$ hvis og bare hvis $\varphi_1 = \varphi_2$. Hver restklasse i C^* modulo R_+^* består med andre ord av en rett linje i det komplekse plan som stråler ut fra origo. Vi ser umiddelbart at $C^*/R_+^* \cong T$. Hvis vi på den annen side betrakter kongruensen modulo T får vi $ab^{-1} = \frac{r_1}{r_2} e^{i(\varphi_1 - \varphi_2)} \in T$ hvis og bare hvis $r_1 = r_2$. Restklassene modulo T er med andre ord dannet av sirkler omkring origo. Her får vi $C^*/T = R_+^*$. Om R som vanlig betegner den additive gruppen av de reelle tall og $2\pi Z$ er undergruppen av de hele pos. og neg. multipla av 2π vil tydeligvis (den multiplikative gruppen) T igjen være isomorf med den additive gruppen $R/2\pi Z$.

5. Grupper med operatorer. Isomorfisatsene. Mange satser i gruppeteorien kan gis en mer generell formulering ved å anvende begrepet "gruppe med operatorer" og dette har stor betydning for mange anvendelser.

La G være en gruppe og Ω en mengde av elementer som virker som

operatorer i G i den forstand at det til $\alpha \in \Omega$ og $g \in G$ svarer et entydig bestemt element $\alpha g \in G$. G sies å være en gruppe med operatorer (Ω) hvis elementene i Ω på denne måten virker som endomorfismer i G, d.v.s. $\alpha(g + h) = \alpha g + \alpha h$ for $\alpha \in \Omega$, g, $h \in G$. En undergruppe H av G sies å være en Ω-undergruppe hvis $\alpha h \in H$ hvergang $\alpha \in \Omega$ og $h \in H$.

Eksempler. 1) Hvis a er et fast element i G vil avbildningen $x \to axa^{-1}$ være en automorfisme d.v.s. en isomorfi av G på seg selv. Automorfismer som er av denne form kalles indre automorfismer. G er derfor en gruppe med operatorer om en setter Ω lik mengden av de indre automorfismer. Ω-undergruppene faller her sammen med de invariante undergruppene i G.

2) Et vektorrom kan oppfattes som en gruppe med operatorer hvor G er den underliggende additive gruppen og Ω er skalarkroppen. Ω-undergruppene er her undervektorrommene.

3) Den additive gruppen i en ring R (se kapitlet om ringer) kan oppfattes som en gruppe med operatorer hvor Ω identifiseres med R og "virkningen" av operatoren $r \in R$ på elementet $g \in R(+)$ er vanlig ringmultiplikasjon r·g. Er f.eks. R kommutativ blir Ω-undergruppene i R(+) identisk med idealene i R. Vi viser nå den enkle

Sats 10. Den nödvendige og tilstrekkelige betingelse for at ekvivalensrelasjonen $\equiv$ ($\equiv_h$ eller $\equiv_v$) indusert av en undergruppe H av G skal være en kongruensrelasjon m.h.p. Ω d.v.s. $a \equiv b \pmod H \Rightarrow \alpha a \equiv \alpha b \pmod H$ for $\alpha \in \Omega$ er at H er en Ω-undergruppe.

Bevis: Vi bemerker först at om $\alpha \in \Omega$ så er $\alpha a = \alpha a \cdot e = \alpha a \cdot \alpha e$ d.v.s. $\alpha e = e$. Anta så at $\equiv$ er en kongruens m.h.p. Ω og at $a \in H$. Da vil $a \equiv e \pmod H$ og dermed $\alpha a \equiv \alpha e \equiv e \pmod H$ som viser at $\alpha a \in H$. Er omvendt H en Ω-undergruppe följer av $a \equiv b \pmod H$ at $ab^{-1} \in H$ som gir $\alpha(ab^{-1}) = \alpha a \cdot \alpha(b^{-1}) = \alpha a \cdot (\alpha b)^{-1} \in H$, og dette betyr at $\alpha a \equiv \alpha b \pmod H$.

Denne satsen viser at om H er en invariant undergruppe kan kvotientgruppen G/H på en naturlig måte betraktes som en gruppe med operatorområde Ω dersom H er en Ω-undergruppe. For da kan vi definere $\alpha(aH) = (\alpha a) \cdot H$ eller om vi betegner den kanoniske homomorfien av G på G/H med φ : $\alpha(\varphi(a)) = \varphi(\alpha a)$. Denne likningen uttrykker som en ser at φ kommuterer med alle operatorene $\alpha \in \Omega$. At

elementene i Ω dermed opererer som endomorfismer i G/H følger av $\alpha(\varphi(a)\cdot\varphi(b)) = \alpha(\varphi(ab)) = \varphi(\alpha(ab)) = \varphi(\alpha(a)\cdot\alpha(b)) = \varphi(\alpha a)\cdot\varphi(\alpha b) = \alpha(\varphi(a))\cdot\alpha(\varphi(b))$.

Når vi sammenlikner grupper med operatorer (f.eks. med hensyn på isomorfi) betrakter vi alltid grupper med samme operatorområde Ω. Vi kaller da en homomorfi φ en Ω-homomorfi hvis vi har $\alpha(\varphi(a)) = \varphi(\alpha a)$. Hvis φ dessuten er en-entydig kaller vi den en Ω-isomorfi. I følge det som er sagt ovenfor vil derfor hvis H er en invariant Ω-undergruppe av G den kanoniske homomorfien $G \to G/H$ være en Ω-homomorfi. Omvendt hvis $G \to G'$ er en Ω-homomorfi av G på G' vil kjernen H foruten som för å være invariant også være en Ω-undergruppe. For om $\varphi(a) = e'$ vil også $\varphi(\alpha a) = \alpha(\varphi(a)) = \alpha e' = e'$. Endelig er det klart at korrespondansen $aH \leftrightarrow \varphi(a)$ etablerer en Ω-isomorfi mellom G/H og G'. Vi har derfor följende utvidelse av Sats 8

Sats 11. (Den fundamentale homomorfisatsen for grupper med operatorer.) La G være en gruppe med operatorområde Ω og H en invariant Ω-undergruppe av G. Da er avbildningen $G \to G/H$ en Ω-homomorfi. Omvendt hvis φ er en Ω-homomorfi av G på G' vil kjernen i denne homomorfien være en invariant Ω-undergruppe H_φ av G og G' er Ω-isomorf med G/H_φ.

Vi skal så bevise de to isomorfisatsene.

Sats 12. (Förste isomorfisats.) La G være en gruppe med operatorområde Ω hvor H og N er to invariante Ω-undergrupper slik at $N \subseteq H$. Da er G/H og $\frac{G/N}{H/N}$ Ω-isomorfe.

Bevis: En ser for det förste lett at H/N er en invariant undergruppe av G/N. Om vi betrakter Ω-homomorfiene $\varphi_1: G \to G/N$ og $\varphi_2: G/N \to \frac{G/N}{H/N}$ vil sammensettingen av φ_1 og φ_2 gi en Ω-homomorfi av G på $\frac{G/N}{H/N}$. Siden kjernen i denne sammensatte homomorfien tydeligvis er H följer satsen direkte av Sats 11.

Sats 13. (Annen isomorfisats.) La G være en gruppe med operatorområde Ω hvor H er en Ω-undergruppe og N en invariant Ω-undergruppe. Da er $H \cap N$ en invariant Ω-undergruppe av H og gruppene $H \cup N/N$ og $H/H \cap N$ er Ω-isomorfe.

Bevis: Her betyr $H\cdot N$ som vanlig mengden av alle produkter $h\cdot n$ hvor $h \in H$ og $n \in N$. $H\cdot N$ er den minste Ω-undergruppe av G som inne-

holder H og N. La så $x \in H$ og $a \in H \cap N$. Da blir $xax^{-1} \in H$ fordi H er en undergruppe og $xax^{-1} \in N$ fordi N er invariant i G og derfor også i H. Altså $xax^{-1} \in H \cap N$ og $H \cap N$ er invariant i H. La så den kanoniske homomorfien $G \to G/N$ betegnes med φ. Nå er $\varphi(H \cdot N) = \varphi(H)$ en Ω-undergruppe $\bar{H}$ av G/N og vi får at φ induserer to homomorfier av Ω-undergruppene HN og H inn på $\bar{H}$. De respektive kjerner er henholdsvis N og $H \cap N$ slik at vi etter Sats 11 får de to Ω-isomorfiene $HN/N \cong \bar{H}$ og $H/H \cap N \cong \bar{H}$. Vi har derfor også $HN/N \cong H/H \cap N$.

6. Satsene til Schreier og Jordan-Hölder for grupper med operatorer.

Vi innförer först noen begreper. La G være en gruppe med operatorområde Ω. En endelig rekke av Ω-undergrupper av G slik at

(1) $$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = \{e\}$$

kaller vi en normalrekke hvis enhver G_i er invariant Ω-undergruppe av G_{i-1}. Kvotientgruppene G_{i-1}/G_i kalles normalrekkens faktorer. En annen normalrekke

(2) $$G \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n = \{e\}$$

kalles en utvidelse av (1) dersom alle G_i i (1) også opptrer i (2). I en generell normalrekke utelukker vi ikke den mulighet at et ledd kan forekomme flere ganger altså $G_i = G_{i+1}$. Hvis alle G_i er forskjellige snakker vi om en normalrekke uten gjentagelse. En normalrekke uten gjentagelser som ikke tillater noen utvidelse uten gjentagelser bortsett fra den selv kaller vi en komposisjonsrekke. Det er tydelig at en normalrekke uten gjentagelser er en komposisjonsrekke hvis og bare hvis hver faktor G_{i-1}/G_i er en enkel gruppe i den forstand at den ikke inneholder andre undergrupper enn seg selv og undergruppen som reduserer seg til enhetselementet alene. (En konstaterer nemlig lett at Ω-undergruppene i G/H er i en-entydig korrespondanse med de Ω-undergrupper av G som inneholder Ω-undergruppen H.) Vi sier at to normalrekker er isomorfe (eller ekvivalente) hvis vi kan finne en en-entydig korrespondanse mellom de to rekkers faktorer slik at korresponderende faktorer er Ω-isomorfe. Vi bruker her det vanlige isomorfitegnet og det er tydelig at isomorfi mellom normalrekker er en ekvivalensrelasjon. Vi understreker at denne korrespondansen ikke behöver å bevare faktorenes rekkefölge. Generelt vil vi ha hvis (1) og (2) var isomorfe at $G_{i-1}/G_i = H_{j-1}/H_j$ med $i \neq j$.

Ved beviset for Schreiers sats vil vi få bruk for följende

Lemma. Hvis $G \supseteq G_1 \supseteq \ldots \supseteq G_m = \{e\}$ og $G \supseteq H_1 \supseteq \ldots \supseteq H_n = \{e\}$ er to isomorfe normalrekker så kan man til enhver utvidelse av den förste rekken finne en dertil isomorf utvidelse av den andre rekken.

Bevis: La oss anta at den förste rekken er blitt utvidet slik at avsnittet mellom G_i og G_{i+1} etter utvidelsen ser slik ut

$$G_i \supseteq G_{i,1} \supseteq G_{i,2} \supseteq G_{i,k} = G_{i+1} \tag{3}$$

Etter den förste isomorfisatsen (Sats 12) har denne rekken faktorer som er parvis Ω-isomorfe med rekken

$$G_i/G_{i+1} \supseteq G_{i,1}/G_{i+1} \supseteq \ldots \supseteq G_{i,k}/G_{i+1} = \{e\} \tag{4}$$

Etter antagelsen vet vi nå at G_i/G_{i+1} er Ω-isomorf med en passende faktor H_j/H_{j+1} i den andre rekken. H_j/H_{j+1} tillater derfor en normalrekke

$$H_j/H_{j+1} \supseteq H_{j,1}/H_{j+1} \supseteq \ldots \supseteq H_{j+1}/H_{j+1} = \{e\}$$

fullstendig identisk med (3), d.v.s. $H_{j,t}/H_{j+1} \simeq G_{i,t}/G_{i+1}$ for $1 \leq t \leq k$. Av denne får vi nå en normalrekke med parvis samme faktorer (igjen etter 1.isomorfisats).

$$H_j \supseteq H_{j,1} \supseteq \ldots \supseteq H_{j,k} = \{e\}$$

som da også må være isomorf (her til og med når det gjelder faktorenes rekkefölge) med (3). Dermed er lemmaet bevist.

Sats 14. (Schreiers sats). Hvis N_1 og N_2 er to normalrekker i G kan vi finne to utvidelser av henholdsvis N_1 og N_2 som er isomorfe.

Bevis: La de to gitte rekkene være

$$N_1 = \{G \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = \{e\}\}$$

og

$$N_2 = \{G \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n = \{e\}\}$$

Vi skal före et induksjonsbevis på följende måte: Satsen er tydeligvis riktig for tilfellene $m = n = 1$ og $m = 1, n = 2$. Vi beviser den så for $n = 2$ og vilkårlig m ved induksjon med hensyn på m. Dernest for vilkårlig n (og m) ved ny induksjon med hensyn på n.

For $n = 2$ kan vi skrive N_2 på formen $G \supseteq H \supseteq E = \{e\}$ og vi innförer Ω-undergruppene $D = G_1 \cap H$ og $F = G_1 \cup H = G_1 \cdot H$. For de normalrekkene vi skal danne nedenfor er det her först nödvendig å

konstatere at $G_1 \cap H$ er en normal Ω-undergruppe av både G_1 og H (det har vi allerede gjort i beviset for Sats 13), at G_1 og H er normale undergrupper av F (siden de jo er normale i hele G) samt at F er normal i G. Det siste ser vi slik $xG_1Hx^{-1} = (xG_1x^{-1})(xHx^{-1}) \subseteq G_1H$ siden G_1 og H hver for seg er normale Ω-undergrupper av G.

Etter induksjonsantagelsen har nå rekkene av lengde m-1 og 2

$$\{G_1 \supseteq G_2 = \dots \supseteq G_m = E\} \text{ og } \{G_1 \supseteq D \supseteq E\}$$

isomorfe utvidelser

(1) $$\{G_1 \supseteq \dots \supseteq G_2 \supseteq \dots \supseteq G_m = E\} \simeq \{G_1 \supseteq \dots \supseteq D \supseteq \dots \supseteq E\}.$$

På grunn av annen isomorfisats er nå $F/H \simeq G_1/D$ og $F/G_1 \simeq H/D$ og derfor

(2) $$\{F \supseteq G_1 \supseteq D \supseteq E\} \simeq \{F \supseteq H \supseteq D \supseteq E\}$$

Om vi i (1) på begge sider föyer til F som förste ledd vedblir isomorfien å holde og höyre side vil da representere en utvidelse av venstre side av (2). Etter lemmaet ovenfor kan vi da finne en utvidelse av höyre-siden i (2) som er isomorf med höyre-siden i (1) (når vi der har tilföyet F). Altså:

(3) $$\{F \supseteq G_1 \supseteq \dots \supseteq D \supseteq \dots \supseteq E\} \simeq \{F \supseteq \dots \supseteq H \supseteq \dots \supseteq D \supseteq \dots \supseteq E\}.$$

Siden isomorfien i (1) bevares ved å föye til G og F og isomorfien i (3) bevares ved å föye til G får vi ved å sammenlikne (1) og (3) isomorfien

$$\{G \supseteq F \supseteq G_1 \supseteq \dots \supseteq G_2 \supseteq \dots \supseteq G_m = E\} \simeq \{G \supseteq F \supseteq \dots \supseteq H \supseteq \dots$$

$$\dots \supseteq D \supseteq \dots \supseteq E\}$$

Schreiers sats er dermed bevist ved induksjon for det spesielle tilfellet at $n = 2$ (m er vilkårlig). Vi antar så at den holder for n-1 og vilkårlig m og skal så vise at den holder for n og m. Siden den er bevist for $n = 2$ har spesielt rekkene N_1 og rekken $G \supseteq H_1 \supseteq E$ isomorfe utvidelser

(4) $$\{G \supseteq \dots \supseteq G_1 \supseteq \dots \supseteq G_2 \supseteq \dots \supseteq E\} \simeq \{G \supseteq \dots \supseteq H_1 \supseteq \dots \supseteq E\}$$

Siden rekken

(5) $$\{H_1 \supseteq H_2 \supseteq \dots \supseteq H_n = E\}$$

har (n-1) ledd kan vi etter induksjonsantagelsen finne isomorfe ut-

videlser til (5) og den delen av höyresiden av (4) som begynner med H_1. Dette gir da en utvidelse av höyresiden av (4) som har formen $\{G \supseteq \dots \supseteq H_1 \supseteq \dots \supseteq H_2 \supseteq \dots \supseteq H_3 \supseteq \dots \supseteq E\}$. Videre får vi da igjen ved å bruke lemmaet en dertil isomorf utvidelse av venstre siden av (4) slik at

$$(6)\quad \{G \supseteq \dots \supseteq G_1 \supseteq \dots \supseteq G_2 \supseteq \dots \supseteq E\} \simeq \{G \supseteq \dots \supseteq H_1 \supseteq \dots \supseteq H_2 \supseteq \dots \supseteq E\}$$

som viser at Schreiers sats gjelder for vilkårlig m og n.

Hvis det skulle finnes gjentagelser i (6) f.eks. på venstresiden slik at $G_i = G_{i+1}$ for en eller annen i så vil $G_i/G_{i+1} = E$ og vi vil også ha $H_j/H_{j+1} = E$ eller $H_j = H_{j+1}$ for en passende j. Gjentagelsene på venstre side må forekomme like ofte som på höyre side og om vi stryker dem på begge sider (d.v.s. om G_i forekommer k ganger stryker vi k-1 av dem) vil vi på begge sider i (6) få normalrekker uten gjentagelser. Vi får tydeligvis av dette at to normalrekker uten gjentagelser alltid har isomorfe utvidelser uten gjentagelser. Av dette följer nå som

Korollar 1. (Jordan-Hölders sats) To komposisjonsrekker i G er alltid isomorfe. Siden to komposisjonsrekker ikke tillater andre utvidelser uten gjentagelser enn seg selv må de etter Schreiers sats være isomorfe.

Dette korollaret uttaler ikke noe om eksistensen av komposisjonsrekker. Meningen er bare den at om to slike eksisterer er de isomorfe. Vi noterer også följende

Korollar 2. Hvis G har en komposisjonsrekke lar enhver normalrekke uten gjentagelser seg utvide til en komposisjonsrekke. Spesielt hvis H er en vilkårlig invariant Ω-undergruppe av G finnes det da en komposisjonsrekke som inneholder H som ledd.

Vi kaller en gruppe opplösbar hvis den har en normalrekke hvor alle faktorgruppene G_{i-1}/G_i er abelske. Hvis G/H er abelsk og N er en annen invariant Ω-undergruppe av G slik at $H \subseteq N \subseteq G$ vil også faktorgruppene N/H og G/N være abelske. At den förste er abelsk er klart siden den er en undergruppe av G/H. At den andre er abelsk följer av at N kan skrives som en union av restklasser modulo H : $N = \bigcup a_i H$ og vi får da for to elementer aN og bN i G/N : $aN \cdot bN = aH \cdot \bigcup a_i H \cdot bH \bigcup a_i H$; her er alle opptredende faktorer elementer i G/H og kan permuteres som vi vil. Ved å bruke distributiviteten av multiplikasjonen m.h.p. unionen ser en lett at dette uttrykket

også er lik $bN \cdot aN$. Av dette følger nå

Korollar 3. Har en opplösbar gruppe G en komposisjonsrekke så er alle faktorgruppene i en slik enkle abelske grupper. Hvis G er endelig er faktorgruppene sykliske grupper med primtallsorden.

Den siste delen følger av at en endelig abelsk gruppe G uten andre undergrupper enn seg selv og $\{e\}$ må være en syklisk gruppe av primtallorden. For om G er av orden $n \geq 2$ og a et element i G forskjellig fra e må undergruppen generert av a uttömme hele G. Altså $G = \{e, a, a^2, \ldots a^{n-1}\}$ hvor n er det minste naturlige tall slik at $a^n = e$. Var $n = n_1 n_2$ med $1 < n_1 < n$ ville mengden $\{e, a^{n_2}, a^{2n_2}, \ldots a^{(n_1-1)n_2}\}$ danne en ekte undergruppe av G imot forutsetningen.

Av dette får vi nå videre

Korollar 4. Ethvert helt positivt tall lar seg entydig spalte i et produkt av (positive) primtall.

Bevis: La n være et naturlig tall. Eksistensen av minst en primtall-oppspalting $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ er opplagt. La så G være den sykliske gruppen av orden n generert av elementet a og p_1 et primtall som går opp i n ; $n = n_1 \cdot p_1$. Da vil elementet a^{p_1} generere en syklisk undergruppe G_1 av G med orden n_1; $G_1 = \{e, a^{p_1} \ldots a^{(n_1-1)p_1}\}$. G/G_1 blir av ordenen $\frac{n}{n_1} = p_1$. Vi foretar et liknende resonement på G_1 og får en ny undergruppe G_2 av G_1 av ordenen $n_2 = \frac{n}{p_1 \cdot p_2}$ slik at G_1/G_2 er av ordenen p_2. På denne måten får vi at det til enhver oppspaltning $n = p_1 p_2 \cdots p_j$ blir tilordnet en komposisjonsrekke

$$G \supset G_1 \supset \ldots \supset G_j = E$$

hvor alle kvotienter G_{i+1}/G_i har primtallorden og nettopp utgjör primfaktorene i en oppspaltning av n. Jordan-Hölders sats (Korollar 1) gir da umiddelbart entydigheten av denne oppspaltningen.

For det siste korollaret skal vi gi et par definisjoner. Et vektorrom over en kropp K er en abelsk gruppe skrevet additivt med et operatorområde Ω som er en kropp K og slik at om $\alpha, \beta \in K$ så er $(\alpha\beta)a = \alpha(\beta a)$ og $1 \cdot a = a$ når 1 er enhetselementet i K. Begrepet vektorrom er altså et spesialtilfelle av begrepet gruppe med operatorer. Om V er et vektorrom sier vi at en undermengde B av V er en basis for V dersom 1) elementene i B er lineært uavhengige (over K) 2) B genererer V, d.v.s. V er det minste vektorrommet som inneholder

B. Hvis V har en basis B som består av et endelig antall elementer sier vi at V er endelig-dimensjonalt. Det følgende korollaret viser at dette tallet er en invariant karakteristisk for selve vektorrommet.

Korollar 5. To basiser for et og samme endelig-dimensjonale vektorrom inneholder like mange elementer.

Bevis: La $\{x_1 \dots x_n\}$ være en basis for V. Denne basisen gir opphav til følgende komposisjonsrekke for V

$$V = [x_1 \dots x_n] \supset [x_1 \dots x_{n-1}] \supset \dots \supset [x_1, x_2] \supset [x_1] \supset \{0\}.$$

At dette virkelig er en komposisjonsrekke for V følger slik: Var $[x_1 \dots x_{i-1}] \subset U \subseteq [x_1 \dots x_i]$ vil et $x \in U - [x_1 \dots x_{i-1}]$ være av formen $x = \sum_{j=1}^{i} \alpha_j x_j$ hvor $\alpha_i \neq 0$. Da må også $x - \sum_{j=1}^{i-1} \alpha_j x_j = \alpha_i x_i \in U$ og $x_i \in U$, d.v.s. $U = [x_1 \dots x_i]$. Invariansen av tallet n følger nå direkte av Jordan-Hölders sats.

§ 2. Kommutative ringer og idealer.

7. Ringdefinisjonen. Vi skal nå gå over til å behandle et annet fundamentalt algebraisk begrep - nemlig ringbegrepet. I en gruppe hadde vi bare en operasjon som vi skrev som en multiplikasjon. Nå skal vi betrakte algebraiske systemer R hvor det er definert to operasjoner ($\supset$: to avbildninger av $R \times R$ inn i R). Vi skal skrive de to operasjonene som $\cdot$ og $+$ og betegner dem som multiplikasjon og addisjon. Vi definerer: En ring er en mengde R hvori det er definert to operasjoner - addisjon og multiplikasjon - slik at R danner en abelsk ($\supset$: kommutativ) gruppe m.h.p. addisjonen, multiplikasjonen er assosiativ: $a(bc) = (ab)c$ og addisjonen og multiplikasjonen er bundet sammen ved de to distributive lovene $a(b+c) = ab+ac$ og $(b+c)a = ba+ca$.

Skjematisk ser derfor aksiomsystemet for en ring slik ut

1. $a+b = b+a$
2. $a+(b+c) = (a+b)+c$
3. $a+0 = a$
4. $a+(-a) = 0$
5. $a(bc) = (ab)c$
6. $a(b+c) = ab+ac$, $(b+c)a = ba+ca$.

Vi noterer oss med en gang at $a \cdot 0 = 0$ for alle $a \in R$ for på grunn av 6 er $a \cdot 0 = a(b-b) = ab-ab = 0$.

Ved det generelle ringbegrepet forutsetter en altså ikke at multiplikasjonen er kommutativ.. I det fölgende skal vi imidlertid gjöre denne forutsetningen slik at vi bare betrakter kommutative ringer. Andre viktige typer av ringer er ring med enhetselement, integritetsområde og kropp. Vi sier at den kommutative ringen R har et enhetselement e dersom $ea = a$ for alle $a \in R$. Vi vil betegne mengden av elementer forskjellig fra 0-elementet i R med $R^* = R-\{0\}$. En viktig type av ringer er de som har enhetselement og hvor R^* er lukket under multiplikasjonen i R, d.v.s. hvor $a \neq 0 \ \& \ b \neq 0 \Rightarrow ab \neq 0$. Disse ringer kalles integritetsområder. Den gitte betingelse sier at nullelementet ikke kan skrives som et produkt av to elementer som begge er forskjellig fra 0. Vi sier derfor også at et integritetsområde er en kommutativ ring med enhetselement og uten nulldivisorer. Vi har fölgende lille sats som gir en annen karakterisering av integritetsområdene.

Sats 15. En kommutativ ring R med enhetselement er et integritetsområde hvis og bare hvis den tilfredsstiller forkortningsregelen $a \cdot b = ac \Rightarrow b=c$ for enhver $a \neq 0$.

Bevis: Anta at I er et integritetsområde d:: ikke har nulldivisorer og at $ab = ac$ d.v.s. $ab-ac = 0$ eller $a(b-c) = 0$ (etter aksiom 6). Siden $a \neq 0$ og vi ikke har nulldivisorer må $b-c = 0$ d.v.s. $b = c$. Anta omvendt $a \neq 0$, $ab = 0$ og forkortningsregelen. Da gir $ab = 0 = a0$ ved forkortning med a at $b = 0$.

Vi merker oss altså at om R^* er multiplikativ semigruppe (d:: lukket under multiplikasjon) så er den også automatisk en semigruppe med forkortningsregel.

Hvis ikke R^* bare danner en ikke-tom multiplikativ semigruppe (med forkortninsregel), men også en gruppe sier vi at R er en kropp. Etter hva vi beviste helt til å begynne med om grupper er det ekvivalent å si at R er en kropp om divisjon i R alltid er utförbar, altså at likningen $ax = b$ for $a \neq 0$ og b vilkårlig alltid har en lösning. Etter hva vi så får da ringen automatisk et multiplikativt enhetselement.

Eksempler. Vi skal her bare nevne noen eksempler i fleng. Nöyere behandling av flere viktige eksempler vil bli gitt i tilknytning til behandlingen av idealbegrepet nedenfor. 1) Ringen Z av de hele

rasjonale tall under vanlig addisjon og multiplikasjon. 2) Ringene av henholdsvis rasjonale, reelle og komplekse tall under samme operasjoner. 3) Ringen av alle n-n-matriser under vanlige matriseaddisjon og matrisemultiplikasjon. 4) Ringene av alle kontinuerlige, henholdsvis begrensede reelle (eller komplekse funksjoner med et vilkårlig topologisk rom som argumentområde. 5) Ringen av alle undermengder av en gitt mengde hvor multiplikasjonen er snitt-operasjonen og addisjonen er operasjonen symmetrisk differens $A-B = (A \cup B)-(A \cap B)$.

8. Ideal, kongruens, restklassering, homomorfi. En kan ledes til idealbegrepet på nöyaktig samme måte som en ble ledet til begrepet invariant undergruppe i gruppeteorien, nemlig ved å undersöke når den ekvivalensrelasjonen $a \equiv b \pmod{H}$ som induseres av en additiv undergruppe i den additive gruppe i ringen også er en kongruensrelasjon m.h.p. multiplikasjon. Det vil si for hvilke undergrupper H av $R(+)$ $a \equiv b \Rightarrow ac \equiv bc$. At dette er en kongruens m.h.p. addisjon har vi jo allerede vist idet enhver undergruppe av den kommutative gruppen $R(+)$ er invariant. Dette er imidlertid ikke den historiske opprinnelsen til idealbegrepet som först oppsto i teorien for de hele algebraiske tall i tilknytning til problemet om entydig oppspaltning i primfaktorer.. Innföringen av idealbegrepet blir her först og fremst motivert ved den följende Sats 16.

Definisjon. Med et ideal i en ring R forstår vi en undermengde $\mathcal{A}$ av R som er en undergruppe av R's additive gruppe og er slik at om $a \in \mathcal{A}$ og $r \in R$ så er $ar \in \mathcal{A}$. Eksempler på idealer vil bli gitt etter at vi har bevist endel grunnleggende satser om dem.

Sats 16. Den ekvivalensrelasjonen $\equiv_{\mathcal{A}}$ som bestemmes av en additiv undergruppe $\mathcal{A}$ av $R(+)$ er en kongruensrelasjon m.h.p. multiplikasjonen hvis og bare hvis $\mathcal{A}$ er et ideal i R. Avbildningen $\mathcal{A} \longrightarrow \equiv_{\mathcal{A}}$ gir en en-entydig korrespondanse mellom idealene i R og mengden av alle kongruensrelasjoner i R (kongruenser m.h.p. både addisjon og multiplikasjon).

Bevis: La $\mathcal{A}$ være et ideal i R og la $a \equiv b \pmod{\mathcal{A}}$, $\Rightarrow$: $a-b \in \mathcal{A}$. Den multiplikative idealegenskapen gir da $r(a-b) \in \mathcal{A}$ for vilkårlig $r \in R$. Av distributivitetsaksiomet följer $ra-rb \in \mathcal{A}$ som betyr $ra \equiv rb \pmod{\mathcal{A}}$. Anta omvendt at $\equiv_{\mathcal{A}}$ er en multiplikativ kongruensrelasjon. Da följer av $a \in \mathcal{A}$ som betyr $a \equiv 0 \pmod{\mathcal{A}}$ at $ra \equiv r \cdot 0 \equiv 0 \pmod{\mathcal{A}}$ $\Rightarrow$: $ra \in \mathcal{A}$ og $\mathcal{A}$ er et ideal. - Förste del

av beviset ovenfor viser at avbildningen $\mathfrak{a} \to \equiv_{\mathfrak{a}}$ er en avbildning av mengden av alle idealer i R inn i mengden av alle kongruensrelasjoner. For å få frem siste del av satsen gjenstår det derfor å vise to ting: 1) At denne avbildningen er entydig ↔: to forskjellige idealer i R gir opphav til to forskjellige kongruensrelasjoner. 2) At avbildningen er på mengden av alle kongruensrelasjoner i R ↔: at enhver kongruensrelasjon i R har formen $\equiv_{\mathfrak{a}}$ hvor $\mathfrak{a}$ er et ideal i R. 1) er opplagt idet om $\mathfrak{a}_1 \neq \mathfrak{a}_2$ har vi et element a slik at $a \in \mathfrak{a}_1$ men $a \notin \mathfrak{a}_2$ og da blir $a \equiv 0 (\mathfrak{a}_1)$ mens $a \not\equiv 0 (\mathfrak{a}_2)$ som viser at $\equiv_{\mathfrak{a}_1} \neq \equiv_{\mathfrak{a}_2}$. For å vise 2) anta at $\sim$ er en vilkårlig kongruensrelasjon (m.h.p. både $\cdot$ og +) i R. Den klassen m.h.p. $\sim$ som inneholder 0 er da et ideal $\mathfrak{a}$ i R. For av kongruensegenskapene til $\sim$ følger at av $a \sim 0$ følger $0+(-a) \sim a+(-a)$ ↔: $-a \sim 0$ og $a \sim 0$ & $b \sim 0 \Rightarrow a+b \sim 0$ samt $a \sim 0 \Rightarrow ra \sim r0 \sim 0$. $a \sim b$ er ensbetydende med $a-b \in \mathfrak{a}$ (siden $\sim$ er en additiv kongruensrelasjon) og dette er igjen ensbetydende med $a \equiv b \pmod{\mathfrak{a}}$ som viser at $\equiv_{\mathfrak{a}}$ og $\sim$ er identiske. Sats 16 medfører at vi for restklassene modulo et ideal $\mathfrak{a}$ på en naturlig måte kan definere både en addisjon og en multiplikasjon. Om $\mathfrak{a}+b$ og $\mathfrak{a}+c$ er to slike restklasser vil summen og produktet av disse to restklassene være henholdsvis restklassene $\mathfrak{a}+(b+c)$ og $\mathfrak{a}+bc$. Vi får jo f.eks. dette siste ved direkte "mengdemultiplikasjon" $(\mathfrak{a}+b)\cdot(\mathfrak{a}+c) = \mathfrak{a}\mathfrak{a}+\mathfrak{a}\cdot c+b\mathfrak{a}+bc \subseteq \mathfrak{a}+bc$. (Her betyr generelt om A og B er to undermengder av R mengdeproduktet $A \cdot B$ mengden av alle produkter $a \cdot b$ hvor $a \in A$ og $b \in B$.) Vi ser her at selve mengdeproduktet av $\mathfrak{a}+b$ og $\mathfrak{a}+c$ ikke nödvendigvis må være lik $\mathfrak{a}+bc$, men bare er inneholdt i denne restklassen. Men det er denne entydig bestemte restklassen som mengdeproduktet er inneholdt i som tas til definisjon på produktet i restklasse-mengden $R/\mathfrak{a}$.

Første del av satsen ovenfor har vi forövrig allerede bevist i mer generell form i Sats 10. Som vi har bemerket tidligere kan jo den additive gruppen i en ring oppfattes som en operatorgruppe hvor $\Omega = R$ og hvor virkningen av et element $r \in \Omega = R$ på et element $a \in R$ kort og godt er produktet ra. Operatoren r definerer med andre ord avbildningen $a \to ra$. Ω-undergruppene i R blir da idealene i R og den generelle homomorfisatsen Sats 11 gir her

Sats 17. Hvis R er en kommutativ ring og $\mathfrak{a}$ er et ideal i R vil avbildningen $R \to R/\mathfrak{a}$ være en ring-homomorfi. Omvendt hvis φ er en ring-homomorfi av R på R' vil kjernen i denne homomorfien være

et ideal $\mathfrak{a}_\varphi$ i R og vi har ring-isomorfien $R' = {}^R/\mathfrak{a}_\varphi$.

At det homomorfe billede av en ring er en ring kan bevises direkte på nöyaktig samme måte som for Sats 8. Det trengs forövrig en liten bemerkning for å få Sats 17 som et spesialtilfelle av Sats 11. At vi har en operatorhomomorfi φ betyr jo i dette spesialtilfellet at $\varphi(ra) = r\varphi(a)$ eller om vi skriver $\varphi(x) = \bar{x}$ at $\overline{ra} = r\bar{a}$. Men hvis $r_1 \equiv r_2 \pmod{\mathfrak{a}_\varphi}$ så er $\overline{r_1 a} = \overline{r_2 a}$ og derfor $r_1\bar{a} = r_2\bar{a}$. Med andre ord to elementer i R gir identiske operatorer over ${}^R/\mathfrak{a}$ når de hörer til samme restklasse modulo $\mathfrak{a}$. Slike operatorer kan derfor identifiseres og vi får ${}^R/\mathfrak{a}$ som en operatorgruppe med ${}^R/\mathfrak{a}$ som operatorområde og da blir den opprinnelige operatorhomomorfien en ring-homomorfi idet vi får $\overline{ra} = \bar{r}\cdot\bar{a}$.

9. Generering av idealer. Snitt og union av idealer. Hvis $\{\mathfrak{a}_i\}_{i\in I}$ er en vilkårlig familie av idealer i en ring R er det klart at snittet $\bigcap_{i\in I}\mathfrak{a}_i$ igjen er et ideal i R. La så A være en vilkårlig undermengde av ringen R. Da vil det alltid finnes idealer som inneholder A for vi har jo spesielt $A \subseteq R$ og R er et ideal i R. Tar vi snittet av alle idealer som inneholder A får vi etter bemerkningen ovenfor igjen et ideal $\mathfrak{a}$ som inneholder A og dette idealet vil være det entydig bestemte minste ideal som inneholder A. Vi sier da at $\mathfrak{a}$ er generert av A. La oss bestemme det genererte idealet $\mathfrak{a}$ eksplisitt utfra elementene i A. Om $\{a_i\}_{1\le i\le k}$ er en endelig undermengde av A må siden $\mathfrak{a}$ er et ideal som inneholder A elementene av formen $\sum_{i=1}^{k} r_i a_i$ hvor $r_i \in R$ höre til $\mathfrak{a}$. I det generelle tilfelle hvor R ikke har noe enhetselement vet vi imidlertid ikke om elementene $a_1 \dots a_k$ selv kan skrives på denne form. Det samme gjelder mer generelt for elementene av formen $\sum_{i=1}^{k} n_i a_i$ hvor n_i er hele positive eller negative tall og na betyr $a+a+\dots+a$ (n ganger) hvis $n \ge 1$, $0a = 0$ og $(-n)a$ med $n \ge 1$ betyr $-(na)$, $(=n(-a))$. Det genererte ideal $\mathfrak{a}$ vil altså sikkert inneholde alle summer av formen

$$(1) \qquad \sum_{i=1}^{k} r_i a_i + \sum_{j=1}^{l} n_j a_j$$

På den annen side verifiserer en lett at mengden av alle summer av denne formen danner et ideal som inneholder A. Dette idealet må altså være det genererte ideal. Når R har et enhetselement e er

$na = n(ea) = (ne)a = ra$ med $r \in R$ slik at den siste summen i (1) blir "absorbert" i den første. Hvis $A = \{a_1 \cdots a_n\}$ er endelig skriver en ofte det genererte ideal som $(a_1 \cdots a_n)$. Hvis spesielt $n = 1$ skriver vi (a) og vi har da et <u>hovedideal</u> (generert av elementet a).

La oss så betrakte union av idealer. Hvis $\{\mathfrak{a}_i\}$ er en familie av idealer i R forstår vi ved unionen (eller summen) av $\mathfrak{a}_i$'ene idealet generert av den mengdeteoretiske unionen av dem. Denne unionen vil ganske enkelt bestå av alle endelige summer av formen $\sum_{i=1}^{k} a_i$ med $a_i \in \mathfrak{a}_i$: Summen (og differensen) av to slike summer er igjen en slik sum og produktet $r \sum_{i=1}^{k} a_i = \sum_{i=1}^{k} a_i'$ med $a_i' \in \mathfrak{a}_i$ er også en slik sum. Spesielt består unionen $\mathfrak{a} \cup \mathfrak{b}$ av alle summer av formen $a+b$ med $a \in \mathfrak{a}$ og $b \in \mathfrak{b}$. (Når vi snakker om union av idealer dreier det seg altså aldri om mengdeteoretisk union hvis da dette ikke blir uttrykkelig sagt.) En ser ofte skrivemåten $(\mathfrak{a}, \mathfrak{b})$ for idealunionen $\mathfrak{a} \cup \mathfrak{b}$. Hvis $\mathfrak{b}$ er et hovedideal (b) skriver en $(\mathfrak{a}, b)$ istedet for $(\mathfrak{a}, (b))$ idet idealene generert av de mengdeteoretiske unionene $\mathfrak{a} \cup \{b\}$ og $\mathfrak{a} \cup (b)$ er identiske.

<u>10. Primidealer og maksimale idealer</u>. Vi skal nå definere to viktige typer av idealer. Vi sier at idealet $\mathfrak{p}$ i R er et <u>primideal</u> i R hvis

$$ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \quad \text{eller} \quad b \in \mathfrak{p}$$

Dette betyr med andre ord at om $a \notin \mathfrak{p}$ og $b \notin \mathfrak{p}$ så er også $ab \notin \mathfrak{p}$. Anderledes uttrykt: Differensmengden $R - \mathfrak{p}$ danner en undersemigruppe av den multiplikative semigruppen i R. Begrepet primideal danner en naturlig generalisering av begrepet primtall. For om vi innenfor ringen Z av de hele rasjonale tall betrakter hovedidealet (p) generert av et primtall betyr $a \in (p)$ at p er divisor i a : p/a og primidealegenskapen sier derfor her at

(1) $$p/ab \Longrightarrow p/a \quad \text{eller} \quad p/b$$

som jo nettopp er en egenskap som karakteriserer primtallene. Hovedidealene (p) i Z er derfor alle primidealer og som vi skal se nedenfor finnes det ikke andre primidealer i Z enn disse.

<u>Sats 18. Idealet $\mathfrak{p}$ er et primideal i R hvis og bare hvis $R/\mathfrak{p}$ ikke har nulldivisorer (det vil si er et integritetsområde om R har et enhetselement)</u>.

Bevis: Om $a \longrightarrow \bar{a}$ betegner homomorfien av R på $R/\mathfrak{p}$ følger satsen umiddelbart av at $a \in \mathfrak{p}$ og $\bar{a} = \bar{0}$ er ekvivalente utsagn. Det som karakteriserer et primideal $\mathfrak{p}$ i R, nemlig at $R-\mathfrak{p}$ er multiplikativt avsluttet blir jo da ekvivalent med at $\bar{R}-\{\bar{0}\}$ er multiplikativt avsluttet i R ↄ: at $R = R/\mathfrak{p}$ ikke har nulldivisorer.

Et ideal $\mathfrak{m}$ i R slik at $\mathfrak{m} \neq R$ og det ikke finnes noe ideal $\mathfrak{a}$ i R slik at $\mathfrak{m} \subset \mathfrak{a} \subset R$ sier vi er et maksimalt ideal i R. $A \subset B$ betyr generelt at mengden A er ekte inneholdt i B d.v.s. $A \subsetneq B$ og $A \neq B$. Vi kan gi en tilnærmet karakterisering av de maksimale idealene på en liknende måte som Sats 18 karakteriserer primidealene. Vi får en fullstendig karakterisering som et korollar hvis vi forutsetter eksistensen av et enhetselement.

Sats 19. Hvis $\mathfrak{m}$ er et ideal i R vil $R/\mathfrak{m}$ være en kropp hvis og bare hvis følgende to betingelser er oppfylt. 1) $\mathfrak{m}$ er et maksimalt ideal i R. 2) $a^2 \in \mathfrak{m}$ medfører $a \in \mathfrak{m}$.

Bevis: Anta at $R/\mathfrak{m}$ er en kropp. Da har $R/\mathfrak{m}$ ingen nulldivisorer og $\mathfrak{m}$ må være et primideal ifølge Sats 18 og betingelsen 2) må spesielt være oppfylt. Vi skal så vise at $\mathfrak{m}$ er maksimal. Som vanlig betegner vi den restklasse som a hører til med $\bar{a}$. Etter definisjonen på en kropp inneholder $R/\mathfrak{m}$ mer enn ett element og vi har derfor $\mathfrak{m} \subset R$. Hvis $\bar{a} \neq \bar{0}$ og $\bar{b}$ er vilkårlig i $R/\mathfrak{m}$ vil det siden $R/\mathfrak{m}$ er en kropp finnes et $\bar{x} \in R/\mathfrak{m}$ slik at $\bar{a}\bar{x} = \bar{b}$. Med andre ord hvis $a \notin \mathfrak{m}$ og b vilkårlig i R finnes det et $x \in R$ slik at $ax \equiv b(\mathfrak{m})$ ↄ: $ax-b = m$ eller $b = ax-m$ med $m \in \mathfrak{m}$. Dette medfører at $b \in (\mathfrak{m}, a)$ og det for alle $b \in R$ når bare forutsetningen $a \notin \mathfrak{m}$ er oppfylt. Altså $(\mathfrak{m}, a) = R$ for enhver $a \notin \mathfrak{m}$. Dette betyr at $\mathfrak{m}$ er et maksimalt ideal i R. La oss omvendt anta at 1) og 2) er oppfylt og så bevise at $R/\mathfrak{m}$ er en kropp. Vi må vise at $\bar{a}\bar{x} = \bar{b}$ er lösbar i $\bar{x}$ når $\bar{a} \neq \bar{0}$. Siden $\bar{a} \neq \bar{0}$ betyr at $a \notin \mathfrak{m}$ må vi ifølge 2) også ha $a^2 \notin \mathfrak{m}$. Siden idealet $\{ax\}_{x \in R} = \mathfrak{n}$ bestående av alle multipla av a inneholder a^2 har vi derfor $\mathfrak{n} \not\subset \mathfrak{m}$ og $(\mathfrak{m}, \mathfrak{n}) = R$ siden $\mathfrak{m}$ er maksimalt i R. Dette gir $b = m+ax_0$ når $a \notin \mathfrak{m}$. Eller $ax_0 \equiv b \pmod{\mathfrak{m}}$ som betyr at likningen $\bar{a}\bar{x} = \bar{b}$ har lösningen $\bar{x} = \bar{x}_0$.

Korollar 1. Hvis R har et enhetselement så er $\mathfrak{m}$ et maksimalt ideal i R hvis og bare hvis $R/\mathfrak{m}$ er en kropp.

Bevis: Vi trenger bare å vise at i tilfelle R har et enhetselement så er 2) en følge av 1). La $\mathfrak{m}$ være maksimal og anta $a \notin \mathfrak{m}$. Da er $(\mathfrak{m}, a) = R$ og ethvert element i R kan derfor skrives på formen $m+ax$.

Spesielt kan vi anta at enhetselementet $e = m_o + ax_o$. Dette gir ved multiplikasjon med a identiteten $a = am_o + a^2x_o$. Hvis $a^2 \in \mathfrak{m}$ ville vi derfor etter denne likningen få $a \in \mathfrak{m}$ imot forutsetningen. Vi må altså ha $a \notin \mathfrak{m} \Longrightarrow a^2 \notin \mathfrak{m}$ som er ekvivalent med 2).

Korollar 2. I en ring med enhetselement er ethvert maksimalt ideal et primideal. Dette följer av Sats 18 sammen med Korollar 1 siden en kropp ikke har nulldivisorer.

Korollar 3. En ring med enhetselement R er en kropp hvis og bare hvis R ikke har andre idealer enn R og $\{0\}$.

Eksempler. Selv om vi ovenfor (Korollar 1) har brukt eksistensen av et enhetselement for å vise at betingelsen 1) i Sats 19 impliserer betingelsen 2) kunne det jo fremdeles tenkes at implikasjonen $1 \Longrightarrow 2$ var generelt gyldig og at derfor 2) kunne slöyfes i formuleringen av Sats 19. At dette ikke er tilfelle kan vi se på et enkelt eksempel. La R være ringen av de like tall (under vanlig addisjon og multiplikasjon) og la $\mathfrak{m} = (4)$ være hovedidealet i R generert av tallet 4. Dette idealet er maksimalt i R for föyer vi til et tall som ikke hörer til $\mathfrak{m}$ d: er av formen $4m+2$ vil $2 = 4m+2-4m \in (4,4m+2)$. Med andre ord $(4,4m+2) = (2) = R$ for ethvert helt m og (4) er derfor et maksimalt ideal i R. Men betingelsen 2) er ikke oppfylt i R for $2 \notin (4)$ mens $2^2 \in (4)$.

La oss dernest nevne et par eksempler som viser at vi ikke har noen omvending av Korollar 2. La $Z[x]$ betegne ringen av alle polynomer i en variabel x med hele rasjonale koeffisienter under vanlig addisjon og multiplikasjon. Her vil hovedidealet (x) generert av polynomet x være et primideal. Det består jo nöyaktig av de polynomer som ikke har noe konstantledd og produktet av to polynomer med konstantledd $\neq 0$ er et polynom med konstantledd $\neq 0$. Men dette idealet er ikke maksimalt for vi har f.eks. $(x) \subset (x,2) \subset R$ hvor begge inklusjonene er ekte. Idealet $(x,2)$ som består av alle polynomer hvis konstantledd er et like tall er imidlertid et maksimalt ideal i $Z[x]$.

Vi skal så se på et eksempel som står i forbindelse med viktige moderne undersökelser i analysen. La C nå betegne ringen av alle reelle kontinuerlige funksjoner definert i det lukkede intervallet $[0,1]$. Vi skal bestemme de maksimale idealene i C. Om dette har vi följende sats.

Sats 20. La $a \in [0,1]$. Da vil mengden av de funksjoner $f \in C$ som er slik at $f(a) = 0$ danne et maksimalt ideal $\mathfrak{m}_a$ i C og det finnes ikke andre maksimale idealer i C enn disse. Korrespondansen $a \longrightarrow \mathfrak{m}_a$

er en-entydig.

Bevis: Etter definisjonen har vi $\mathfrak{m}_a = \{f,\ f \in C \ \&\ f(a) = 0\}$. At $\mathfrak{m}_a$ er et ideal i C er klart. La så $f \in C$ være slik at $f \notin \mathfrak{m}_a$, det vil si $f(a) = b \neq 0$. La oss betegne med f_b funksjonen som er konstant lik b i hele intervallet $[0,1]$. Da vil $f_b \in C$ og $(f-f_b)(a) = 0$ $\supset$: $f-f_b \in \mathfrak{m}_a$ og $f_b \in (\mathfrak{m}_a, f)$. Siden $f_b \neq 0$ i hele $[0,1]$ er også $\frac{1}{f_b} \in C$ og funksjonen f_1 konstant lik 1 vil siden $f_1 = f_b \cdot \frac{1}{f_b}$ på grunn av den multiplikative idealegenskapen höre til $(\mathfrak{m}_a, f)$ som gir $(\mathfrak{m}_a, f) = C$ og $\mathfrak{m}_a$ er derfor maksimal i C som påstått. La oss dernest anta at $\mathfrak{m}$ er et maksimalt ideal i C som ikke er av typen $\mathfrak{m}_a$ ovenfor. Det må da for ethvert $a \in [0,1]$ finnes en funksjon $f \in \mathfrak{m}$ slik at $f(a) \neq 0$. (Ellers ville nemlig $f(a) = 0$ for alle $f \in \mathfrak{m}$ og vi måtte ha $\mathfrak{m} \subseteq \mathfrak{m}_a$ som på grunn av den antatte maksimalitet av $\mathfrak{m}$ ville gi $\mathfrak{m} = \mathfrak{m}_a$). Siden C bare består av kontinuerlige funksjoner vil om $f(a) \neq 0$ også $f(x) \neq 0$ i en viss omegn om a. Vi kan dessuten uten innskrenking anta at f er ≥ 0 overalt i $[0,1]$ for hvis f ikke var positiv kunne vi bruke den positive funksjonen f^2. Vi får altså for ethvert $a_i \in [0,1]$ en funksjon $f_i \in \mathfrak{m}$ som er positiv og $> \varepsilon_i > 0$ i en viss åpen omegn O_i omkring a_i. Mengdene O_i danner en åpen overdekking av $[0,1]$ og vi kan ifölge Borel-Lebesgues sats (siden $[0,1]$ er kompakt !) plukke ut et endelig antall av dem: $O_1, O_2 \ldots O_n$ slik at allerede disse danner en overdekking av $[0,1]$ $\supset$: $[0,1] = \bigcup_{i=1}^{n} O_i$. Av de tilsvarende funksjonene $f_1 \ldots f_n$ konstruerer vi en ny funksjon $f = \sum_{i=1}^{n} f_i$ som kommer til å höre til $\mathfrak{m}$ siden alle f_i gjör det. Dessuten er $f(x) > \mathrm{Min}(\varepsilon_1 \ldots \varepsilon_n) > 0$ overalt i $[0,1]$, p.g.a. positiviteten av f_i'ene. Dette sikrer at vi får $\frac{1}{f} \in C$ som sammen med $f \in \mathfrak{m}$ gir $1 = \frac{1}{f} \cdot f \in \mathfrak{m}$. Men det betyr at $\mathfrak{m} = C$ imot forutsetningen om at $\mathfrak{m}$ er maksimal i C. Denne motsigelsen viser at det ikke finnes andre maksimale idealer i C enn de som er av formen $\mathfrak{m}_a = \{f, f(a) = 0\}$. Entydigheten av avbildningen $a \longrightarrow \mathfrak{m}_a$ fölger direkte av den ting at om $a_1 \neq a_2$ så finnes det alltid en kontinuerlig funksjon som er null i a_1 men ikke i a_2.

Etter Korollar 1 (til Sats 19) vet vi at kvotientringen $C/\mathfrak{m}_a$ skal være en kropp. Det er lett å se at dette er kroppen av de reelle tallene. For $f \equiv g \pmod{\mathfrak{m}_a}$ betyr at $(f-g)(a) = 0$ $\supset$: $f(a) = g(a)$. En restklasse modulo $\mathfrak{m}_a$ betår derfor nettopp av alle funksjoner $f \in C$ som antar en fast reell verdi og restklassen kan identifiseres med denne verdien. Vi kan også se det slik: Avbildningen $f \rightarrow f(a)$ er

en homomorfi av C på R (= kroppen av de reelle tall) som har $\mathfrak{m}_a$ som kjerne. Etter den fundamentale homomorfisatsen må vi derfor ha $C/\mathfrak{m}_a = R$.

11. Hovedidealringer. Euklidske ringer. Det er selvfölgelig å vente at idealteorien i en ring blir særlig enkel om ethvert ideal er hovedideal ɔ: kan genereres av et enkelt element. En slik ring kaller vi en hovedidealring. For visse ringer kan en konstatere at de er hovedidealringer ved å anvende en generell form av den klassiske Euklidske algoritme. De ringer hvor dette er mulig kalles Euklidske ringer og defineres slik: En kommutativ ring R sies å være en Euklidsk ring dersom det over R-{0} er definert en funksjon δ slik at

1) $\delta(a)$ er et helt rasjonalt tall ≥ 0
2) Hvis $a \neq 0$ og $b \neq 0$ så er også $ab \neq 0$ og $\delta(ab) \geq \delta(a)$
3) Hvis $a \neq 0$ og b vilkårlig eksisterer det to elementer q og r slik at $b = aq+r$ hvor enten $r = 0$ eller $\delta(r) < \delta(a)$ dersom $r \neq 0$.

Bemerkning: Denne definisjonen er hentet fra van der Waerden. Jacobson har en noe strengere definisjon. I van der Waerdens definisjon fordres i motsetning til Jacobsons ikke eksistensen av et enhetselement. Med definisjonen ovenfor kan imidlertid som vi skal se eksistensen av enhetselement bevises.

Eksempler på Euklidske ringer er (1) Ringen av alle hele rasjonale tall med $\delta(a) = |a|$. 2) Ringen av alle hele Gaussiske tall a+ib (a og b $\in$ Z) med $\delta(c) = a^2+b^2$ (se v.d.W. s.68-69). 3) Polynomringen K[x] av alle polynomer i en variabel x og koeffisienter fra kroppen K. Her settes $\delta(p(x))$ = graden $(p(x))$. Eksemplene (1) og (3) vil bli behandlet nedenfor.

Sats 21. Enhver Euklidsk ring R er en hovedidealring og ethvert ideal (a) i R er til og med identisk med mengden av alle multipla av a ɔ: (a) = Ra.

Bevis: La $\mathfrak{a}$ være et ideal i R. Er $\mathfrak{a} = (0)$ er det ikke noe å bevise. Anta derfor $\mathfrak{a} \neq (0)$ og la $c \in \mathfrak{a}$ med $c \neq 0$. Da er $\delta(c)$ definert og ≥ 0. Det må derfor finnes et $a \in \mathfrak{a} - \{0\}$ slik at $0 \leq \delta(a) \leq \delta(c)$ for alle $c \in \mathfrak{a} - \{0\}$. Til dette a og et vilkårlig $c \in \mathfrak{a}$ eksisterer det derfor etter 3) et q og r slik at $c = aq+r$ med $\delta(r) < \delta(a)$ hvis $r \neq 0$. Etter a's minimalegenskap er imidlertid dette umulig og vi får etter den annen mulighet i 3) at $r = 0$ ɔ: $c = aq$ og $\mathfrak{a} = Ra$ som påstått.

Korollar. En Euklidsk ring har alltid et enhetselement.

Bevis: Etter Sats 21 har vi spesielt at $R = Ra$ for passende a. Spesielt har vi derfor $a = ca$ for et $c \in R$. For et vilkårlig element $r = qa$ i ringen får vi ved å multiplisere $a = ca$ med q at $aq = caq$ d: $r = cr$ som viser at c er enhetselement i R.

Sats 22. I en hovedidealring R med enhetselement har to elementer a,b alltid en største felles divisor d som lar seg skrive på formen $d = ra+sb$ med $r,s \in R$.

Bevis: Idealet (a,b) består av alle elementer av formen $ra+sb$ og da (a,b) er identisk med et hovedideal (d) vil $d = ra+sb$ for passende r og s. $(a,b) = (d)$ viser videre at $a = k_1 d$ og $b = k_2 d$; d er med andre ord divisor i a og b og den er største felles divisor for hvis $c|a$ og $c|b$ vil siden $d = ra+sb$ også $c|d$.

12. Produktsoppspaltning i Euklidske ringer. Vi skal nå bevise hovedsatsen om entydig oppspaltning i produkt av irreduktible elementer i en Euklidsk ring. Først noen definisjoner. Er generelt R et integritetsområde med enhetselement e så sier vi at elementet $a \in R$ er en enhet i R dersom a har en invers $b = a^{-1}$ i R slik at $ab = e$. At b er en divisor i a, det vil si $a = bc$ skriver vi $b|a$. Om både $a|b$ og $b|a$ kaller vi a og b for assosierte elementer. En ser lett at to elementer a,b i R er assosierte hvis og bare hvis det eksiterer en enhet e_1 slik at $a = be_1$. Et element $a \neq 0$ som ikke er noen enhet kalles irreduktibelt hvis en oppspaltning $a = bc$ alltid medfører at b eller c er en enhet.

Sats 23. Ethvert element i en Euklidsk ring som er forskjellig fra null og ikke er noen enhet kan spaltes i et produkt av irreduktible elementer. Denne oppspaltingen er i det vesentlige entydig i den forstand at om $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ er to slike oppspaltinger av a er $r = s$ og indeksene kan velges slik at p_i er assosiert med q_i.

Bevis: For å bevise eksistensen av en oppspaltning av a i irreduktible elementer anvender vi induksjon med hensyn på tallet $\delta(a)$. Anta at eksistensen er sikret for alle b med $\delta(b) < n$ og la $\delta(a) = n$. Hvis a er irreduktibel er det ikke noe å bevise. Er a reduktibel har vi en oppspalting $a = bc$ hvor hverken b eller c er en enhet. Med andre ord a og b er ikke assosierte og siden $b|a$ betyr det at a ikke går opp i b. Vi har derfor etter egenskapen 3) ved en Euklidsk ring at $b = aq+r$ hvor $r \neq 0$ og derfor $\delta(r) < \delta(a)$. Setter vi inn

$a = bc$ får vi $r = b-aq = b(\epsilon-cq)$. Av 2) kan vi derfor slutte at $\delta(r) \geq \delta(b)$ og $\delta(b) \leq \delta(r) < \delta(a)$. Av dette følger spesielt at om $\delta(a) = 0$ så er a irreduktibel og eksistensen er sikret i dette tilfellet. På samme måte er $\delta(c) < \delta(a)$ og etter induksjonsantakelsen kan derfor både b og c spaltes i et produkt av irreduktible elementer. Det samme gjelder dermed også for produktet $a = bc$.

Anta så at

(1) $$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

er to oppspaltinger av a i irreduktible elementer. Hvis $r = 1$ er entydigheten klar. Vi anvender derfor induksjon med hensyn på r. Først trenger vi imidlertid å påvise at et irreduktibelt element p er et "primelement" i den forstand at om $p \mid ab$ så har vi $p \mid a$ eller $p \mid b$ eller med andre ord at hovedidealet (p) er et primideal. $(p) \subseteq (c)$ er ensbetydende med $c \mid p$ og siden en Euklidsk ring er en hovedidealring finnes det derfor ikke andre idealer enn de hovedidealer (c) hvor c enten er assosiert med p eller er en enhet, som inneholder (p). Det betyr at (p) er et maksimalt ideal i R og derfor også et primideal. Av (1) får vi $p_1 \mid q_1 \cdots q_s$ og derfor ved passende valg av indekser at $p_1 \mid q_1$ eller $q_1 = p_1 \cdot e_1$. Her må e_1 være en enhet siden q_1 er irreduktibel og p_1 og q_1 er assosierte. Setter vi dette inn i likningen (1) og forkorter med p_1 (som er mulig siden R er et integritetsområde) får vi

$$p_2 p_3 \cdots p_r = (e_1 q_2) \cdots q_s$$

Etter induksjonsantagelsen er faktorene her parvis assosierte og satsen er bevist.

Eksempel. Ringen Z av de hele rasjonale tall er en hovedidealring siden vi der har en Euklidsk algoritme ved å sette $\delta(a) = |a|$. Av Sats 23 følger da entydigheten av oppspaltningen av de hele tall (> 0) som produkt av primtall. Denne entydigheten har vi forövrig også fått tidligere som et korollar av Jordan-Hölders sats. Ethvert ideal i Z er altså et hovedideal (m) generert av et helt tall m. Ifölge Sats 16 finnes det derfor ikke andre kongruenser i Z enn dem som er av formen $a \equiv b \pmod{(m)}$, men dette betyr nöyaktig det samme som det man i tallteorien skriver $a \equiv b \pmod{m}$, d: $a-b = km$. Vi ser her bort fra tilfellet $m = 0$ hvor kongruensen reduserer seg til likhet i Z. Den tilsvarende restklasseringen $Z/(m)$ består av m elementer $0,1,2,\ldots m-1$ som adderes og multipliseres på vanlig måte - bare det at

resultatet av operasjonen skal være resten man får ved divisjon av det utkomne med m. Vi vet generelt etter Korollar 2 til Sats 19 at ethvert maksimalt ideal i Z er et primideal. I dette eksemplet gjelder imidlertid også det omvendte når $m \neq 0$. For om (m) er et primideal er $Z/(m)$ et integritetsområde etter Sats 18 og siden det er endelig följer det av Sats 3 at $Z/(m)$ er en kropp og dermed er (m) et maksimalt ideal ifölge Sats 19. Begrepene primideal og maksimalt ideal faller altså sammen i ringen Z av de hele tall. Forövrig er det klart at (m) er et primideal hvis og bare hvis m er et primtall. For $ab \in (m)$ betyr $ab = km \Rightarrow m|ab$ og hvis m er et primtall medförer dette $m|a$ eller $m|b \Rightarrow a \in (m)$ eller $b \in (m)$, altså er (m) et primideal. Omvendt hvis m ikke er primtall $\Rightarrow m = ab$ med $|a| < |m|$ og $|b| < |m|$ vil vi ha $a \notin (m)$ og $b \notin (m)$ og (m) er derfor ikke noe primideal. - Bemerkningene ovenfor viser oss spesielt at det til ethvert primtall p svarer en endelig kropp $Z/(p)$ med p elementer. Vi kaller denne kroppen for restklassekroppen modulo p. (Se Sats 28.)

13. Polynomringer. En type av ringer som er spesielt viktige for den Galoiske teori er de såkalte polynomringer. Mengden av alle polynomer $p(x_1 \ldots x_n)$ i n variable med koeffisienter fra en fast ring R danner under vanlig addisjon og multiplikasjon av polynomer en ring. Denne polynomringen betegner vi med $R[x_1 \ldots x_n]$. Et spesielt enkelt og viktig tilfelle er det hvor $n = 1$ og R er en kropp K altså polynomringen $K[x]$ i en variabel x ved koeffisienter fra en kropp K. Det som gjör at dette tilfellet er spesielt enkelt er at $K[z]$ er en Euklidsk ring og dermed hovedidealring. Vi starter med å vise dette:

Sats 24. Hvis K er en kropp er $K[x]$ en Euklidsk ring. Den Euklidske algoritme er her slik at om $a(x) \neq 0$ og $b(x)$ begge hörer til $K[x]$ kan vi finne polynomer $q(x)$ og $r(x) \in K[x]$ slik at $b(x) = q(x)a(x)+r(x)$ hvor $r(x)$ enten er nullpolynomet eller har en grad som er mindre enn graden til $a(x)$. Derfor kan funksjonen $\delta(p(x)) = \text{grad } p(x)$ brukes til å vise at 1), 2) og 3) i definisjonen på en Euklidsk ring er tilfredstillet for $K[x]$.

Bevis: La $a(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0$ og $b(x) = b_n x^n + \ldots + b_0$ med $a_m \neq 0$, $b_n \neq 0$. Vi kan anta at $n \geq m$ for er $n < m$ er allerede $b(x) = 0 \cdot a(x) + b(x)$ med $q(x) = 0$ en fremstilling av den önskede type. Med $n \geq m$ kan vi skrive

$$b(x) = \frac{b_n}{a_m} x^{n-m} \cdot a(x) + b_1(x)$$

hvor $b_1(x) = (b_{n-1} - \frac{b_n}{a_m} a_{m-1})x^{m-1} + \ldots$ er av höyst (n-1)'te grad. Vi kan nå hvis $n-1 \geq m$ skrive $b_1(x)$ på liknende måte $b_1(x) = kx^{n-1-m}a(x)+b_2(x)$ hvor grad $b_2 \leq n-2$. Slik kan vi tydeligvis fortsette (her ligger egentlig en induksjonsslutning !) til vi kommer ned til et $b_k(x)$ med grad $< m$ og dette $b_k(x)$ er det $r(x)$ vi söker. $q(x)$ vil bli dannet av den summen av monomer som $a(x)$ kan settes utenfor som felles faktor.

Korollar 1. Om polynomet $p(x)$ divideres med polynomet $x-c$ er resten konstanten $p(c)$.

Bevis: Siden $x-c$ er av förste grad må $r(x) = p(x)-(x-c)q(x)$ være av nullte grad d: lik en konstant (eller = konstanten 0 som ikke tillegges grad). Denne konstanten kan derfor bestemmes ved å sette inn en passende verdi for x. Setter vi $x = c$ får vi $r = p(c)$.

Korollar 2. Hvis $p(c) = 0$ har $p(x)$ den lineære faktor $x-c$ d: $p(x) = q(x)(x-c)$.

Et polynom i $K[x]$ sies å være irreduktibelt (over K) hvis det ikke kan skrives som et produkt av to polynomer som begge minst er av förste grad. Et förstegradspolynom er derfor spesielt alltid irreduktibelt. Av Sats 23 følger

Sats 25. Ethvert polynom av grad ≥ 1 i $K[x]$ kan skrives entydig som et produkt av en konstant ($\in K$) og irreduktible polynomer alle med höyeste koeffisient lik 1. (1 er enhetselement i kroppen.)

For behandlingen av en del eksempler i tilknytning til den Galoiske teorien vil det være nyttig å ha bevist det såkalte Eisensteinske irreduktibilitetskriterium. Siden vi imidlertid bare skal bruke dette kriteriet i tilknytning til eksempler tillater vi oss i beviset å benytte ubevist følgende lille setning: Hvis et polynom med hele rasjonale koeffisienter kan skrives som et produkt av polynomer med rasjonale koeffisienter så kan det også skrives som et produkt av polynomer med hele koeffisienter. (For bevis av dette i en mer generell form se [9] s. 98-99).

Sats 26. (Eisensteins irreduktibilitetskriterium). La $a(x) = a_n x^n + \ldots + a_0$ være et polynom med hele rasjonale koeffisienter. Hvis da p er et primtall slik at $p \nmid a_n$, $p \mid a_i$ for $0 \leq i \leq n-1$ og $p^2 \nmid a_0$. Da er $a(x)$ irreduktibel over kroppen av de rasjonale tall.

Bevis: Hvis vi har en oppspaltning

$$a(x) = (b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0)(c_k x^k + \ldots + c_0)$$

kan vi ifölge den ubeviste hjelpesatsen som ble nevnt ovenfor anta at b'ene og c'ene er hele tall. Siden $a_0 = b_0 c_0$ får vi av betingelsene $p^2 \nmid b_0 c_0$ og $p \mid b_0 c_0$ at nöyaktig et av tallene b_0 og c_0 må være delelig med p. La oss anta $p \nmid b_0$ og $p \mid c_0$. Etter betingelsene vet vi også at $p \nmid a_n$ d: $p \nmid b_m c_k$ som gir $p \nmid c_k$. Siden $p \mid c_0$ må det derfor finnes en indeks r slik at $p \mid c_0$, $p \mid c_1 \ldots p \mid c_{r-1}$, men $p \nmid c_r$. Da $a_r = b_0 c_r + b_1 c_{r-1} + \ldots + b_r c_0$ og p går opp i alle ledd i summen unntatt det förste vil $p \nmid a_r$. Ifölge betingelsene i satsen må vi da ha $r = n$ og graden til det siste polynomet i oppspaltingen for $a(x)$ blir n. Dette viser at vi ikke kan ha noen oppspalting av $a(x)$ i polynomer av lavere grad og $a(x)$ er derfor irreduktibelt.

§ 3. Kropper.

14. Kropper, primkropper og kroppers karakteristikk. Vi gjentar at vi med en kropp forstår en kommutativ ring (bestående av minst to elementer) hvor elementene $\neq 0$ danner en gruppe under multiplikasjon. Hvis K er en kropp og A er en undermengde av K som danner en kropp m.h.p. de operasjoner som allerede er definert i K sier vi at A er en underkropp av K. For at dette skal finne sted må for det förste A være en underring av K d: hvis $a, b \in A$ så er også $a-b$ og $ab \in A$. Videre må A inneholde det multiplikative enhetselementet og dessuten a^{-1} hvis $a \in A$ og $a \neq 0$. Det er umiddelbart klart at snittet av en vilkårlig familie av underkropper av K igjen er en underkropp. Med en primkropp i K forstår vi en underkropp av K som ikke inneholder andre underkropper av K enn seg selv. Vi har fölgende enkle

Sats 27. Enhver kropp K inneholder en entydig bestemt primkropp P.

Bevis: Snittet av alle underkropper til K er en underkropp som tydeligvis ikke kan inneholde andre underkropper enn seg selv. Den er altså en primkropp. Om videre P_1 og P_2 er to primkropper i K vil vi nödvendigvis siden $P_1 \cap P_2$ igjen er en underkropp av P_1 og P_2 måtte ha $P_1 = P_1 \cap P_2 = P_2$. Fölgende sats gir en fullstendig beskrivelse av hvilke typer av primkropper som kan opptre

Sats 28. Hvis K er en gitt kropp vil primkroppen P i K enten være isomorf med den endelige restklassekroppen modulo p (se eksemplet s. 27) eller isomorf med kroppen av de rasjonale tall.

Bevis: La P være primkroppen i K. P inneholder nullelementet 0 og enhetselementet e og dermed alle summer av formen $ne = \pm \sum e (n \in Z)$. På grunn av distributiviteten av multiplikasjon m.h.p. addisjon har vi regnereglene

$$ne+me = (n+m)e$$

og

$$ne \cdot me = nme^2 = nme$$

Dette viser at de heltallige multipla av enhetselementet e danner en underring R av K og avbildningen $n \to ne$ av Z på R er åpenbart en homomorfi. Etter den generelle homomorfisatsen må da $Z/\mathfrak{p} = R$ hvor $\mathfrak{p}$ er kjernen i homomorfien $n \to ne$ d: de n som er slik at $ne = 0$. Da R er en underring av en kropp og derfor ikke kan inneholde nulldivisorer må $\mathfrak{p}$ være et primideal og derfor $\mathfrak{p} = (p)$ hvor p er et primtall eller $\mathfrak{p} = (0)$, etter hva vi fant om idealene i Z på side 27. Vi har altså to muligheter:

1) $\mathfrak{p} = (p)$ hvor p er et primtall som er det minste tall > 0 slik at $pe = 0$. I dette tilfellet vet vi at $R = Z/(p)$ er en kropp og siden primkroppen i K inneholder R må K's primkropp nettopp være restklassekroppen modulo p; $P \cong Z/(p)$.

2) $\mathfrak{p} = (0)$. I dette tilfellet får vi $R = Z/(0) \cong Z$ slik at primkroppen P må inneholde ringen R isomorf med ringen Z av de hele rasjonale tall. Siden P er en kropp må P også inneholde alle bröker $\frac{a}{b} = ab^{-1}$ med $a,b \in R$, $b \neq 0$ og dermed inneholde en underkropp som er isomorf med kroppen av de rasjonale tall Q. Siden P er primkropp må $P \cong Q$. Sats 28 er dermed bevist.

Denne satsen leder til följende viktige klassifisering av kropper: K sies å ha karakteristikk p dersom dens primkropp er restklassekroppen modulo p og ha karakteristikk null dersom primkroppen er (isomorf med) kroppen Q av de rasjonale tallene. I det förste tilfellet er altså p karakterisert ved at det er det minste hele tall > 0 slik at $pe = 0$. I det andre tilfellet har vi $ne \neq 0$ for alle $n \neq 0$.

Sats 29. Hvis $a \neq 0$ er et element i K og k betegner karakteristikken til K vil $na = ma$ være ekvivalent med at $n \equiv m \pmod k$.

Bevis: Multipliserer man likningen $na = ma$ med a^{-1} får man $ne = me$ som etter definisjonen på karakteristikken betyr at $n \equiv m \pmod k$. Dette beviset går like godt den andre veien.

Ved å sette $m = 0$ og $k = p$ gjelder spesielt at $na = 0$ er ekvivalent med at $p \mid n$ når $a \neq 0$. Dette betyr at for alle $a \neq 0$ er p det minste hele tall > 0 slik at $pa = 0$.

Sats 30. I en kropp med karakteristikk $p>0$ gjelder identitetene $(a+b)^p = a^p+b^p$ og $(a-b)^p = a^p-b^p$.

Bevis: I enhver kommutativ ring bevises binomialformelen på nöyaktig samme måte som for tall slik at vi har $(a+b)^p = a^p+\binom{p}{1}a^{p-1}b+\ldots+\binom{p}{p-1}ab^{p-1}+b^p$. Her er imidlertid alle koeffisientene $\binom{p}{i} = \frac{p(p-1)\ldots(p-(i-1))}{1\cdot 2\ldots i}$ hvor $1 \leq i \leq p-1$ delelig med p siden $\binom{p}{i}$ er et helt tall hvor primtallet p inngår som faktor i telleren, men ikke i nevneren. Alle de ledd som svarer til disse i må derfor være null og $(a+b)^p = a^p+b^p$. Den andre formelen får vi ved å sette $a+b = c$ i den förste $\supset$: $c^p = (c-b)^p+(b^p$ eller $(c-b)^p = c^p-b^p$.

15. Utvidelse av kropper. Hvis kroppen K inneholder kroppen F som underkropp sier vi at K er en utvidelse(skropp) eller overkropp til F. Hovedproblemet i kropp-teorien er å få en oversikt over alle mulige utvidelseskropper til en gitt kropp. En tilfredsstillende lösning av dette problem ville jo gi en oversikt over alle kropper siden enhver kropp kan betraktes som utvidelse av sin primkropp som vi allerede kjenner fullstendig ved Sats 28. Dette skulle til å begynne med gi en tilstrekkelig motivering for å betrakte dette utvidelsesproblemet. Den Galoiske teorien gir nettopp et viktig bidrag til lösningen av dette problemet.

La F være en fast kropp (den betegnes ofte som grunnkroppen) og K en utvidelseskropp til F. Hvis nå M er en vilkårlig undermengde av K betegner vi den minste underkroppen av K som inneholder både F og M med $F(M)$. Kroppen $F(M)$ er entydig bestemt som snittet av alle underkropper av K som inneholder $F \cup M$. En sier ofte at $F(M)$ er oppstått ved adjunksjon av M til F. $F(M)$ inneholder, siden den er en kropp, mengden av alle rasjonale uttrykk i et endelig antall elementer fra M med koeffisienter fra F. Men siden denne mengden tydeligvis allerede er en kropp er den lik den entydig bestemte minste underkropp av K som inneholder $F \cup M$ og er derfor identisk med $F(M)$. Vi har hermed et eksplisitt uttrykk for elementene i $F(M)$. Vi definerer videre $F[M]$ (med hakeparentes) som den minste ringen i K som inneholder $F \cup M$ og denne ringen er lik snittet av alle ringer i K som inneholder $F \cup M$. $F[M]$ består tydeligvis av alle polynomer i alle endelige antall av m'er $\in M$ med koeffisienter fra F. Hvis spesielt M er en endelig mengde $M = \{m_1, m_2, \ldots m_n\}$ skriver vi istedet for $F(M)$ og $F[M]$ henholdsvis $F(m_1, \ldots m_n)$ og $F[m_1, \ldots m_n]$. Etter hva vi har sagt om den eksplisitte form for elementene i $F(M)$ og

$F[M]$ som henholdsvis rasjonale og hele rasjonale uttrykk i et endelig antall elementer fra M med koeffisienter fra F er det tydelig at f.eks. enhver $F(M)$ kan skrives som en union av utvidelseskropper av den endelige formen $F(m_1,\ldots m_n)$. Adjunksjon av en vilkårlig mengde M til F er altså blitt tilbakeført til adjunksjon av endelige mengder samt dannelsen av mengdeteoretisk union av kropper. Nå er det videre klart at $F(m_1,\ldots m_n) = F(m_1,\ldots m_{n-1})(m_n)$ hvor det siste uttrykket betegner kroppen fremkommet ved adjunksjon av m_n til kroppen $F(m_1,\ldots m_{n-1})$. Dermed er utvidelse ved en endelig mengde $\{m_1,\ldots m_n\}$ tilbakeført til n suksessive adjunksjoner av et enkelt element. Disse utvidelsene kalles <u>enkle kropputvidelser</u> og er altså av formen $F(m)$. Det er derfor naturlig først å pröve å få en oversikt over disse.

<u>16. Enkle kropputvidelser. Algebraiske og transendente utvidelser</u>. La F være en kropp med en utvidelseskropp K og la α være et vilkårlig element i K. Vi betrakter den enkle utvidelseskroppen $F(\alpha)$. Vi vet at $F(\alpha)$ iallfall inneholder <u>ringen</u> $F[\alpha]$ som består av alle polynomer av formen $\sum_{i=0}^{n} a_i \alpha^i$ med $a_i \in F$. Vi betrakter nå polynomringen $F[x]$ (= mengden av alle polynomer i et element (bokstav) x som ikke har noe med K å gjöre) og avbildningen

$$f(x) \longrightarrow f(\alpha) \quad \text{eller} \quad \sum_{i=0}^{n} a_i x^i \longrightarrow \sum_{i=0}^{n} a_i \alpha^i$$

Dette gir en homomorfi av $F[x]$ på $F[\alpha]$. Etter den generelle homomorfisatsen vil da

$$F[\alpha] \cong F[x]/\mathfrak{p}$$

hvor $\mathfrak{p}$ er idealet bestående av alle polynomer $f(x)$ slik at $f(\alpha) = 0$, d.v.s. de polynomer som har α som rot. Nå vet vi at $F[\alpha]$ som delmengde av kroppen K ikke har nulldivisorer og $\mathfrak{p}$ må derfor være et primideal. Videre kan ikke $\mathfrak{p}$ være hele $F[x]$ for det finnes polynomer - slik som f.eks. konstantene - som ikke har α som nullpunkt. Vi har allerede sett at $F[x]$ er en Euklidisk ring og dermed er en hovedidealring slik at vi får to muligheter

I. $\mathfrak{p} = (p(x))$ hvor $p(x)$ er et irreduktibelt polynom. Var nemlig $p(x) = f(x)\cdot g(x)$ med $f,g \in F[x]$ og begge to av grad lavere enn graden til $p(x)$ kunne ikke $(p(x))$ være noe primideal siden $f,g \notin (p(x))$. Av $(p(x)) \subsetneq (f(x))$ följer at $p(x) = f(x)g(x)$ med $f,g \in F[x]$ og siden $p(x)$ er irreduktibel vil $f(x)$ eller $g(x)$ være

en konstant (d.v.s. et element i F). Dette gir mulighetene $(f(x)) = (p(x))$ og $(f(x)) = F[x]$ som viser at $(p(x))$ er et maksimalt ideal i $F[x]$. Ringen

$$F[\alpha] \cong F[x]/(p(x)) \tag{1}$$

er derfor i virkeligheten en kropp. Siden $F[\alpha] \subseteq F(\alpha)$ må vi ifölge minimalegenskapen til $F(\alpha)$ ha $F(\alpha) = F[\alpha]$ slik at isomorfien (1) gir den sökte enkle utvidelseskroppen $F(\alpha)$.

II. $\varphi = (0)$. Dette betyr at homomorfien $F[x] \longrightarrow F[\alpha]$ er en isomorfi. Det finnes da ikke noe polynom i $F[x]$ bortsett fra nullpolynomet som har α som rot og regning med polynomer i α blir nöyaktig som om α var en ubestemt störrelse (som ikke har noe med K å gjöre) slik som x. Av isomorfien $F[x] \cong F[\alpha]$ får vi ved å gå over til de respektive kvotientkropper at $F(x) \cong F(\alpha)$. Den enkle utvidelseskroppen $F(\alpha)$ blir altså i dette tilfellet isomorf med kroppen av alle rasjonale funksjoner i en variabel med koeffisienter fra F.

I tilfellet I ovenfor hvor α er rot i en algebraisk likning $p(x) = 0$ sier vi at α er algebraisk over (eller m.h.p.) F og $F(\alpha)$ er en enkel algebraisk utvidelse av F. I tilfellet II hvor α ikke tilfredsstiller noen likning $f(x) = 0$ med $f \in F[x]$ og $f \neq 0$ sier vi at α er transendent over F og at $F(\alpha)$ er en enkel transendent utvidelse av F. Med disse definisjonene har vi altså bevist följende

Sats 31. En enkel utvidelse $F(\alpha)$ er enten algebraisk eller transendent. I förste tilfelle er $F(\alpha) \cong F[x]/(p(x))$ hvor $p(x)$ er et irreduktibelt polynom i $F[x]$ karakterisert entydig på en konstant multiplikativ faktor nær som det polynom av lavest grad i $F[x]$ slik at $p(\alpha) = 0$. I annet tilfelle er $F(\alpha)$ isomorf med kroppen $F(x)$ av alle rasjonale funksjoner i en ubestemt x med koeffisienter fra F.

Entydigheten av $p(x)$ ser vi slik: Om $p(x) = a_n x^n + \ldots + a_o$ og $q(x) = b_n x^n + \ldots + b_o$ er et annet polynom av grad n (d: a_n og $b_n \neq 0$) slik at $q(\alpha) = 0$ så vil også polynomet $p(x) - \frac{a_n}{b_n} q(x)$ som er av höyst $(n-1)$'te grad ha α som rot. Det betyr etter minimalegenskapen til n at dette polynomet er nullpolynomet og $q(x) = \frac{b_n}{a_n} p(x)$. Dette entydig bestemte tallet n kaller vi graden av α over F og også graden av $F(\alpha)$ over F. Som en viktig konsekvens av betraktningene ovenfor har vi i det algebraiske tilfellet följende

Sats 32. La $F(\alpha)$ være en enkel algebraisk utvidelse av F av grad n. Da kan ethvert element $\beta \in F(\alpha)$ skrives entydig som et polynom av grad høyst $n-1$, $\beta = a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}$ med $a_i \in F$. Med disse polynomene regner man som med restklasser i $F[x]$ modulo $p(x)$.

Bevis: Vi så ovenfor at $F(\alpha) = F[\alpha]$ slik at et element i $F(\alpha)$ er av formen $f(\alpha)$ hvor $f \in F[x]$. Ifölge Sats 24 kan vi skrive $f(x) = q(x)p(x)+r(x)$ hvor graden av $r(x)$ er $< n$. Innsetting av $x = \alpha$ i denne identiteten gir $f(\alpha) = r(\alpha)$. Entydigheten följer slik: Er $\beta = a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1} = b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}$ vil $(a_{n-1}-b_{n-1})\alpha^{n-1}+\ldots+(a_0-b_0) = 0$ som medförer $a_i = b_i$ for alle i siden α ikke kan være nullpunkt for noe polynom over F av grad mindre enn n.

To utvidelser K_1 og K_2 av F sies å være ekvivalente (eller F-isomorfe) hvis det finnes en isomorfi av K_1 på K_2 hvor ethvert element i F avbildes på seg selv. Om ekvivalente utvidelser har vi följende

Sats 33. To enkle transendente utvidelser av en kropp F er alltid ekvivalente. Hvis α og β er nullpunkter i ett og samme irreduktible polynom $p(x)$ over F, vil de to enkle algebraiske utvidelser $F(\alpha)$ og $F(\beta)$ være ekvivalente. Vi kan her finne en isomorfi som förer ethvert element i F over i seg selv og α over i β.

Bevis: Ifölge Sats 31 er en enkel transendent utvidelse av F isomorf med kroppen $F(x)$ av alle rasjonale uttrykk i en ubestemt x og med koeffisienter fra F. Vår eneste "frihet" består her bare i hva vi vil kalle den ukjente. Kaller vi den ukjente henholdsvis x og y får vi en entydig bestemt isomorfi mellom $F(x)$ og $F(y)$ ved å la ethvert element i F gå over i seg selv og x gå over i y.

Dernest det algebraiske tilfellet. Elementene i $F(\alpha)$ og $F(\beta)$ har henholdsvis formene

$$(1) \qquad \sum_{i=0}^{n-1} a_i\alpha^i \quad \text{og} \quad \sum_{i=0}^{n-1} b_i\beta^i$$

og det er lett å se at avbildningen

$$\sum_{i=0}^{n-1} a_i\alpha^i \longrightarrow \sum_{i=0}^{n-1} a_i\beta^i$$

er en isomorfi som oppfyller betingelsene i satsen. I virkeligheten er dette like opplagt som i det transendente tilfellet. For hvis α er et

vilkårlig nullpunkt i det irreduktible polynomet $p(x)$ vil vi alltid ha isomorfien $F(\alpha) \cong F[x]/(p(x))$ og her inngår ikke α i det hele tatt på höyre side - bare $p(x)$ slik at det også her bare er spörsmål om hva vi vil kalle et nullpunkt i $p(x)$. Om vi kaller det α eller β er hipp som happ, i alle tilfeller regner vi med summene (1) som med polynomer modulo $p(x)$.

Vi har i det foregående under betraktningen av utvidelse av kropper hele tiden forutsatt at alle utvidelsene skjedde innenfor en fast kropp K m.h.p. en underkropp F. Eksistensen av en enkel utvidelse $F(\alpha)$ med $\alpha \in K$ var da umiddelbart innlysende idet $F(\alpha)$ er snittet av alle underkropper i K som inneholder F og α. Det erimidlertid av prinsipiell interesse å kunne frigjöre oss fra denne forutsetningen om at det hele foregår innenfor en på forhånd gitt K. Dette er mulig fordi vi kan vise at om F og et irreduktibelt polynom $p(x) \in F[x]$ er gitt kan vi eksplisitt konstruere oss en overkropp K som inneholder et element α slik at $p(\alpha) = 0$. Dermed vil vi ha konstruert en K som inneholder både F og α og eksistensen av $F(\alpha)$ vil være sikret som för. Vi merker oss imidlertid at vi her har en ny problemstilling. Istedet for at F og α er gitt slik som i det "konkrete" tilfellet ovenfor hvor alt foregår innenfor en på forhånd gitt K - er det i det andre tilfellet F og et irreduktibelt polynom $p(x) \in F[x]$ som er gitt og en söker en overkropp K av F slik at $p(x) = 0$ har en lösning $\alpha \in K$. (Såkalt "symbolsk adjunksjon". Vi beviser nå eksistensen av en slik K

Sats 34. La F være en gitt kropp. Da finnes det for det förste en enkel transendent utvidelse av F. Dernest hvis $p(x)$ er et irreduktibelt polynom over F finnes det en enkel algebraisk utvidelse $F(\alpha)$ til F slik at $p(\alpha) = 0$. Både i det transendente og i det algebraiske tilfellet er den enkle utvidelsen entydig på en ekvivalens nær. (Ekvivalensbegrepet er definert ovenfor.)

Bevis: Det transendente tilfellet er opplagt. Her representerer kroppen $F(x)$ av alle rasjonale uttrykk i et bokstav x med koeffisienter fra F en enkel transendent utvidelse og vi har sett at to slike utvidelser $F(x)$ og $F(y)$ er ekvivalente. La så $p(x)$ være et irreduktibelt polynom i $F[x]$. Vi har sett at om F har en enkel algebraisk utvidelse $F(\alpha)$ innenfor en gitt K med α rot i $p(x) = 0$ så må nödvendigvis $F(\alpha) = F[x]/(p(x))$. Vår oppgave blir derfor å vise at $F[x]/(p(x))$ - helt uavhengig av noen $K \supseteq F$ - virkelig er en enkel

algebraisk utvidelse av F generert av en rot i $p(x) = 0$. Det første - nemlig at $F[x]/(p(x))$ er en utvidelse av F (d.v.s. inneholder en underkropp isomorf med F) ser vi slik: Avbildningen $F \longrightarrow F[x]/(p(x))$ som avbilder et element $a \in F$ på den restklassen som det konstante polynomet a hörer til modulo $p(x)$ er tydeligvis en homomorfi av F inn i $F[x]/(p(x))$. Denne homomorfien er en isomorfi; for om $a \neq 0$ vil det tilsvarende polynomet (av nullte grad) ikke være med i den restklassen som representerer nullelementet i $F[x]/(p(x))$ for denne restklassen består av alle polynomer av formen $f(x)p(x)$ med $f(x) \in F[x]$. Vi kan derfor identifisere F med en viss underkropp av $F[x]/(p(x))$ og dermed betrakte kroppen $F[x]/(p(x))$ som en utvidelse av F. Det gjenstår bare å vise at likningen $p(x) = 0$ har en lösning α i $F[x]/(p(x))$ slik at vi får $F[x]/(p(x))$ identisk med den enkle algebraiske utvidelsen $F(\alpha)$. La oss kalle den restklassen i $F[x]/(p(x))$ som polynomet x ligger i for α. Av

$$p(x) = a_0+a_1x+\ldots+a_nx^n \in (p(x))$$

og av at avbildningen $F[x] \longrightarrow F[x]/(p(x))$ er en homomorfi följer at

$$\bar{a}_0+\bar{a}_1\alpha+\ldots+\bar{a}_n\alpha^n = \bar{0}$$

hvor $\bar{a}_i$ betegner billedet av $a_i \in F$ ved denne homomorfien. Men etter den identifikasjonen vi gjorde i förste del av beviset kan vi slöyfe strekene over a'ene og null slik at vi virkelig har $p(\alpha) = 0$. Entydighetsutsagnet i satsen er bevist i og med Sats 33.

Eksempel. Metoden ovenfor kan f.eks. brukes til å konstruere kroppen C av de komplekse tall utfra kroppen R av de reelle tall samt polynomet x^2+1. At polynomet x^2+1 er irreduktibelt over R kan vi se ved å bruke Eisensteins kriterium, idet en setter $x+1$ istedet for x og får polynomet x^2+2x+2 som faller inn under kriteriet. Irreduktibiliteten av x^2+1 er også direkte innlysende. Kaller vi den restklassen som x hörer til modulo x^2+1 for i får vi $R(i) = R[x]/(x^2+1$ og $R(i)$ blir her isomorf med "kroppen av de komplekse tall". Etter Sats 32 vet vi jo at et element i $R(i)$ kan skrives entydig på formen $a+ib$ siden i er av annen grad over R og en konstaterer lett at regning med lineæruttrykk $a+bx$ modulo x^2+1 foregår nöyaktig som regning med "komplekse tall". Når vi her bruker gåseöyne antyder vi at vi tenker oss at vi allerede har innfört kroppen C på en annen måte som tallpar (a,b), $a,b \in R$ med de vanlige regneregler (multiplikasjonen er f.eks. definert ved $(a,b)(c,d) = (ac-bd, ad+bc)$). Kaller vi

denne kroppen for C kan en også her bevise (se Theorem 2 s. 108 i [2]) at C inneholder en underkropp isomorf med R -nemlig parene av formen (a,0) og inneholder en rot i likningen $x^2+1 = 0$ (paret (0,1)) og det slik at C = R((0,1)). Disse to metodene til å utvide R til C er ekvivalente i den presise forstand som ble definert ovenfor.

17. Utvidelseskropper betraktet som vektorrom over grunnkroppen. Ved eksistenssatsen ovenfor (Sats 34) har vi sett at det i og for seg er unödvendig å postulere eksistensen av en overkropp K til F hvori alle enkle utvidelser av F skal foregå siden vi er i stand til å konstruere eksplisitt en slik K for hver enkel utvidelse. Hva angår algebraiske utvidelser som ikke er enkle, men hvor vi får med alle rötter i en likning f(x) = 0 med $f(x) \in F(x)$ skal vi senere bevise en liknende eksistenssats. For de betraktninger vi skal gjöre i det fölgende og som alle angår utvidelser av formen $F(\alpha_1 \ldots \alpha_n)$ hvor α'ene kan oppfattes som rötter i et polynom $f(x) \in F[x]$ - behöver vi derfor ikke ha noen skrupler med å tenke oss F som underkropp av en "stor" kropp hvori alle utvidelser foregår.

Om K er en utvidelseskropp til F kan K på triviell måte oppfattes som et vektorrom med skalarkropp F. Addisjonen er den addisjonen som allerede er gitt i K ogmultiplikasjon av en "skalar" $\in$ F med en "vektor" $\in$ K er den multiplikasjonen som allerede er definert i K. Det hele består altså i grunnen i at multiplikasjon av to elementer i differensmengden K-F ikke kommer i betraktning. Dette å betrakte en utvidelseskropp som et vektorrom over grunnkroppen er meget nyttig og leder straks til endel enkle, men viktige resultater. Först muliggjör denne betraktningen en generell definisjon av utvidelsers grad. Vi begrenser oss her til det endelige tilfellet.

Definisjon: La F være en kropp og K en utvidelseskropp til F. Hvis vektorrommet K over F har endelig dimensjon n sies K å være en endelig utvidelse av F av grad n og vi skriver n = [K:F]. Denne definisjonen har mening etter det Korollaret til Schreiers sats hvor vi fikk definert dimensjonen av et endeligdimensjonalt vektorrom. Det generelle gradbegrepet som er definert her er i overensstemmelse med det spesielle gradbegrepet som ble definert tidligere for enkle algebraiske utvidelser. Vi noterer dette som

Sats 35. Graden n av et element α som er algebraisk over F er lik dimensjonen av $F(\alpha)$ betraktet som vektorrom over F. $F(\alpha)$ har en basis som består av elementene $1, \alpha, \alpha^2 \ldots \alpha^{n-1}$.

Bevis: At α er algebraisk av n'te grad betyr at α er nullpunkt i et irreduktibelt polynom av grad n og vi vet at ethvert element i $F(\alpha)$ lar seg skrive entydig på formen $a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}$ med $a_i \in F$. Det betyr at $\{1,\alpha\ldots\alpha^{n-1}\}$ danner en basis for $F(\alpha)$ over F og at dimensjonen derfor er n.

Korollar. Hvis to elementer α og β som er algebraiske over F genererer samme (ɔ: ekvivalente) utvidelse $F(\alpha) \cong F(\beta)$ vil α og β ha samme grad over F.

Da vil jo $F(\alpha)$ og $F(\beta)$ ha samme dimensjon over F og graden av α må være lik graden av β etter Sats 35.

Vi har sett at en enkel algebraisk utvidelse er en endelig utvidelse (iflg. definisjonen ovenfor og Sats 35). Vi skal nå omvendt se at en endelig utvidelse av F bare består av elementer som er algebraiske over F:

Sats 36. Ethvert element α i en endelig utvidelse K av F er algebraisk over F og tilfredsstiller en irreduktibel likning over F av grad høyst n hvor $n = [K:F]$ er graden av den gitte utvidelsen.

Bevis: Siden vektorrommet K (over F) har dimensjon n vil de n+1 elementene $1,\alpha,\alpha^2,\ldots\alpha^n$ være lineært avhengige (ellers måtte de være en delmengde av en basis og det strider mot invariansen av dimensjonstallet n). ɔ: $b_0+b_1\alpha+\ldots+b_n\alpha^n = 0$ hvor $b_i \neq 0$ for minst én i. Men det betyr at α er algebraisk over F og av grad høyst n.

Som en direkte følge av Sats 35 og Sats 36 har vi følgende

Korollar. Ethvert element i en enkel algebraisk utvidelseskropp $F(\alpha)$ er algebraisk over F.

Vi skal så utlede noen enkle egenskaper ved suksessive endelige utvidelser.

Sats 37. Hvis elementene $\alpha_1,\ldots\alpha_n$ danner en basis for en endelig utvidelse K av F og $\beta_1,\ldots\beta_m$ danner en basis for en endelig utvidelse L av K vil de m·n produkter $\alpha_i\beta_j$ med $1 \leq i \leq n$, $1 \leq j \leq m$ danne en basis for L over F.

Bevis: Ethvert element $\beta \in L$ kan skrives på formen $\beta = \sum_{j=1}^{m} \gamma_j \beta_j$ hvor $\gamma_j \in K$. Disse γ_j kan i sin tur skrives på formen $\sum_{i=1}^{n} a_i\alpha_i$ med $a_i \in F$. Dette gir $\beta = \sum_{j=1}^{m} (\sum_{i=1}^{n} a_{ij}\alpha_i)\beta_j = \sum_{i,j} a_{ij}\alpha_i\beta_j$

og viser at produktene $\alpha_i\beta_j$ danner et sett av generatorer for vektorrommet L over F. Den andre egenskapen som er med å karakterisere en basis er at generatorene er lineært uavhengige. Av $\sum a_{ij}\alpha_i\beta_j = \sum_j (\sum_i a_{ij}\alpha_i)\beta_j = 0$ följer siden β'ene danner en basis over K at alle summene $\sum_i a_{ij}\alpha_i = 0$. Da α'ene danner en basis over F följer $a_{ij} = 0$ for alle i,j og dette viser at $\{\alpha_i\beta_j\}$ danner en basis for L over F.

Denne satsen har en rekke konsekvenser.

Korollar 1. Hvis K er en endelig utvidelse av F og L en endelig utvidelse av K vil L være en endelig utvidelse av F med grad $[L:F] = [L:K]\cdot[K:F]$.

Korollar 2. Hvis K er en endelig utvidelse av F med grad $[K:F] = n$ vil ethvert element $\alpha \in K$ være algebraisk og ha en grad som er en divisor av n.

Bevis: At α er algebraisk vet vi allerede fra Sats 36. Korollaret följer da direkte av formelen $[K:F] = [K:F(\alpha)]\cdot[F(\alpha):F]$ hvor siste faktor nettopp er graden til α over F

Istedet for $[F(\alpha):F]$ som altså er graden av α m.h.p. F skriver vi også $[\alpha:F]$.

Korollar 3. Et element α i en endelig utvidelse K av F genererer hele utvidelsen, d.v.s. $K = F(\alpha)$ hvis og bare hvis $[\alpha:F] = [K:F]$.

Bevis: Av $[K:F] = [\alpha:F][K:F(\alpha)]$ följer at $[\alpha:F] = [K:F]$ hvis og bare hvis $[K:F(\alpha)] = 1$ som er ensbetydende med $K = F(\alpha)$.

Korollar 4. Hvis $K = F(\alpha_1 \ldots \alpha_r)$ er en kropp generert av r elementer α_i slik at hver α_i er algebraisk over $F(\alpha_1 \ldots \alpha_{i-1})$ da er K en endelig utvidelse av F og ethvert element i K er derfor algebraisk over F.

Bevis: Hvert av gradtallene $[F(\alpha_1 \ldots \alpha_{i-1}\alpha_i):F(\alpha_1 \ldots \alpha_{i-1})]$ er endelig og ifölge Korollar 1 er derfor også $[K:F]$ endelig og ethvert element i K er algebraisk over F ifölge Sats 36.

18. Et par anvendelser på algebraiske tall og konstruksjonsproblemer (kubens fordobling). För vi går videre i den generelle teorien skal vi först gjöre et par anvendelser av det vi allerede har utledet. Vi begynner med noen bemerkninger om algebraiske tall. Et algebraisk tall α er et komplekst tall (f.eks. oppfattet på en av de to måtene som

er beskrevet på side som tilfredsstiller en likning $a_n\alpha^n+a_{n-1}\alpha^{n-1}+\ldots+a_0 = 0$ hvor alle a_i er rasjonale tall. Med andre ord et algebraiske tall er et komplekst tall som er algebraisk over kroppen Q av de rasjonale tall. På grunnlag av det vi har vist om algebraiske utvidelser kan vi gi enkle beviser for et par fundamentale satser om algebraiske tall.

Sats 38. Mengden av algebraiske tall danner en kropp.

Bevis: Vi trenger å vise at sum, differens, produkt og kvotient (med nevner $\neq 0$) av to algebraiske tall α, β igjen er et algebraisk tall. Men alle disse operasjonsresultatene er inneholdt i underkroppen $Q(\alpha,\beta)$ av C. Siden α er algebraisk over Q og β algebraisk over Q og derfor også over $Q(\alpha)$ vil $Q(\alpha,\beta)$ etter Korollar 4 være en endelig utvidelse av Q og derfor ifölge Sats 36 bare inneholde algebraiske tall.

Vi sier generelt at en kropp F er algebraisk avsluttet (eller algebraisk komplett) dersom ethvert polynom med koeffisienter i F har minst ett nullpunkt i F. Dette medförer umiddelbart at alle nullpunktene er i F ved å bruke Korollar 2 til Sats 24 som samtidig viser at over en algebraisk avsluttet kropp kan ethvert polynom spaltes i lineærfaktorer (og det på entydig måte). Det finnes i dette tilfellet ikke andre irreduktible polynomer enn de som er av förste grad. At F er algebraisk avsluttet betyr at det ikke finnes andre algebraiske utvidelser av F enn F selv. Det såkalte "algebraens fundamentalteorem" sier at kroppen C av komplekse tall er algebraisk avsluttet. Dette er ganske overraskende når vi tenker på hvorledes C er fremkommet, nemlig ved en eneste algebraisk adjunksjon av en rot i den spesielle likningen $x^2+1 = 0$. Satsen sier at adjunksjon av en hvilken som helst rot i en annen likning med reelle koeffisienter - ja til og med komplekse - ikke förer til noe "nytt". Betegnelsen "algebraens fundamentalteorem" er uheldig (van der Waerden foreslår betegnelsen "fundamentalsatsen for læren om de komplekse tall"). Ved å bruke Liouvilles sats fra funksjonsteorien kan en gi et ytterst kort og elegant bevis for satsen slik at vi like godt kan ta det med her.

Sats 39. ("Algebraens fundamentalteorem") Kroppen C av de komplekse tallene er algebraisk avsluttet.

Bevis: La $f(z)$ være et polynom som ikke har noe komplekst nullpunkt. Da vil $\frac{1}{f(z)}$ være en holomorf funksjon i hele det komplekse z-plan

som holder seg begrenset når $|z| \to \infty$. Etter Liouvilles sats er da $\frac{1}{f(z)}$ en konstant og $f(z)$ må derfor selv være en konstant. Dette beviser satsen.

Med de rent algebraiske midler vi har utviklet i det foregående kan vi imidlertid bevise den følgende

Sats 40. Kroppen A av de algebraiske tall er algebraisk avsluttet.

Bevis: La $x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_0 = 0$ være en likning med koeffisienter $\alpha_i \in A$. Over kroppen Q av de rasjonale tall genererer disse koeffisientene en kropp $K = Q(\alpha_0, \alpha_1 \ldots \alpha_{n-1})$ som p.g.a. Korollar 4 til Sats 37 er en endelig utvidelse av Q. En kompleks rot β i den gitte likning er algebraisk over K slik at $K(\beta)$ er en endelig utvidelse av K. Etter første del av Korollar 1 til Sats 37 vil da $K(\beta)$ være en endelig utvidelse av Q og β er algebraisk over Q, d.v.s. β er et algebraisk tall.

Vi skal nå se at Sats 37 har en konsekvens som ligger til grunn for umuligheten av "kubens fordobling". Det er følgende

Sats 41. La $p(x)$ være et irreduktibelt polynom av 3dje grad over en kropp F og la K være en utvidelse av F av grad 2^m. Da vil $p(x)$ også være irreduktibelt over K.

Bevis: Anta at $p(x)$ var reduktibel over K. Siden $p(x)$ er av tredje grad betyr det at $p(x)$ har minst en lineær faktor som hörer til $K[x]$ eller med andre ord at K inneholder en rot α i $p(x) = 0$. Etter Korollar 2 til Sats 37 förer dette til likningen $2^m = 3 \cdot [K:F(\alpha)]$ hvilket er umulig og $p(x)$ er derfor irreduktibel over K.

Sats 41 viser at en irreduktibel tredje-gradlikning ikke kan löses ved suksessive adjunksjoner av kvadratrötter. For et visst antall slike kvadratrotsadjunksjoner vil alltid lede til en utvidelse av grad 2^m og en slik utvidelse kan etter det vi nettopp har sett ikke inneholde noen rot av en irreduktibel tredje-grads likning.

I problemet om kubens fordobling gjelder det med passer og linjal å konstruere en kubus med dobbelt så stort volum som en gitt kubus. Vi skal antyde beviset for umuligheten av dette. La oss anta at den gitte kubus har sidekant av lengde 1. Konstruksjonen skal foregå i et plan slik at det som er gitt er altså et kvadrat med sidekant 1. De tall (= lengder) som er gitt umiddelbart i og med dette kvadratet er tallene 1 og $\sqrt{2}$. Kaller vi kroppen av de rasjonale tall for Q har vi derfor til å begynne med bare störrelser som hörer til

kroppen $Q(\sqrt{2})$. Det er nå mulig å vise at ved å anvende passer og linjal (etter bestemte foreskrevne regler) kan en bare oppnå å konstruere störrelser (lengder) som hörer til en kvadratisk utvidelse av den kroppen av störrelser en tidligere hadde. Dette kommer selvfölgelig av at likningen for en sirkel (som svarer til bruk av passeren) er av annen grad og at likningen for en rett linje (som svarer til bruk av linjalen) er av förste grad. Skjæringspunkter (og lengder mellom skjöringspunkter) for sirkler og rette linjer vil derfor alltid bli uttrykt rasjonalt eller ved bruk av kvadratrötter. Gjentatt bruk av passer og linjal vil derfor bare lede til störrelser som hörer til en utvidelse av grad 2^m over grunnkroppen Q. Men siden volumet av den gitte kubus er 1 gjelder det å konstruere en sidekant x slik at $x^3 = 2$. Etter Eisensteins kriterium er likningen $x^3-2 = 0$ irreduktibel og den kan derfor etter Sats 41 ikke ha noen rot i en utvidelse av grad 2^m. Dette viser umuligheten av kubens fordobling. For en fullstendigere behandling av dette problemet og andre konstruksjonsproblemer henviser vi til [5] og L. Weisner: Introduction to the theory of equations. N.Y. 1938. (Se også T. Nagell Lärobok i algebra. Uppsala 1949.)

19. Rotkroppen til en algebraisk likning. Vi skal nå studere utvidelser av F som fremkommer ved å adjungere alle rötter i en algebraisk likning $f(x) = 0$, $f \in F[x]$. Vi har fölgende

Definisjon. En utvidelse N av F kalles for rotkroppen til et polynom $f \in F[x]$ hvis f kan skrives som et produkt av lineærfaktorer $f(x) = \beta(x-\alpha_1)\ldots(x-\alpha_n)$ i N og $N = F(\alpha_1 \ldots \alpha_n)$.

Bemerkning. Mer presist burde vi i definisjonen sagt "en rotkropp" istedet for "rotkroppen" i bestemt form - men definisjonen rettferdiggjöres ved at vi for gitt F og f kan bevise at det bare finnes en N med de to gitte egenskaper. Vi nöyer oss forelöpig med å bevise eksistensen av en rotkropp N med de to gitte egenskaper.

Sats 42. Ethvert polynom f over en gitt F har en rotkropp.

Bevis: Vi tilbakeförer dette eksistensbeviset til eksistensbeviset for enkle algebraiske utvidelser. Vi bruker induksjon med hensyn på graden til f. For et polynom av förste grad vil F være en rotkropp til F og satsen er i orden i det tilfellet. Anta nå at satsen er riktig for en vilkårlig kropp F og for alle polynomer over F av grad n-1 og anta at polynomet f(x) av n'te grad har en irreduktibel faktor

$p(x)$. Etter Sats 34 eksisterer det da en enkel algebraisk utvidelse $K = F(\alpha_1)$ generert av en rot α_1 i $p(x) = 0$. Innenfor K har derfor også $f(x) = 0$ roten $x = \alpha_1$ og vi kan etter Sats 24, Korollar 2 skrive $f(x) = (x-\alpha_1)g(x)$ (oppspalting med koeffisienter fra K!). Her er $g(x)$ et polynom av grad $n-1$ og det eksisterer da etter induksjonsantagelsen en rotkropp N over K generert av de $n-1$ rötter $\alpha_2 \ldots \alpha_n$ i $g(x)$: $N = K(\alpha_2, \alpha_3, \ldots, \alpha_n)$ eller $N = F(\alpha_1)(\alpha_2 \ldots \alpha_n) = F(\alpha_1 \ldots \alpha_n)$ som viser at N er en rotkropp til f over F.

Sats 42 kan brukes til å bevise en ytterligere eksistenssats. Nemlig at enhver kropp har en algebraisk avsluttet utvidelse. Vi har tidligere sett at både kroppen Q av de rasjonale tall og kroppen R av de reelle tall tillater en slik algebraisk avsluttet utvidelse; nemlig kroppen C av de komplekse tall. Q tillot dessuten en mindre algebraisk avsluttet utvidelse ved kroppen A av de algebraiske tall. Eksistensbeviset for generelle kropper F er enkelt når F har karakteristikk p idet en bruker Sats 42. (Se [2] s.410-411). Beviset i det generelle tilfellet bruker utvalgsaksiomet i form av Zorns lemma (eller transfinit induksjon).

På en måte kan vi si at en rotkropp N til polynomet $f(x) \in F[x]$ er en minimal overkropp til F som inneholder alle f's rötter. Er nemlig K en utvidelse av en slik rotkropp N så kan vi ikke ha $f(\alpha) = 0$ for $\alpha \in K-N$. For $f(x) = \beta(x-\alpha_1)\ldots(x-\alpha_n)$ er lik null bare når $x = \alpha_1, \ldots, \alpha_n$.

§ 4. Galois-teori.

20. Den Galoiske gruppen til en rotkropp: Ved en automorfisme forstår en generelt en isomorf avbilding av et algebraisk system (gruppe, ring, kropp etc.) på seg selv. For at en en-entydig avbildning φ av kroppen K på seg selv skal være en automorfisme er det nok at $\varphi(a+b) = \varphi(a)+\varphi(b)$ og $\varphi(ab) = \varphi(a)\cdot\varphi(b)$. Dette medförer asom en lett kan verifisere at $\varphi(0) = 0$, $\varphi(e) = e$, $\varphi(a-b) = \varphi(a)-\varphi(b)$ og $\varphi(ab^{-1}) = \varphi(a)(\varphi(b))^{-1}$, spesielt $\varphi(b^{-1}) = (\varphi(b))^{-1}$. Innenfor kroppen av de komplekse tall vil f.eks. avbildningen φ definert ved $\varphi(a+ib) = a-ib$ være en automorfisme. Hvis φ_1 og φ_2 begge er automorfismer av K på K vil den sammensatte avbildningen $\varphi_1\varphi_2$ definert ved $(\varphi_1\cdot\varphi_2)(a) = \varphi_2(\varphi_1(a))$ også definere en automorfisme

i K, likeså avbildningen φ^{-1}, definert ved at $\varphi^{-1}(a) = b$, dersom $a = \varphi(b)$ og φ er en automorfisme. Det er tydelig at med disse definisjonene vil mengden av alle automorfismer i K danne en gruppe G(K) hvor enhetselementet er den automorfismen som avbilder ethvert element i K på seg selv. Hvis $F \subseteq K$ kan vi betrakte den undermengden av den fulle automorfismegruppen til K som består av alle de automorfismer i K som lar elementene i F invariant i den forstand at $\varphi(a) = a$ for alle $a \in F$. Denne automorfismemengden danner tydeligvis en undergruppe av den fulle automorfismegruppen til K og vi kaller denne undergruppen for automorfismegruppen til K over F. Vi kan passende betegne den med G(K,F). En ser lett at den fulle automorfismegruppen G(K) til K også kan oppfattes på denne måten, idet G(K) = G(K,P) hvor P er primkroppen i K. Om e er enhetselementet i K er jo $\varphi(e) = e$ og derfor også $\varphi(ne) = ne$ slik at alle elementer i primkroppen er invariante overfor en vilkårlig automorfisme i K. Idet vi sier at to elementer i K er konjugerte over F når de begge er nullpunkter i samme irreduktible polynom over F har vi følgende

Sats 43. La K være en endelig utvidelse av F og $\varphi \in G(K,F)$. Da vil for et vilkårlig element $\alpha \in K$ de to elementene α og $\varphi(\alpha)$ være konjugerte over F.

Bevis: Ifölge Sats 36 er α algebraisk over F og er nullpunkt i et (entydig) irreduktibelt polynom $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ med $a_i \in F$ d: $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Siden $\varphi(a_i) = a_i$ og forövrig bevarer alle rasjonale relasjoner vil også $\varphi(\alpha)^n + a_{n-1}\varphi(\alpha)^{n-1} + \ldots + a_0 = 0$ som viser at $p(\varphi(\alpha)) = 0$ og dermed at α og $\varphi(\alpha)$ er konjugerte.

Definisjon. La $N = F(\alpha_1 \ldots \alpha_n)$ være rotkroppen til et polynom f(x) over F. Vi kaller da gruppen G(N,F) for den Galoiske gruppen til likningen f(x) = 0 eller også Galois-gruppen til rotkroppen N over F.

Bemerkning. I denne definisjonen har vi stilltiende antatt at rotkroppen N er entydig bestemt på en ekvivalens nær. Denne entydigheten vil imidlertid först bli bevist i Sats 46.

Vi beviser först en sats som viser at den Galoiske gruppen alltid kan identifiseres med en viss gruppe av permutasjoner i mengden av de forskjellige röttene til f(x) i N. Når vi bruker uttrykket mengden av forskjellige rötter så er det ikke noe annet enn mengden av röttene - vi vil bare være sikker på at det er klart at en dobbeltrot som f.eks.

1 i $(x-1)^2 = 0$ ikke skal telle to ganger. Da har vi

Sats 44. La $f(x)$ være et polynom av n'te grad som har nöyaktig k forskjellige rötter i en rotkropp $N = F(\alpha_1 \ldots \alpha_k)$. Da vil enhver automorfisme i Galois-gruppen $G(N,F)$ bestemme en permutasjon $\alpha_i \leftrightarrow \varphi(\alpha_i)$ av de forskjellige röttene til $f(x)$ og omvendt vil automorfismen φ være entydig bestemt ved den permutasjonen den bevirker i denne mengden av forskjellige rötter i $f(x)$.

Bevis: La $\varphi \in G(N,F)$. Det följer da av Sats 43 at φ avbilder en rot i $f(x)$ på en rot i $f(x)$ og siden φ er en-entydig avbilder den forskjellige rötter på forskjellige rötter. φ bevirker altså en permutasjon av mengden $\{\alpha_1 \ldots \alpha_k\}$ av de forskjellige röttene i $f(x)$ og denne permutasjonen er ikke noe annet enn φ's restriksjon til denne mengden. Omvendt vil vi om φ er en automorfisme kunne rekonstruere virkningen av φ på et vilkårlig element $\alpha \in K$ utfra kjenskapet til $\varphi(\alpha_i)$ for alle röttene α_i. For $\alpha \in F(\alpha_1 \ldots \alpha_k)$ vil kunne skrives som et polynom $\alpha = g(\alpha_1 \ldots \alpha_k)$ i de k störrelsene $\alpha_1 \ldots \alpha_k$ med koeffisienter fra F. (Vi bruker her identiteten $F(\alpha) = F[\alpha]$ k ganger) og vi får siden φ er en automorfisme at $\varphi(\alpha) = g(\varphi(\alpha_1) \ldots \varphi(\alpha_k))$ som viser at $\varphi(\alpha)$ er bestemt ved kjenskapet til $\varphi(\alpha_i)$, $1 \leq i \leq k$. Dette viser at om to automorfismer i $G(N,F)$ er forskjellige må deres restriksjoner til $\{\alpha_1 \ldots \alpha_k\}$ også være forskjellige og altså gi opphav til forskjellige permutasjoner i mengden $\{\alpha_1 \ldots \alpha_k\}$. Dette viser

Korollar 1. Den Galoiske gruppen til en likning $f(x) = 0$ er isomorf med en undergruppe av permutasjonsgruppen til mengden av (de forskjellige) röttene til $f(x)$.

Vi sier her uttrykkelig undergruppe. Enhver permutasjon av röttene trenger ikke å være restriksjon av en φ i $G(N,F)$.

Korollar 2. Den Galoiske gruppen til en likning av n'te grad har en orden som er en divisor i $n!$

Bevis: La k være antall av forskjellige rötter. Da vil $k \leq n$ og $k! \mid n!$. Ordenen av den fulle permutasjonsgruppen til $\{\alpha_1 \ldots \alpha_k\}$ er $k!$ og siden $G(N,F)$ er isomorf med en undergruppe av denne vil ordenen av $G(N,F)$ være divisor i $k!$ og dermed også i $n!$

Eksempel. Etter Eisensteins kriterium vet vi at likningen $p(x) = x^4 - 3 = 0$ er irreduktibel over kroppen Q av de rasjonale tallene. Likningen har de 4 forskjellige röttene $x = re^{i\varphi}$; $\varphi = 0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi$

og $r = \sqrt[4]{3}$ = den reelle positive fjerderoten av 3. Når $i = \sqrt{-1}$ kan vi skrive röttene som r, ir, -r og -ir. Rotkroppen til polynomet x^4-3 over Q er altså kroppen $Q(r, ir, -r, -ir) = Q(r,i)$. Som en ser av dette eksemplet behöver ikke (selv i det irreduktible tilfellet) generator-mengden $\alpha_1 \ldots \alpha_n$ i $F(\alpha_1 \ldots \alpha_n)$ være "minimal", slik at vi ikke kan stryke noen av α'ene (eller m.a.o. erstatte den med en annen mindre mengde). Rotkroppen kan altså i dette tilfellet tenkes å fremkomme ved to suksessive enkle algebraiske utvidelser. Först utvider vi Q til Q(r), dernest Q(r) til Q(r,i). Vi har her en situasjon $F \subseteq K \subseteq L$ som den som er beskrevet i Sats 37. Utvidelsen Q(r) er av fjerde grad over Q siden r tilfredsstiller en irreduktibel likning av fjerde grad over Q. Som vektorrom over Q kan vi velge $\{1, r, r^2, r^3\}$ som basis (Sats 35). Q(r) inneholder bare reelle tall og inneholder derfor ikke i. Utvidelsen fra Q(r) til Q(r,i) kan derfor ikke være av förste grad. Men den er av annen grad siden i tilfredsstiller $x^2+1 = 0$ aom har koeffisienter fra Q og dermed fra Q(r). (x^2+1 vedblir å være irreduktibel over Q(r)). Denne siste utvidelsen har derfor som vektorrom over Q(r) basisen $\{1,i\}$. Etter Sats 37 får vi derfor at produktmengden $\{1, r, r^2, r^3\}\{1,i\} = \{1, r, r^2, r^3, i, ir, ir^2, ir^3\}$ danner en basis for rotkroppen Q(r,i) som vektorrom over Q og graden av utvidelsen Q(r,i) over Q er derfor 8. Siden ethvert element kan skrives som en lineærkombinasjon av disse elementene med koeffisienter fra Q vil en automorfisme φ i den Galoiske gruppen være fullstendig kjent om vi kjenner $\varphi(r)$ og $\varphi(i)$. Utfra dette er det relativt enkelt å bestemme den Galoiske gruppen G(N,F) fullstendig i dette tilfellet og en finner at G(Q(r,i),Q) er en gruppe med 8 elementer. For en fullstendig gjennomgåelse av dette eksemplet henviser vi til Birkhoff & Mac Lane s. 415-16. Vi noterer her bare den ting at ordenen til den Galoiske gruppen G(Q(r,i),Q) er lik graden av utvidelsen Q(r,i) over Q. Vi skal senere vise at dette er spesialtilfelle av en generell sats.

21. Separable og inseparable polynomer. Vi har ovenfor definert begrepet rotkropp over F med hensyn på et polynom f og den tilhörende Galoiske gruppe. For å få en pen teori kan vi imidlertid ikke la polynomet f være helt vilkårlig. Det finnes nemlig kropper F med karakteristikk p hvor et irreduktibelt polynom f av grad n over F har færre enn n rötter i den tilhörende rotkroppen. Anderledes uttrykt: elementet α kan være algebraisk av n'te grad over F, men ha færre enn n konjugerte. Dette forhold kan som vi skal se ikke opp-

tre når F har karakteristikk 0, men vi kan finne eksempler på det når F har karakteristikk p. Her er et eksempel: La P(u) betegne en enkel transendent utvidelse av restklasse-kroppen P modulo primtallet p, og la F være underkroppen $P(u^p)$ av P(u) generert av elementet $t = u^p$ (som også er transendent over P). Over F er imidlertid u algebraisk idet u der tilfredsstiller $f(x) = x^p - t = 0$. Vi påstår at f er irreduktibel over F. Var f reduktibel ville den ifölge Gauss lemma allerede være reduktibel over P[t] (kvotientkroppen til denne ringen er jo P(t)) og en eventuell oppspalting ville ha formen $x^p - t = g(x,t) \cdot h(x,t)$. Vi kan imidlertid også se på denne dekomposisjonen som en oppspalting av $x^p - t$ som et lineært polynom i t siden g og h $\in P[x][t]$ $(= P[t][x])$. Men et lineært polynom er irreduktibelt og g eller h må være en enhet i P[t][x], d.v.s. et element i P. Dette viser irreduktibiliteten av $x^p - t$ - nå som polynom i P[t][x]. Men denne irreduktible likningen av p'te grad har bare en rot i P(u) til tross for at den kan dekomponeres fullstendig i lineærfaktorer innenfor P(u): $x^p - u^p = (x-u)^p$ (Sats 30).

Definisjon. Et polynom f(x) av grad n med koeffisienter fra F er separabelt over F hvis f har n forskjellige rötter i en passende rotkropp N over F. Ellers sier vi at f er ineparabelt over F. En utvidelse K = F sies å være separabel over F hvis ethvert element i K er rot i et separabelt polynom over F (dette er ensbetydende med at det irreduktible polynom $\in F[x]$ som $\alpha \in K$ tilfredsstiller er separabelt over F).

Vi skal utlede et enkelt kriterium for separabilitet ved å bruke begrepet formell derivert av et polynom. La $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ være et polynom over F. Med den formelle deriverte av f(x) forstår vi polynomet $\delta f(x) = a_1 + 2a_2 x + \ldots + na_n x^{n-1}$ hvor ka som vanlig betegner $a+a+\ldots+a$, k ganger. Hvis F er kroppen R av reelle tall er denne rent formelle definisjonen i overensstemmelse med differensialregningens derivasjonsbegrep. Vi kan her rent algebraisk utfra definisjonen ovenfor bevise regler fra differensialregningen som

$$\delta(f+g) = \delta(f) + \delta(g); \quad \delta(fg) = f \cdot \delta g + \delta f \cdot g, \quad \delta(f^m) = mf^{m-1} \cdot \delta f .$$

Det er bare direkte å bruke definisjonen av δ. Vi kan nå bevise

Sats 45. La f(x) være et polynom over F. La d(x) være den störste felles divisor av f(x) og $\delta f(x)$ (d(x) er entydig bestemt når vi tenker oss at koeffisienten foran den höyeste potensen er 1). Hvis d(x) = 1 er f(x) separabel, ellers er f(x) inseparabel.

Bevis: Etter Sats 42 har vi til f og F en rotkropp N hvori f kan spaltes i lineærfaktorer $f(x) = \beta(x-\alpha_1)^{s_1}\cdots(x-\alpha_k)^{s_k}$. $\alpha_i \neq \alpha_j$ Hvis vi deriverer f formelt ser vi at δf blir en sum av k-1 ledd som alle har $(x-\alpha_1)^{s_1}$ som faktor og et k'te ledd $\beta \cdot s_1(x-\alpha_1)^{s_1-1}(x-\alpha_2)^{s_2}\cdots(x-\alpha_k)^{s_k}$. Med andre ord hvis $s_1 > 1$ vil $(x-\alpha_1)$ gå opp i δf mens den ikke vil gjöre det hvis $s_1 = 1$. Gjör vi det samme med $s_2, \ldots s_k$ ser vi at f og δf alltid har en felles faktor unntatt når $s_1 = s_2 = s_k = 1$. Men dette siste er ekvivalent med separabilitet siden det bare er i dette tilfelle at f har så mange rötter (i N) som graden til f angir. Dette beviser Sats 45.

Korollar 1. Et irreduktibelt polynom er separabelt hvis dets formelle deriverte er forskjellig fra null.

Bevis: Hvis $f(x)$ er irreduktibel vil $(f(x), \delta f(x)) = 1$ unntatt når δf er et multiplum av $f(x)$ og siden graden av $\delta f(x)$ er mindre enn graden av $f(x)$ kan dette bare inntreffe når $\delta f = 0$.

Korollar 2. Ethvert irreduktibelt polynom over en kropp med karakteristikk null er separabelt.

Bevis: Följer av Korollar 1 idet förste ledd $na_n x^{n-1}$ er forskjellig fra null siden $na_n \neq 0$ for alle n og $a_n \neq 0$ i en kropp med karakteristikk null.

Av dette korollaret följer at enhver endelig utvidelse av en kropp med karakteristikk null er separabel i den forstand som ble definert ovenfor.

22. Rotkropper og Galois-grupper for separable polynomer. Vi skal begynne dette avsnittet med å vise tre lemmaer som handler om utvidelse av isomorfier.

Lemma 1. La φ være en isomorfi mellom de to kroppene F og F'. Til et irreduktibelt polynom $p(x) \in F[x]$ svarer det da entydig et irreduktibelt polynom $p'(x) \in F'[x]$ ved at korresponderende koeffisienter i $p(x)$ og $p'(x)$ går over i hverandre ved isomorfien. Hvis $F(\alpha)$ og $F'(\alpha')$ er enkle utvidelser ved rötter α og α' i henholdsvis $p(x)$ og $p'(x)$ vil φ kunne utvides til en isomorfi φ^* mellom $F(\alpha)$ og $F'(\alpha')$ slik at $\alpha' = \varphi^*\alpha$.

Bevis: Dette er i grunnen ikke annet enn det vi allerede har vist i Sats 33. For utvidelsen φ^* er gitt eksplisitt ved likningen

$$\varphi^*(a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}) = a_0'+a_1'\alpha'+\ldots+a_{n-1}'\alpha'^{n-1}$$

når $a_i' = \varphi(a_i)$, $\alpha' = \varphi(\alpha)$ og n er graden av α over F.

Lemma 2. La isomorfien φ mellom F og F' overføre polynomet $f(x)$ i polynomet $f'(x)$ og la $N \supseteq F$ og $N' \supseteq F'$ være rotkroppen over F og F' til henholdsvis f og f'. Da kan isomorfien utvides til en isomorfi mellom N og N'.

Bevis: Vi beviser dette ved induksjon m.h.p. graden $m = [N:F]$. For $m = 1$ er lemmaet opplagt idet vi har $F = N$ og φ er allerede utvidet til N. La så $m > 1$ og anta at lemmaet er riktig for alle rotkropper N av grad $< m$ over en vilkårlig F. Siden $m > 1$ ligger ikke alle f's rötter i F og vi må ha minst én irreduktibel faktor $p(x)$ i $f(x)$ som har grad $d > 1$. La α være en rot av $p(x)$ i N og la $p'(x)$ være det polynomet over F' som svarer til $p(x)$ ved isomorfien φ ($p'(x)$ vil da være en faktor i $f'(x)$). Rotkroppen N' inneholder en rot α' av $p'(x)$ og etter Lemma 1 kan φ utvides til en isomorfi φ^* mellom $F(\alpha)$ og $F'(\alpha')$ slik at $\varphi^*(\alpha) = \alpha'$.

Siden N er rotkropp til f over F er den også rotkropp til f over $F(\alpha)$, men graden av den siste utvidelsen er m/d. På samme måte er N' rotkropp til f' over $F'(\alpha')$ og induksjonsantagelsen gir at φ^* kan utvides fra $F(\alpha)$ til N og lemmaet er bevist.

Lemma 3. Hvis polynomet f i Lemma 2 er separabelt kan isomorfien utvides til N på nöyaktig $m = [N:F]$ forskjellige måter.

Bevis: På samme måte som i Sats 43 vet vi at en utvidet isomorfi vil overføre en rot α i den irreduktible faktoren $p(x)$ av $f(x)$ i en rot α' i den tilsvarende irreduktible faktoren $p'(x)$ av $f'(x)$. Om graden av $p(x)$ som ovenfor er d vil utvidelsen av φ fra F til $F(\alpha)$, kunne foregå på d forskjellige måter, idet vi kan definere $\varphi(\alpha) = \alpha'$ og dette gir nöyaktig d muligheter siden $p'(x)$ har d forskjellige rötter når $f'(x)$ er separabel over F.

Vi anvender igjen induksjon. Tilfellet $m = 1$ er opplagt og hvis Lemmaet gjelder for alle utvidelser med $[N:F] < m$ vil vi ha at de d isomorfiene hver for seg kan utvides på $[N:F(\alpha)] = m/d$ forskjellige måter til hele N. I det hele får vi da $d \cdot \frac{m}{d}$ utvidelser av φ til hele N.

Av disse lemmaene följer nå flere ting. For det förste entydigheten av rotkroppen N til et gitt polynom f over F:

Sats 46. To rotkropper N og N' til et polynom f over F er ekvivalente over F.

Bevis: At N og N' er ekvivalente over F betyr pr. definisjon at vi har en isomorfi φ mellom N og N' slik at $\varphi(a) = a$ for alle $a \in F$. Dette er nå en direkte følge av Lemma 2, idet vi ifølge dette lemmaet kan utvide den identiske avbildningen av F på F til en isomorfi mellom N og N' og denne isomorfien blir en ekvivalens over F.

Sats 47. Ordenen av Galois-gruppen $G(N,F)$ til et separabelt polynom er lik graden $[N:F]$ av rotkroppen til f over F.

Bevis: Dette er et spesialtilfelle av Lemma 3 idet vi setter $F = F'$ og $N = N'$. Her gir en mulig utvidelse av den identiske automorfismen i F til hele N nettopp en automorfisme i $G(N,F)$ og omvendt gir en automorfisme i $G(N,F)$ en utvidelse av den identiske automorfismen i F. Denne korrespondansen mellom utvidelser av den identiske automorfismen i F og automorfismer i Galois-gruppen $G(N,F)$ er tydeligvis en-entydig og satsen følger av Lemma 3.

Sats 48. La N være rotkroppen til et separabelt polynom over F og anta at $\alpha \in N$ er slik at $\varphi(\alpha) = \alpha$ for enhver $\varphi \in G(N,F)$. Da er $\alpha \in F$.

Denne satsen sier at det er ikke andre elementer i N som er invariante overfor alle automorfismer i Galois-gruppen til et separabelt polynom enn de som er i F.

Bevis: La K være den undermengden av N som består av alle de elementer som overföres i seg selv ved enhver automorfisme i $G(N,F)$. En konstaterer lett at K er en kropp som inneholder F. N blir også rotkropp til f over K og det er klart at $G(N,F) \cong G(N,K)$. Av dette og Sats 47 följer at $[N:F] = [N:K]$ og det betyr at $K = F$. (For er $K \neq F$ blir $[K:F] > 1$ og likningen $[N:F] = [N:K][K:F]$ blir uforenlig med $[N:F] = [N:K]$.)

Vi skal også benytte lemmaene ovenfor til å gi en karakterisering av selve rotkroppene.

Definisjon. En endelig utvidelse N av F sies å være normal over F hvis ethvert irreduktiblet polynom over F som har en rot i N kan spaltes i et produkt av lineærfaktorer i N.

Sats 49. En endelig utvidelse av F er normal over F hvis og bare hvis den er rotkroppen til et eller annet polynom over F.

Bevis: Anta först at N er normal over F og la α være et element i differensmengden $N-F$ (hvis $N = F$ er satsen i orden). Da vil α tilfredsstille en irreduktibel likning $p_1(x) = 0$ og siden N er normal over F vil N inneholde alle röttene i $p_1(x)$ og dermed også hele rotkroppen M til polynomet $p_1(x)$. Hvis $M \neq N$ vil et element $\beta \in N-M$ tilfredsstille en irreduktibel likning $p_2(x) = 0$ over F og av samme grunn som för vil den större rotkroppen til $p_1(x) \cdot p_2(x)$ være inneholdt i N. Siden graden av N over F er endelig kan vi tydeligvis holde på med disse utvidelsene til vi får frem N som rotkroppen til et polynom $p_1(x) \cdot p_2(x) \cdots p_k(x)$. Anta omvendt at N er rotkroppen til polynomet $f(x)$ over F, men at N ikke er normal over F. Da finnes det et irreduktibelt polynom $p(x)$ over F som har én, men ikke alle rötter i N. (Med at $p(x)$ ikke har alle rötter i N mener vi at $p(x)$ ikke kan spaltes i lineærfaktorer i N. En ser lett at dette er ekvivalent med at rotkroppen til $p(x)$ over F ikke er ekvivalent med noen overkropp av F som er inneholdt i N.) Dette betyr at $p(x)$'s oppspaltning i irreduktible faktorer innen N inneholder minst en lineærfaktor og minst et polynom $q(x)$ av grad ≥ 2. La denne oppspaltningen være $p(x) = (x-\alpha) \cdots q(x)$ slik at $\alpha \in N$ og $q(x)$ er irreduktibel over N og av grad ≥ 2. La α' være en rot i $q(x) = 0$. Egentlig danner vi her kroppen $N' = N(\alpha') = N[x]/(q(x))$ ved symbolsk adjunksjon. Men siden α' også er rot i $p(x) = 0$ innenfor N' får vi $F(\alpha) \cong F(\alpha')$ og da N er rotkroppen til f over F og dermed også over $F(\alpha)$ og N' er rotkroppen til f over $F(\alpha')$, får vi av Lemma 2 at isomorfien $F(\alpha) = F(\alpha')$ kan fortsettes til en isomorfi mellom N og N'. Denne isomorfien er en ekvivalens over F og vi må derfor ha $[N:F] = [N':F]$. Men dette strider mot at N' er en virkelig utvidelse av N og vi har oppnådd den önskede motsigelse.

Av förste del av beviset følger

Korollar. Enhver endelig normal og separabel utvidelse av F er rotkroppen til et passende valgt separabelt polynom over F.

23. Symmetriske polynomer. För vi går over til å bevise hovedsatsen i den Galoiske teorien, skal vi först gjöre en anvendelse av Galoisgruppene på symmetriske polynomer. Et polynom $g(x_1 \cdots x_n)$ sies å være symmetrisk om det går over i seg selv ved en vilkårlig premutasjon av x'ene.

Sats 50. La $N = F(\alpha_1 \cdots \alpha_n)$ være rotkroppen til et separabelt polynom $f(x)$ av n'te grad, over F og la $g(x_1 \cdots x_n)$ være et symmetrisk

polynom over F. Da vil elementet $\alpha = g(\alpha_1 \cdots \alpha_n)$ ligge i grunnkroppen F.

Bevis: Fra Sats 44 vet vi at en automorfisme φ i Galois-gruppen G(N,F) forårsaker en permutasjon $\alpha_i \to \varphi\alpha_i$ av röttene i f(x). Symmetrien av $g(x_1 \cdots x_n)$ medförer derfor at $\alpha = g(\alpha_1 \cdots \alpha_n)$ går over i $g(\varphi(\alpha_1), \cdots \varphi(\alpha_n)) = g(\alpha_1 \cdots \alpha_n) = \alpha$ ved enhver $\varphi \in G(N,F)$. Ifölge Sats 48 betyr det at $\alpha \in$ F.

En direkte følge av denne satsen er en litt svekket utgave av hovedsatsen om symmetriske polynomer som sier at ethvert symmetrisk polynom (over F) kan skrives som en hel rasjonal funksjon (= polynom) i de såkalte elementære symmetriske polynomer definert ved

$$\sigma_1 = x_1 + x_2 + \cdots + x_n, \quad \sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \cdots \quad \sigma_n = x_1x_2 \cdots x_n .$$

Av satsen ovenfor får en i förste omgang bare at et symmetrisk polynom kan skrives som en rasjonal funksjon av σ'ene og ikke som en hel rasjonal funksjon.

Sats 51. Ethvert polynom over F som er symmetrisk i de n ubestemte $x_1 \cdots x_n$ kan skrives som en rasjonal funksjon av de n tilsvarende elementære symmetriske funksjoner $\sigma_1 \cdots \sigma_n$.

Bevis: Vi betrakter de to transendente utvidelsene $K = F(\sigma_1, \cdots \sigma_n)$ og $N = F(x_1 \cdots x_n)$ av F. Vi har $F \subseteq K \subseteq N$ og en ser at N er algebraisk over K siden generatorene $x_1 \cdots x_n$ til N er rötter i likningen

$$f(x) = (x-x_1)(x-x_2)\cdots(x-x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n = 0$$

og $f(x) \in K[x]$. N er altså rotkroppen til det separable polynomet f over K. La så $g(u_1 \cdots u_n)$ være et vilkårlig symmetrisk polynom i n variable over F. Polynomet g kan selvfölgelig også betraktes som et symmetrisk polynom over den större kroppen K og om vi i $g(u_1 \cdots u_n)$ innsetter röttene $x_1 \cdots x_n$ i det separable polynomet f(x) over K får vi etter Sats 50 et element $g(x_1 \cdots x_n)$ som tilhörer $K = F(\sigma_1 \cdots \sigma_n)$ og g er derfor en rasjonal funksjon av σ'ene som påstått.

24. Hovedsatsen i den Galoiske teorien. Vi beviser först følgende sats for generelle kropper:

Sats 52. La N være en kropp, H en endelig gruppe av automorfismer i N og K den underkropp av N som består av alle elementer i N som er invariante overfor enhver automorfisme i H. Da vil graden $[N:K]$ av utvidelsen N over K være endelig og mindre eller lik ordenen av H.

Bevis: Hvis ordenen av H er n må vi vise at enhver mengde av $n+1$ forskjellige elementer $c_1, c_2, \ldots c_{n+1}$ i N er lineært avhengige over K. Utfra de n automorfismene $\varphi \in H$ får vi et likningssystem av n homogene lineære likninger

$$(1) \qquad \varphi(c_1)y_1 + \varphi(c_2)y_2 + \ldots + \varphi(c_{n+1})y_{n+1} = 0$$

Vi vet fra teorien for lineære likninger at et slikt system av n homogene likninger i $n+1$ ukjente alltid har en lösning forskjellig fra den trivielle lösningen $y_1 = y_2 = y_{n+1} = 0$. Vi kan derfor tenke oss at vi velger tallet $m \leq n+1$ som det minste hele tall slik at likningssystemet

$$(2) \qquad \varphi(c_1)y_1 + \ldots + \varphi(c_m)y_m = 0 \; ; \qquad \varphi \in H$$

også har en slik lösning forskjellig fra null-lösningen. Denne lösningen består av elementer $y_1 \ldots y_m \in N$ og er entydig på en multiplikativ konstant faktor nær. For hvis det var to ikke-proporsjonale lösninger ville en passende lineærkombinasjon av dem gi en lösning $\neq$ null-lösningen av et tilsvarende system med $m-1$ likninger imot minimalegenskapen til m. Vi antar nå $y_1 = e$ = enhetselementet i N og fastlegger dermed lösningen helt entydig. Vi anvender nå en vilkårlig automorfisme $\psi \in H$ på likningssystemet (2) og får da om vi setter $\psi\varphi = \varphi'$ likningssystemet:

$$\varphi' c_1(\psi y_2) + \ldots + \varphi' c_m(\psi y_m) = 0$$

Men dette likningssystemet i de variable ψy_i er nöyaktig det samme som (2) idet $\varphi' = \psi\varphi$ gjennomlöper alle automorfismer i H én og kun én gang når φ gjör det samme. Derfor er $\psi y_1, \ldots \psi y_m$ også en lösning av (2) og ifölge entydigheten må vi ha $\psi y_i = k y_i$ for alle i med $k \in N$. Men siden vi har fastlagt $y_1 = e$ og ψ er en automorfisme må $\psi y_1 = e$ samtidig som $\psi y_1 = ke = k$, d.v.s. $k = e$. Av dette följer $\psi y_i = y_i$ for alle i og enhver $\psi \in H$. Det betyr ifölge definisjonen på K at $y_i \in K$ og likningen (2) med φ = identitetsautomorfismen viser den lineære avhengigheten.

Sats 53. (Hovedsatsen i den Galoiske teori). La N være rotkroppen til det separable polynomet $f(x) \in F[x]$ og $G = G(N,F)$ den tilhörende Galoiske gruppe. Det er da en-entydig korrespondanse mellom undergruppene til G og de underkroppene K til N som inneholder F ($F \subseteq K \subseteq N$). Hvis K er gitt består den tilsvarende undergruppe

H = H(K) av alle de automorfismer i G som lar ethvert element i K invariant. Omvendt hvis H er gitt, består den tilsvarende kroppen K = K(H) av alle de elementer i N som er invariante under enhver automorfisme i H. For hver K er gruppen H(K) den Galoiske gruppen til N over K og dens orden er lik graden $[N:K]$ av N over K.

Bevis: Det gjelder å vise at den avbildningen $K \to H(K)$ som er beskrevet eksplisitt i satsen er en en-entydig avbildning av mengden av kropper K som tilfredsstiller $F \subseteq K \subseteq N$ på mengden av alle undergrupper til $G = G(N,F)$. For det förste er det etter definisjonen av H(K) klart at H(K) er en undergruppe av G. Kroppen N er en rotkropp til f over K. Etter slik H(K) er definert er det derfor klart at den er den Galoiske gruppen til N over K. Sats 47 sier da at ordenen av H(K) er lik graden til N over K. Dette er beviset for den siste setningen i satsen. Vi viser så en-entydigheten av $K \to H(K)$. Anta at $K_1 \neq K_2$ slik at vi har et element $\alpha \in K_1$, men $\alpha \notin K_2$. Sats 48 sier da at det finnes en automorfisme $\varphi \in H(K_2)$ slik at $\varphi(\alpha) \neq \alpha$. Det betyr at $\varphi \notin H(K_1)$ (siden $\alpha \in K_1$) og vi har $H(K_1) \neq H(K_2)$. Det gjenstår nå bare å vise at avbildningen $K \to H(K)$ er en avbildning på mengden av undergrupper i G, med andre ord at enhver undergruppe H av G er av formen H(K) for passende valgt K. Om H er en vilkårlig undergruppe av G skal vi vise at vi nettopp kan bruke den K(H) som er definert i satsen eller at vi med andre ord har H = H(K(H)). Dette viser da samtidig at $H \to K(H)$ er den inverse avbildningen til $K \to H(K)$. For å vise at H = H(K(H)) bemerker vi först at K(H) er en kropp slik at $F \subseteq K(H) \subseteq N$ og at vi etter Sats 52 har $[N:K(H)] \leq h$ hvor h er ordenen til H. Ved å sammenlikne definisjonene på H(K) og K(H) er det klart at $H \subseteq H(K(H))$. Nå vet vi ifölge Sats 47 at $[N:K(H)]$ er lik ordenen av H(K(H)). Dette sammen med ulikheten $[N:K(H)] \leq h$ ovenfor, viser at ordenen av H(K(H)) er mindre eller lik ordenen av H og dette medförer H = H(K(H)).

Kommentar. Det er denne en-entydige korrespondansen mellom "mellomkroppene" og undergruppene av den Galoiske grupen. som er essensen i den Galoiske teorien. Ved denne korrespondansen blir en rekke spörsmål om kropper og om de likninger $f(x) = 0$ som definerer rotkroppene tilbakeförte til spörsmål om undergrupper av den Galoiske gruppen. Suksessen ved den Galoiske teorien beror nettopp på at disse siste spörsmålene vanligvis er langt lettere å besvare enn de tilsvarende direkte spörsmålene om kroppene. Som et eksempel på en egenskap for

mellomkroppene som "reflekteres" i en tilsvarende egenskap hos de korresponderende gruppene, kan nevnes at K er en normal utvidelse av F hvis og bare hvis den tilsvarende undergruppen $H(K)$ er en normal (invariant) undergruppe av den Galoiske gruppen $G(N,F)$. (Se Sats 69.) Vanligvis overförer en terminologien fra gruppeteorien på kroppsutvidelser idet en f.eks. snakker om henholdsvis abelske og sykliske utvidelser hvis den tilsvarende Galois-gruppe er abelsk eller syklisk.

Vi skal nå gå over til anvendelser av den foregående generelle teori. Först skal vi bruke det vi har utledet om rotkropper til å bestemme de viktigste egenskapene ved endelige kropper. Senere skal vi bruke den egentlige Galois-teorien (Sats 53) til å vise "ulösbarheten" av 5te-grads-likningen.

25. Endelige kropper. Siden en kropp med karakteristikk 0 inneholder en primkropp isomorf med kroppen av de rasjonale tall og derfor er uendelig må en endelig kropp F ha karakteristikk p og F kan betraktes som en endelig utvidelse av sin primkropp P_p. (Det kan jo ikke finnes flere lineært uavhengige elementer over P_p enn antallet av elementer i hele F og det er endelig). La oss anta at F har basisen $\alpha_1, \ldots \alpha_n$ over P_p, d.v.s. ethvert element i F kan skrives entydig på formen $\sum_{i=1}^{n} a_i \alpha_i$; $a_i \in P_p$. Siden koeffisienten foran α_i kan velges på p måter finnes det i alt p^n elementer i F. Vi har dermed bevist

Sats 54. Antallet av elementer i en endelig kropp er alltid en potens av kroppens karakteristikk, altså en primtallpotens.

Vi skal så undersöke om det kan finnes flere forskjellige endelige kropper med samme antall elementer. Følgende sats viser at dette ikke er tilfelle.

Sats 55. To endelige kropper med like mange elementer er isomorfe.

Bevis: I en endelig kropp med $q = p^n$ elementer vil elementene $\neq 0$ danne en multiplikativ gruppe av orden $q-1$. Ordenen til ethvert element i denne gruppen må være en divisor i $q-1$ og alle elementene $\neq 0$ i F vil tilfredsstille likningen $x^{q-1} = e$. Alle elementene $a_1 \ldots a_q$ i F inkludert 0 vil tilfredsstille likningen $x^q - x = 0$. Etter Sats 24, Korollar 2 vil derfor produktet $(x-a_1)\ldots(x-a_q)$ være en divisor av x^q-x. Men siden $(x-a_1)\ldots(x-a_q)$ også er av grad q og har höyeste koeffisient 1 må vi ha

$$x^q - x = (x-a_1)\ldots(x-a_q)$$

Dette viser at F er rotkroppen til $x^q-x(=ex^q-ex)$ over P_p. Enhver annen endelig kropp F' med q elementer vil på samme måte være rotkroppen til polynomet $e'x^q-e'x$ hvor e' er enhetselementet i F'. Vi har nå en isomorfi mellom primkroppen P_p i F og primkroppen P'_p i F' (som bl.a. overförer e i e'). Etter Lemma 2 i 22. kan denne isomorfien utvides til en isomorfi mellom F og F' og satsen er dermed bevist.

De to satsene ovenfor innskrenker muligheten for dannelsen av endelige kropper. Antallet av elementer i en endelig kropp må være en primtallpotens p^n og det finnes höyst èn kropp med p^n elementer. At vi ikke kan foreta noen videre innskrenkning viser følgende

Sats 56. Til ethvert primtall p og ethvert positivt helt tall n eksisterer det en endelig kropp med $q = p^n$ elementer - nemlig rotkroppen til det separable polynomet x^q-x over P_p.

Bevis: Polynomet x^q-x og dets formelle deriverte $qx^{q-1}-1 = -1$ har 1 som störste felles divisor. Etter Sats 45 er derfor x^q-x separabel over P_p og har q forskjellige rötter i den tilsvarende rotkropp N. Sum og differens av to rötter er igjen en rot. For etter Sats 30 har vi $(a\pm b)^p = a^p\pm b^p$ i en kropp med karakteristikk p og $a^{p^n} = a$ og $b^{p^n} = b$ medförer derfor $(a\pm b)^{p^n} = a^{p^n}\pm b^{p^n} = a\pm b$. Produktet ab vil også være rot i $x^q-x = 0$ når a og b er det siden $(ab)^{p^n} = a^{p^n}\cdot b^{p^n} = ab$. Likedan for kvotienten. De q röttene i likningen $x^q-x = 0$ danner derfor en underkropp til rotkroppen N og siden denne underkroppen inneholder alle röttene til polynomet x^q-x må den være identisk med rotkroppen N. Eksistensen av rotkroppen N (Sats 42) gir derfor også eksistensen av en kropp med $q = p^n$ elementer.

Vi skal så bestemme strukturen av den multiplikative gruppen i en endelig kropp.

Sats 57. Hvis F er en endelig kropp vil den multiplikative gruppen $F^* = F-\{0\}$ være en syklisk gruppe.

Bevis: Vi har sett at ethvert element i F^* tilfredsstiller likningen $x^{q-1} = e$ hvor q er antall elementer i F. For å vise at F^* er syklisk må vi finne en såkalt primitiv $(q-1)$'te enhetsrot i F^*, d.v.s. et element a slik at vi ikke har $a^n = e$ for $n < q-1$. Vi skal nå konstruere et slikt element. La $q-1 = p_1^{n_1}\cdots p_k^{n_k}$ være primtalloppspaltingen av q-1. For enhver p_i, $(1 \leq i \leq k)$ har vi $p_i^{n_i} \mid q-1$ slik at röttene i $x^{p_i^{n_i}} = e$ også er rötter i $x^{q-1} = e$ og siden denne siste likningen har alle sine q-1 forskjellige rötter i

F må $x^{p_i^{n_i}} = e$ ha $p_i^{n_i}$ forskjellige rötter i F. Likedan vil $x^{p_i^{n_i-1}} = e$ ha $p_i^{n_i-1}$ forskjellige rötter i F. Siden $p_i^{n_i-1} < p_i^{n_i}$ må det derfor finnes et element $a_i \in F$ slik at $a_i^{p_i^{n_i}} = e$, men $a_i^{p_i^{n_i-1}} \neq e$. I en gruppe vil ethvert n slik at $a^n = e$ være et multiplum av den entydig bestemte minimale $m > 0$ slik at $a^m = e$. Dette tallet m kalles ordenen til a. Derfor vil $p_i^{n_i}$ være ordenen til elementet a_i. Vi påstår nå at ordenen til elementet $a = a_1 \circ a_2 \circ \ldots \circ a_k$ er q-1 slik at a virkelig er en (q-1)'te enhetsrot. Siden $a^{q-1} = e$ er det nok å vise at $a^{\frac{q-1}{p_i}} \neq e$ for $1 \leq i \leq k$. Vi har $a^{\frac{q-1}{p_i}} = a_1^{\frac{q-1}{p_1}} \ldots a^{\frac{q-1}{p_i}} \ldots a_k^{\frac{q-1}{p_k}}$. Her er den i'te faktoren $\neq e$ og alle de andre lik e slik at $a^{\frac{q-1}{p_i}} \neq e$.

Sats 58. I enhver endelig kropp F med p^n elementer vil avbildningene $\varphi_i : a \longrightarrow a^{p^i}$ for $1 \leq i \leq n$ gi n forskjellige automorfismer som utgjör den Galoiske gruppen til F over primkroppen P. Denne Galoiske gruppen G(F,P) er syklisk med automorfismen $\varphi_1 : a \longrightarrow a^p$ som generator.

Bevis: At avildningene $\varphi_i : a \longrightarrow a^{p^i}$ gir homomorfismer av F inn i F fölger direkte av likningene $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ og $(ab)^{p^i} = a^{p^i} b^{p^i}$. Om $a^{p^i} = b^{p^i}$ vil $a^{p^i} - b^{p^i} = (a-b)^{p^i} = 0$ og $a = b$. Dette viser at φ_i er en-entydig og siden F er endelig er φ_i en avbildning av F på F slik at φ_i virkelig er en automorfisme i F. To forskjellige i med $1 \leq i \leq n$ definerer forskjellige automorfismer. For om elementet a er generatoren til den sykliske gruppen F^* (Sats 57) vil $\varphi_i(a) = a^{p^i}$ og $\varphi_j(a) = a^{p^j}$ være forskjellige elementer i F når $1 \leq j < i \leq n$. Av $a^{p^i} = a^{p^j}$ fölger nemlig $a^{p^i - p^j} = e$ som er umulig siden ordenen av a er q-1. Siden F er rotkroppen til det separable polynomet $x^q - x \in P[x]$ vil etter Sats 47 ordenen av G(F,P) være lik $[F:P]$. Men da F har p^n elementer må $[F:P] = n$ (se beviset for Sats 54) og vi kan ikke ha andre automorfismer i F enn de n vi allerede har angitt eksplisitt. Og av den eksplisitte formen ser vi at de alle er potenser av $\varphi_1 : a \longrightarrow a^p$ slik at G(F,P) er den sykliske gruppen av orden n.

Tallteoretiske anvendelser. Om vi bruker de utledede satser om endelige kropper på restklassekroppen modulo p ($\supset : P_p$) får vi frem

endel enkle satser fra tallteorien (ved å oversette likheter i P_p til kongruenser i Z).

1. En kongruens $a_o x^n + \ldots + a_n \equiv 0 \pmod{p}$ har höyst n lösninger i x. Dette er forövrig ikke noe som er spesielt knyttet til endelige kropper. Det följer av at en likning av n'te grad ikke kan ha mer enn n lösninger i noen kropp.

2. Fermats sats: $a^{p-1} \equiv 1 \pmod{p}$ når $p \nmid a$.

Fermats sats kan sees som en konsekvens av flere av de generelle satsene om endelige kropper som vi har utledet. Vi har f.eks. sett at alle elementer i P_p er rötter i likningen $x^p - x = 0$. Vi har altså $a^p \equiv a \pmod{p}$ som gir $a^{p-1} = 1 \pmod{p}$ når $p \nmid a$. Satsen kan også sees som en direkte følge av Sats 57. Det Sats 57 forövrig gir er följende:

3. Hvis p er et gitt primtall kan vi finne et naturlig tall a slik at ethvert helt tall som ikke er delelig med p er kongruent med en passende potens av a modulo p.

4. Vi har sett at elementene i den endelige kroppen med $q = p^n$ elementer nettopp er mengden av rötter i likningen $x^q - x = 0$. Röttene i $x^{q-1} - e = 0$ utgjör derfor nettopp mengden av elementer $\neq 0$ og når disse betegnes som $a_1 \ldots a_{q-1}$ har vi derfor oppspaltingen

$$x^{q-1} - e = \prod_{i=1}^{q-1} (x - a_i).$$

I tilfellet $n = 1$ hvor v identifiserer kroppen med restklassekroppen modulo p får vi Wilsons sats når vi setter $x = 0$

$$(p-1)! \equiv 1 \pmod{p}.$$

<u>26. Enhetsrötter og sirkeldelingskropper</u>. Vi så at en endelig kropp F med $q = p^n$ elementer alltid kan betraktes som rotkroppen til restklassekroppen modulo p (d: kroppen $Z/(p)$) med hensyn på polynomet $x^{q-1} - e$. Dette er et spesialtilfelle av en type kropper som spiller en viktig rolle i den Galoiske teorien og forövrig spesielt for problemet å konstruere med passer og linjal en regulær n-kant (d: dele en sirkel i n like store deler). De kroppene vi sikter til er de såkalte sirkeldelingskropper som vi nå skal definere.

La F være en kropp og la det naturlige tallet n være slik at karakteristikken til F ikke går opp i n. Hvis F har karakteristikk null kan n være vilkårlig. Rotkroppen N til polynomet $x^n - e$ kaller

vi en sirkeldelingskropp over F og röttene i x^n-e kaller vi n'te enhetsrötter over F. Den formelle deriverte av $f(x) = x^n$-e er $\delta f(x) = nx^{n-1}$ som etter betingelsen om at n ikke er delelig med karakteristikken til F - ikke kan ha noen ikke-triviell felles faktor med f(x). Etter Sats 45 er derfor $f(x) = x^n$-e separabel over F og har n forskjellige rötter i N.

Sats 59. Mengen av n'te enhetsrötter - for en fast n som ikke er delelig med karakteristikken - danner en multiplikativ syklisk gruppe E_n av ordenen n.

Bevis: At de n'te enhetsröttene danner en gruppe under multiplikasjon er klart. At den er syklisk bevises ord for ord på samme måte som Sats 57.

Denne satsen beviser eksistensen av en såkalt primitiv n'te enhetsrot; d.v.s. et element $\varepsilon \in N$ slik at $\varepsilon^n = e$, men $\varepsilon^k \neq e$ når $1 \leq k < n$. Mengden av de n forskjellige n'te enhetsrötter er da $e, \varepsilon, \varepsilon^2, \ldots \varepsilon^{n-1}$. Forat ε^k skal være en primitiv n'te enhetsrot er det tydeligvis nödvendig og tilstrekkelig at $(k,n) = 1$ d.v.s. at k og n er innbyrdes primiske. Om φ betegner Eulers φ-funksjon finnes det derfor $\varphi(n)$ forskjellige primitive n'te enhetsrötter og disse danner sammen med e en undergruppe G_n av E_n som er isomorf med den undergruppen av den multiplikative semi-gruppen $Z/(n)$ som består av de restklasser som inneholder representanter relativt primiske med n.

Sats 60. La F ha en karakteristikk som ikke går opp i n. Da vil rotkroppen N til polynomet x^n-e ha en abelsk Galois-gruppe G(N,F) og denne er syklisk hvis n er et primtall.

Bevis: Om ε er en primitiv n'te enhetsrot har vi $N = F(\varepsilon)$ og om φ og ψ er to forskjellige automorfismer i G(N,F) må $\varphi(\varepsilon) \neq \psi(\varepsilon)$. Men siden ε er primitiv vil $\varphi(\varepsilon) = \varepsilon^{n_\varphi}$ med $1 \leq n_\varphi < n$ og vi får at $\varphi \rightarrow n_\varphi$ blir en en-entydig korrespondanse mellom G(N,F) og en viss undermengde av den multiplikative semigruppen $Z/(n)$. Denne korrespondansen er en isomorfi for $\varphi\psi(\varepsilon) = \varphi(\varepsilon^{n_\psi}) = (\varphi(\varepsilon))^{n_\psi} = \varepsilon^{n_\varphi \cdot n_\psi} (= \varepsilon^{n_\psi n_\varphi} = \psi\varphi(\varepsilon))$ og vi får dermed identifisert G(N,F) med en undergruppe av den abelske semigruppen $Z/(n)$. Om n er et primtall p vil de p-1 elementer i $Z/(p) - \{0\}$ danne en syklisk gruppe og G(N,F) kan identifiseres med en undergruppe av denne og blir da også selv syklisk etter Sats 9.

27. Konstruksjon av regulære n-kanter. Sirkeldelingskroppene har fått sitt navn fra problemet om å konstruere en regulær n-kant - eller med

andre ord å dele en gitt sirkel i n like store deler ved hjelp av passer og linjal. Vi skal nå kort antyde hvorledes teorien for disse kroppene kan brukes til å löse dette problemet; det vil si bestemme de n hvor konstruksjonen er mulig.

Vi lar nå grunnkroppen F være kroppen Q av de rasjonale tall. Vi har sett at det finnes $k = \varphi(n)$ primitive n'te enhetsrötter og når disse er $\zeta_1, \zeta_2, \cdots \zeta_k$ setter vi

$$\Phi_n(x) = (x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_n)$$

Dette polynomet kalles for sirkeldelingspolynomet (m.h.p. n) og en kan bevise at det er et polynom med hele rasjonale koeffisienter som er irreduktibelt over Q. (Beviset for dette er ikke særlig vanskelig og vi nöyer oss med å henvise til beviset i [5] s. 126 og s. 171 .) Sirkeldelingskroppen $Q(\varepsilon)$ $(\varepsilon = \zeta_1)$ svarende til polynomet x^n-e er derfor av grad $\varphi(n)$ over Q.

La oss nå betrakte problemet å dele en sirkel i n like store deler ved hjelp av passer og linjal. En ser umiddelbart av en figur at dette förer til konstruksjon av störrelsen

$$2\cos\frac{2\pi}{n} = \varepsilon + \varepsilon^{-1}$$

hvor altså ε er den primitive n'te enhetsroten $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Om vi bruker de samme betegnelsene som i hovedsatsen for den Galoiske teorien får vi at $H(Q(\varepsilon+\varepsilon^{-1}))$ bare består av de to automorfismene som er bestemt ved $\varepsilon \to \varepsilon$ og $\varepsilon \to \varepsilon^{-1}$. Enhver automorfisme i $G(Q(\varepsilon),Q)$ förer jo den primitive n'te enhetsroten ε over i en potens ε^k og dermed ε^{-1} over i ε^{-k} slik at $\varepsilon + \varepsilon^{-1}$ går over i $\varepsilon^k + \varepsilon^{-k}$ og denne störrelsen kan tydeligvis ikke være lik $\varepsilon + \varepsilon^{-1}$ uten at $k = 1$ eller $k = n-1$. (Dette sees lettest av en figur.) Etter Sats 53 er derfor $Q(\varepsilon)$ en utvidelse av annen grad over $Q(\varepsilon+\varepsilon^{-1})$ og siden $[Q(\varepsilon):Q(\varepsilon+\varepsilon^{-1})]\cdot[Q(\varepsilon+\varepsilon^{-1}):Q] = [Q(\varepsilon):Q] = \varphi(n)$ följer det at $Q(\varepsilon+\varepsilon^{-1})$ er en (reell) utvidelse av grad $\frac{\varphi(n)}{2}$ over Q. Siden konstruksjoner med passer og linjal bare förer til störrelser som ved adjunksjon til Q gir utvidelser med en grad som er en potens av 2 er det nödvendig og tilstrekkelig for konstruerbarheten av det reelle tallet $\varepsilon+\varepsilon^{-1}$ at $\frac{\varphi(n)}{2}$ og dermed også $\varphi(n)$ er en potens av 2. Vi kan få en mer eksplisitt betingelse om vi bruker formelen

$$(1) \qquad \varphi(n) = 2^{m-1}p_1^{m_1-1}\cdots p_r^{m_r-1}(p_1-1)\cdots(p_r-1)$$

hvor $n = 2^m p_1^{m_1} \cdots p_r^{m_r}$ er primtall-dekomposisjonen for tallet n. Her er $p_1, \cdots, p_r$ ulike primtall. Anvender vi den utledede betingelse på (1) får vi at n ikke må være delelig med kvadratet av noe ulike primtall og at enhver ulike primfaktor p_i i n må ha formen $p_i = 2^k+1$. Vi kan her til og med spesifisere k'en nærmere. Anta at $k = s \cdot t$ hvor s er et ulike tall > 1. Da vil $2^k+1 = (2^t)^s+1$ være delelig med 2^t+1 idet vi har identiteten $x^{2n+1}+1 = (x+1) \cdot (x^{2n}-x^{2n-1}+\cdots+x^2-x+1)$. Siden p_i er et primtall må derfor k være en potens av 2 og vi har derfor i det vesentlige bevist följgende

Sats 61. Den nödvendige og tilstrekkelige betingelse for at en sirkel kan deles i n like store deler ved hjelp av passer og linjal er at $\varphi(n)$ er en potens av 2. Dette er igjen ekvivalent med at n ikke er delelig med kvadratet av et ulike primtall, samtidig som enhver ulike primfaktor i n er av formen $p = 2^{2^m}+1$.

Av dette får vi blant annet muligheten av å konstruere 3-, 4-, 5-, 6-, 8- og 10-kanter. Videre viser satsen at 7-, 9-, 11- og 13-kanter er umulig å konstruere med passer og linjal. Skal det være mulig å konstruere en regulær p-kant hvor p er primtall må p være av formen $p = 2^{2^m}+1$. Dette gir f.eks. muligheten for å konstruere en regulær 17-kant. (En fullstendig algebraisk behandling av dette tilfellet finnes i [5] s. 176). Fermat trodde i sin tid at alle tallene av formen $2^{2^m}+1$ for $m = 0,1,2,3,\cdots$ var primtall. Dette er da også tilfellet for $m = 0,1,2,3$ og 4. Men Euler fant i 1732 at $2^{2^5}+1 = 641 \cdot 6700417$. (Ha-Ha!)

28. Endelige separable utvidelser er enkle. Det er en viktig sats om algebraiske utvidelser som i grunnen hörer hjemme på et tidligere stadium i teorien for kropputvidelser - men som vi hittil ikke har tatt med. Det er satsen om at enhver endelig separabel utvidelse av en kropp F er enkel, d.v.s. av formen $F(\alpha)$. Spesielt vil enhver rotkropp N til et separabelt polynom, slik vi har det i den Galoiske teorien være av formen $N = F(\alpha)$. Kjennskapet til denne satsen medförer imidlertid ikke noen vesentlig forenkling i beviset for selve hovedsatsen i Galois-teorien og vi har derfor valgt å gi en oppbygging av teorien som er uavhengig av denne satsen. Men satsen gir öket forståelse og også diverse forenklinger ved et mer inngående studium av korrespondansen $K \longrightarrow H(K)$. Vi skal derfor nå bevise denne satsen og anvende den til å bevise at K er en normal utvidelse av F hvis og bare hvis $H(K)$ er en normal (= invariant) undergruppe av den Galoiske gruppen $G(N,F)$.

Sats 62. La $F(\alpha_1, \cdots \alpha_n)$ være en endelig algebraisk utvidelse av F

hvor $\alpha_2, \alpha_3, \cdots \alpha_n$ er separable elementer over F. Da er $F(\alpha_1, \alpha_2, \cdots \alpha_n)$ en enkel utvidelse av F, d.v.s. det finnes et $\theta \in F(\alpha_1, \cdots \alpha_n)$ slik at $F(\theta) = F(\alpha_1, \cdots \alpha_n)$.

Bemerkning. At α er separabel over F betyr at α er rot i et irreduktibelt separabelt polynom over F. Merk at vi i satsen ikke krever at alle α_i er separable over F. Det er nok at n-1 av dem er det.

Bevis: Det er tilstrekkelig å bevise satsen for tilfellet $n = 2$. For om den er riktig for $n = 2$ og for $n = k-1 \geq 2$ har vi $F(\alpha_1, \cdots \alpha_{k-1}) = F(\beta)$ og $F(\alpha_1, \cdots \alpha_{k-1}, \alpha_k) = F(\beta, \alpha_k) = F(\theta)$ slik at den også gjelder for $n = k$. Om den gjelder for $n = 2$ gjelder den dermed for alle $n \geq 2$. Vi skal derfor vise at $F(\alpha, \beta) = F(\theta)$ for passende valgt $\theta \in F(\alpha, \beta)$ når β er separabel over F. La de irreduktible polynomer over F som α og β tilfredsstiller være $f(x)$ og $g(x)$. Vi betrakter så en overkropp K av F(f.eks. rot-kroppen til $f(x) \cdot g(x)$) hvor f og g kan spaltes i lineærfaktorer og hvor derfor f og g har alle sine nullpunkter - henholdsvis $\alpha_1, \cdots, \alpha_r$ og $\beta_1, \cdots, \beta_s$. Vi antar at numereringen er slik at $\alpha = \alpha_1$ og $\beta = \beta_1$. Vi kan anta at F inneholder uendelig mange elementer. For er F endelig vil $F(\alpha, \beta)$ være endelig og vi har $F(\alpha, \beta) = F(\theta)$ hvis θ er en generator for den multiplikative sykliske gruppen $F(\alpha, \beta) - \{0\}$ (Sats 57). Siden β er et separabelt element $\Rightarrow$ $g(x)$ er et separabelt polynom vil $\beta_k \neq \beta_1$ om $k \neq 1$ og likningen $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ har for ethvert i og ethvert $k \neq 1$ höyst en lösning innenfor F. Da de forskjellige valg av i og k bare gir et endelig antall likninger og F kan forutsettes uendlig må det finnes et element $c \in F$ slik at $\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$ for enhver i og enhver $k \neq 1$. Vi setter $\theta = \alpha_1 + c\beta_1 = \alpha + c\beta$ og påstår at θ har den önskede egenskap at $F(\alpha, \beta) = F(\theta)$. At vi har $F(\theta) \subseteq F(\alpha, \beta)$ er uten videre klart. Elementet β tilfredsstiller likningene $g(x) = 0$ og $f(\theta - cx) = 0$. Disse to polynomene $g(x)$ og $f(\theta - cx)$ har koeffisienter i $F(\theta)$ og har ikke andre felles rötter enn β siden $\theta - c\beta_k \neq \alpha_i$ for $k \neq 1$. Siden $g(x)$ er separabel er videre β en enkel rot i $g(x)$, d.v.s. vi har $(x-\beta)^t \nmid g(x)$ for $t \geq 2$. Dette betyr at $x - \beta$ er en största felles divisor for $f(\theta - cx)$ og $g(x)$ over $F(\theta)$ og da en slik största felles divisor også må ha sine koeffisienter fra $F(\theta)$ vil $\beta \in F(\theta)$. Av $\alpha = \theta - c\beta$ följer også $\alpha \in F(\theta)$ som beviser at $F(\alpha, \beta) = F(\theta)$ og dermed $F(\alpha, \beta) = F(\theta)$.

29. Galoiske utvidelser og mer om separable og normale utvidelser. En av de tingene vi vil nå frem til i dette avsnittet er å vise at alle de mellomkroppene K som opptrer i den Galoiske teorien er enkle utvidelser $K = F(\alpha)$ av grunnkroppen F. Vi skal se at det förer til en vesentlig forenkling ved studiet av disse mellomkroppene. Men for å kunne anvende Sats 62 må vi först vise at disse K'ene er separable utvidelser i den forstand som ble definert på s. 47. Forelöpig vet vi jo bare at det polynomet $f(x)$ som definerer rotkroppen N over F skal være separabelt, d.v.s. at röttene $\alpha_1, \alpha_2, \ldots \alpha_n$ i $f(x) = 0$ er separable elementer over F og ikke at ethvert element $\beta \in F(\alpha_1, \ldots \alpha_n)$ er rot i et irreduktibelt separabelt polynom over F slik som det kreves i definisjonen på en separabel utvidelse. Vi skal imidlertid vise at dette er tilfelle (Sats 64). Og vi skal gjöre det ved hjelp av en sats som samtidig viser at vi har en omvending av den viktige Sats 48. For å formulere denne satsen innförer vi följende

Definisjon. La K være en algebraisk utvidelse av F og la $G(K,F)$ betegne gruppen av alle automorfismer i K som lar ethvert element i F invariant. Vi sier da at K er en Galoisk utvidelse av F hvis det ikke er andre elementer i K enn de som er i F som er invariante under enhver automorfisme i $G(K,F)$.

Sats 63. Forat en endelig algebraisk utvidelse K av F skal være Galoisk er det nödvendig og tilstrekkelig at K er en normal og separabel utvidelse av F.

Bevis: Hvis K er en endelig, normal og separabel utvidelse av F vet vi etter korollaret til Sats 49 at K er rotkroppen til et passende valgt separabelt polynom over F. Vi kan derfor anvende Sats 48 som nettopp sier at K er en Galoisk utvidelse av F. Anta omvendt at det ikke er andre elementer i K som er invariante m.h.p. $G(K,F)$ enn de som er i F. Vi skal vise at K er en separabel og normal utvidelse av F eller med andre ord at det irreduktible $p(x)$ (med höyeste koeffisient lik e) som $\alpha \in K$ tilfredsstiller kan spaltes i lineærfaktorer innenfor K og at alle disse lineærfaktorene er forskjellige. La $\alpha_1, \alpha_2, \ldots \alpha_n$ være mengden av de forskjellige konjugerte til α som befinner seg i K (α selv er altså en av disse). Det vil med andre ord si at vi har en oppspalting $p(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\ldots(x-\alpha_n)^{k_n} \cdot q(x)$ innenfor $K[x]$ og det slik at $q(x)$ ikke kan skrives som et produkt innenfor $K[x]$ slik at en faktor er lineær. Fra Sats 44 vet vi at automorfismene i $G(K,F)$ permuterer

α'ene slik at

$$\prod_{i=1}^{n} (x-\alpha_i) = \prod_{i=1}^{n} (x-\varphi(\alpha_i)) \quad \text{når} \quad \varphi \in G(K,F)$$

Koeffisientene i polynomet $g(x) = \prod (x-\alpha_i) \in K[x]$ er derfor invariante overfor enhver $\varphi \in G(K,F)$ og må tilhöre F etter forutsetningen om at K er en Galoisk utvidelse av F. Siden $g(\alpha) = 0$ ($\alpha = \alpha_i$ for en eller annen i) må $g(x)$ være et multiplum av $p(x)$. (Se beviset for Sats 31.) Men da graden av $g(x)$ er mindre eller lik graden av $p(x)$ og begge polynomer har höyeste koeffisient lik e må vi ha $g(x) = p(x)$. Dette viser at $p(x)$ kan skrives som et produkt av lineærfaktorer innenfor $K[x]$ og at disse lineærfaktorene alle er forskjellige.

Sats 64. Rotkroppen til et separabelt polynom over F er en separabel utvidelse av F.

Bevis: Rotkroppen til et separabelt polynom over F er etter Sats 48 en Galoisk utvidelse av F og må derfor etter Sats 63 være en separabel utvidelse av F.

Sats 65. Alle mellomkroppene K som opptrer i den Galoiske teorien er enkle separable utvidelser av formen $K = F(\alpha)$.

Bevis: At mellomkroppene K er separable följer av Sats 64 og at de dermed er enkle utvidelser av grunnkroppen F följer av Sats 62.

Det er klart at Sats 65 forenkler studiet av mellomkroppene K i en vesentlig grad. Ved denne satsen får ethvert element i $K = F(\alpha)$ den oversiktlige basisfremstillingen $\beta = \sum_{i=0}^{n-1} a_i \alpha^i$ hvor n er graden av den irreduktible likning over F som α tilfredsstiller. Som eksempel på forenkling kan nevnes beviset for Lemma 3, s.49 og Sats 47 som sier at ordenen av Galoisgruppen $G(N,F)$ til et separabelt polynom er lik graden $[N:F]$ av N over F. Vi får her umiddelbart av $K = F(\alpha)$ at ordenen av gruppen av automorfismer $G(K,F)$ av en endelig separabel utvidelse er lik $[K:F]$. For om graden av α over F er n betyr det at $[K:F] = n$ og det finnes også nöyaktig n forskjellige automorfismer av K over F, nemlig de som er av formen

$$\varphi\left(\sum_{i=0}^{n-1} a_i \alpha^i\right) = \sum_{i=0}^{n-1} a_i (\varphi(\alpha))^i = \sum_{i=0}^{n-1} a_i \alpha'^i$$

hvor α' er en konjugert til α (d: rot i samme irreduktible likning som α tilfredsstiller over F).

Vi skal nå bruke Sats 65 til å vise at begreper som "normale utvidelser" og "konjugerte utvidelser" kan karakteriseres ved tilsvarende rent gruppeteoretiske egenskaper. Vi definerer under samme forutsetninger som i hovedsatsen i den Galoiske teorien to mellomkropper $K_1 = F(\alpha_1)$ og $K_2 = F(\alpha_2)$ som konjugerte dersom α_1 og α_2 er konjugerte over F, d.v.s. tilfredsstiller en og samme irreduktible likning over F. Vi har da først:

Sats 66. Mellomkroppen K er normal over F hvis og bare hvis den er identisk med alle sine konjugerte kropper.

Bevis: La $K = F(\alpha)$ være normal over F. Etter definisjonen på normalitet må enhver α_i som er konjugert til α höre til $F(\alpha)$ og derfor $F(\alpha_i) \subseteq F(\alpha)$. Men siden $F(\alpha_i)$ og $F(\alpha)$ er ekvivalente over F er også $F(\alpha_i)$ normal og vi får på samme måte $F(\alpha) \subseteq F(\alpha_i)$, d.v.s. $F(\alpha) = F(\alpha_i)$. Omvendt hvis $K = F(\alpha)$ er identisk med enhver $F(\alpha_i)$ hvor α_i er konjugert til α vil vi ha $K = F(\alpha_1, \ldots \alpha_n)$ hvor $\{\alpha_1, \ldots \alpha_n\}$ er mengden av konjugerte til α, ɔ: mengden av nullpunkter i det irreduktible polynom $p(x)$ som α tilfredsstiller over F. K er altså rotkroppen til $p(x)$ over F og derfor normal ifölge Sats 49.

Sats 67. Den Galoiske gruppen $H(K)$ til $K = F(\alpha)$ består av de $\varphi \in G(N,F)$ som er slik at $\varphi(\alpha) = \alpha$. To automorfismer i $G(N,F)$ förer α over i en og samme konjugert α' hvis og bare hvis de hörer til samme venstre-restklasse modulo $H(K)$.

Bevis: $\varphi \in H(K)$ medför at $\varphi(\alpha) = \alpha$ siden $\alpha \in K$. Omvendt vil $\varphi(\alpha) = \alpha$ gi $\varphi(\sum_{i=0}^{n-1} a_i \alpha^i) = \sum_{i=0}^{n-1} a_i (\varphi(\alpha))^i = \sum_{i=0}^{n-1} a_i \alpha^i$ slik at $\varphi(\beta) = \beta$ for enhver $\beta \in K$ og dermed $\varphi \in H(K)$. Anta så at φ og ψ overförer α i ett og samme konjugerte element ɔ: $\varphi(\alpha) = \psi(\alpha)$. Da vil $\psi^{-1}\varphi(\alpha) = \psi^{-1}\psi(\alpha) = \alpha$ og $\psi^{-1}\varphi \in H(K)$ eller $\varphi \in \psi \cdot H(K)$. Omvendt hvis $\varphi = \psi\sigma$ med $\sigma \in H(K)$ vil $\varphi(\alpha) = \psi\sigma(\alpha) = \psi(\alpha)$ siden $\sigma(\alpha) = \alpha$.

Korollar. Graden $[K:F]$ av utvidelsen K over F er lik antallet av restklasser i $G(N,F)$ modulo undergruppen $H(K)$.

Dette följer direkte av $[K:F][N:K] = [N:F]$ og at $[N:K]$ og $[N:F]$ henholdsvis er lik ordenen av $H(K)$ og ordenen av $H(F) = G(N,F)$.

To undergrupper H_1 og H_2 av en gruppe G sies å være konjugerte

hvis det eksisterer et element $g \in G$ slik at $gH_1g^{-1} = H_2$.

Sats 68. Kroppene K_1 og K_2 er konjugerte over F hvis og bare hvis $H(K_1)$ og $H(K_2)$ er konjugerte undergrupper av $G(N,F)$.

Bevis: For å bevise satsen er det nok å vise at

$$(1) \qquad H(F(\varphi\alpha)) = \varphi H(F(\alpha))\varphi^{-1}$$

For denne likningen medfører at de to konjugerte kroppene $F(\alpha)$ og $F(\varphi\alpha)$ ved korrespondansen $K \to H(K)$ går over i to konjugerte undergrupper av $G(N,F)$. Hvis omvendt $F(\alpha)$ og $F(\beta)$ går over i to konjugerte undergrupper $H(F(\alpha))$ og $\varphi H(F(\alpha))\varphi^{-1} = H(F(\beta))$ vil p.g.a. (1) $H(F(\varphi\alpha)) = H(F(\beta))$. Hovedsatsen i Galois-teorien gir da $F(\varphi\alpha) = F(\beta)$ som viser at kroppene $F(\alpha)$ og $F(\beta)$ er konjugerte. Vi viser så riktigheten av identiteten (1). $H(F(\varphi\alpha))$ består av de automorfismer ψ som lar $\varphi(\alpha)$ invariant; d.v.s. $\psi\varphi(\alpha) = \varphi(\alpha)$ eller $\varphi^{-1}\psi\varphi(\alpha) = \alpha$. Dette er ensbetydende med at $\varphi^{-1}\psi\varphi \in H(F(\alpha))$ eller $\psi \in \varphi \cdot H(F(\,))\varphi^{-1}$ som beviser (1).

Sats 69. En mellomkropp K; $F \subseteq K \subseteq N$ er en normal utvidelse av F hvis og bare hvis $H(K)$ er en invariant (normal) undergruppe av den Galoiske gruppen $G(N,F)$.

Bevis: Etter Sats 66 er K en normal utvidelse av F hvis og bare hvis K er identisk med alle sine konjugerte kropper. Ifölge Sats 68 er dette ekvivalent med at $H(K)$ er identisk med alle sine konjugerte undergrupper og dette er igjen ekvivalent med at $H(K)$ er en invariant undergruppe av $G(N,F)$. Hvis K er en normal utvidelse av F har det mening å snakke om Galois-gruppen $G(K,F)$ siden K da er rotkroppen til et separabelt polynom over F. Og det er rimelig å undersöke hvilken relasjon som eksisterer mellom de tre Galois-gruppene $G(N,F)$, $G(N,K)$ og $G(K,F)$. Allerede korollaret til Sats 67 peker henimot följende

Sats 70. Hvis K er en mellomkropp som er en normal utvidelse av F har vi isomorfien $G(K,F) \cong G(N,F)/G(N,K)$.

Bevis: Enhver automorfisme $\varphi \in G(N,F)$ induserer en automorfisme i K - kort og godt ved å ta restriksjonen av φ til K. Dette gir en avbildning av $G(N,F)$ på $G(K,F)$ og denne avbildningen (å ta restriksjonen) er tydeligvis en homomorfi. (At vi får en avbildning på $G(K,F)$ följer av Lemma 2, s.49.) Kjernen i denne homomorfien er etter hovedsatsen i Galois-teorien lik $G(N,K)$ og Sats 8 gir isomorfien i satsen.

§ 5. Anvendelser av Galois-teori på algebraiske likninger.

30. Problemstilling. En algebraisk likning av n'te grad er en likning av formen

(1) $$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0 \quad \text{med} \quad a_n \neq 0,$$

hvor koeffisientene a_i hörer til en viss grunnkropp F. Hovedproblemet i teorien for algebraiske likninger er å avgjöre i hvilke tilfeller likningen (1) lar seg löse ved gjentatt anvendelse av vanlige rasjonale operasjoner samt "rotutdragninger" på koeffisientene a_i. Med andre ord å avgjöre om röttene på en eller annen måte lar seg skrive som et uttrykk bygd opp av elementer i grunnkroppen og tegnene for sum, differens, produkt, kvotient samt tegnene for rotutdragninger av forskjellig grad.

Hensikten med formuleringen ovenfor er bare som en innledning å gjengi den populære og upresise oppfatningen av problemet om algebraiske likningers lösbarhet. For en tilfredsstillende behandling av problemet kreves det en helt presis formulering - spesielt fordi det egentlig dreier seg om to forskjellige problemer, nemlig lösningen av spesielle n'te gradslikninger og lösningen av den generelle n'te-gradslikning. Med en spesiell n'te-gradslikning over F forstår vi en likning av formen (1) hvor alle koeffisientene a_i er å betrakte som faste, ganske bestemte elementer fra F (som f.eks. likningen $x^5 - x - 1 = 0$ når $F = Q$). Da sier vi at en spesiell n'te gradslikning av formen (1) er lösbar ved rotutdragning om det er mulig å finne en endelig kjede av overkropper til F:

(2) $$F \subseteq K_1 \subseteq K_2 = \ldots \subseteq K_m$$

hvor $K_{i+1} = K_i(\alpha_i)$ og α_i er rot i en likning av formen $x^{n_i} - \beta = 0$; $\beta \in K_i$ og slik at rotkroppen N til polynomet f(x) er inneholdt i K_m. En utvidelse av F som er av formen K_m i (2) kaller vi en radikalutvidelse av F. Dette er det presise uttrykk for at röttene i $f(x) = 0$ kan skrives på den måten vi anga til å begynne med. Det er tydelig at $f(x) = 0$ er lösbar ved rotutdragning hvis og bare hvis alle irreduktible faktorer i f(x) leder til likninger som er lösbare. Vi kan derfor i det følgende forutsette at f(x) er irreduktibel over F. Vi skal da se at det blir nok å avgjöre om en rot i $f(x) = 0$ ligger innenfor en passende valgt K_m fordi vi kan ordne oss slik at K_m blir en normal utvidelse av grunnkropppen F.

Når det gjelder begrepet generell n'te gradslikning ser en ofte svært uheldige formuleringer som er egnet til å forvirre. Ofte oppfatter en (1) som en generell N'te gradslikning dersom a_i'ene ikke lenger er faste spesifiserte elementer fra F, men "variable" i F. Det greieste her er vel å anlegge et rent formalistisk synspunkt, nemlig at en generell N'te gradslikning skal være et rent formelt uttrykk av formen

(3) $$a_n x^n + \ldots + a_0 = 0$$

hvor $a_0, a_1 \ldots a_n$ er bokstaver ("ubestemte") som ikke har noe med den gitte grunnkroppen F å gjöre. Dette betyr bare at $F(a_0, \ldots a_n)$ er den transendente utvidelsen av F som består av alle rasjonale uttrykk i bokstavene $a_0, \ldots a_n$ med koeffisienter fra F. Over denne kroppen $F(a_0, \ldots a_n)$ blir nå (3) en spesiell n'te gradslikning og vi definerer problemet om lösbarheten av den generelle n'te gradslikning over F som problemet om lösbarheten av den spesielle n'te gradslikning (3) oppfattet som likning over $F(a_0, \ldots a_n)$. Vi ser altså det noe paradoksale at begrepet "spesiell n'te gradslikning" blir å oppfatte som mer generelt enn begrepet "generell N'te gradslikning"! Det problemet som historisk har spilt störst rolle er problemet om lösbarheten av den generelle n'te gradslikning og da spesielt problemet om den generelle 5'te gradslikning som ble behandlet av Abel. Vi skal i det följende ved hjelp av den Galoiske teori bevise hovedsatsen om lösbarheten av algebraiske likninger. Denne satsen gir et effektivt middel til å avgjöre lösbarhetsproblemet både i det "generelle" og i det "spesielle" tilfellet og vi skal spesielt bruke den til å bevise umuligheten av å löse den generelle n'te gradslikning når $n \geq 5$.

31. Rene likninger og deres Galois-grupper. Alle likninger i det följende er å oppfatte som spesielle likninger. De enkleste spesielle n'te gradslikninger over grunnkroppen F er de som er av typen $x^n - a = 0$ (eller egentlig $ex^n - a = 0$, e er enhetselementet i F) hvor $a \in F$. Likninger av denne typen kaller vi rene likninger og vi skal starte med en sats som uttaler seg om den Galoiske gruppen til en slik likning.

Sats 71. La F være en kropp som er identisk med rotkroppen til polynomet $x^n - e$ over F (med andre ord F inneholder alle de n'te enhetsröttene) og hvor n ikke er delelig med karakteristikken til F. Da vil den Galoiske gruppen til likningen $x^n - a = 0$ med $a \in F$ være syklisk. Hvis omvendt N er en endelig normal og separabel utvidelse

av en slik F med syklisk Galois-gruppe G(N,F) vil vi ha N = F(α) hvor α er rot i en ren likning x^n-a over F.

Bevis: La α betegne en rot i likningen

$$x^n-a = 0 \; ; \quad a \in F \tag{4}$$

La ε betegne en primitiv n'te enhetsrot. (Eksistensen av en slik berodde som vi så på betingelsen om at n ikke er delelig med karakteristikken til F). På grunn av forutsetningen om at de n'te enhetsröttene hörer med til F vil elementene $\alpha, \alpha\varepsilon, \ldots \alpha\varepsilon^{n-1}$ alle ligge i F(α). De tilfredsstiller alle likningen (4) og vil på grunn av primitiviteten av ε utgjöre n forskjellige rötter av denne likningen og dermed utgjöre alle röttene siden likningens grad er n. Altså er F(α) rotkroppen til det separable polynomet x^n-a over F. En automorfisme $\varphi \in G(F(\alpha),F)$ er fullstendig bestemt om vi kjenner $\varphi(\alpha)$ og siden $\varphi(\alpha)$ også må tilfredsstille (4) (Sats 43) har vi iallfall ikke andre automorfismer i $G(F(\alpha),F)$ enn de som er av formen $\varphi(\alpha) = \varepsilon^k\alpha$ hvor $0 \leq k \leq n-1$. Om dette virkelig gir automorfismer i $G(F(\alpha),F)$ for alle verdier av k uttaler vi oss ikke om. Men avbildningen $\varphi \to \varepsilon^k\varphi$ som vi får på denne måten gir i alle tilfeller en en-entydig avbildning av gruppen $G(F(\alpha),F)$ på en viss delmengde av gruppen E_n av n'te enhetsröttene. Og denne avbildningen er en ismorfi. For om $\varphi_1 \to \varepsilon^{k_1}$ og $\varphi_2 \to \varepsilon^{k_2}$ vil $\varphi_1\varphi_2 \to \varepsilon^{k_1+k_2}$ G(F( )) blir på denne måten identifisert med en undergruppe av den sykliske gruppen E_n (Sats 59) og må derfor selv være syklisk (Sats 9).

Omvendt la N være en endelig, normal og separabel utvidelse av F av grad n. Etter korollaret til Sats 62 er da N en enkel algebraisk utvidelse og vi kan sette N = F(α). Forutsetningen er nå at G(N,F) er syklisk og vi betegner en generator i denne gruppen med φ_0. Om ξ er en n'te enhetsrot (og derfor ligger i F etter forutsetningen) danner vi den såkalte Lagrange's resolvente

$$(\xi,\alpha) = \alpha_0+\xi\alpha_1+\ldots+\xi^{n-1}\alpha_{n-1}$$

hvor vi har satt $\alpha_i = \varphi_0^{\,i}\alpha$, $\varphi_0^{\,0} = \varphi_0^{\,n}$ er identitetsautomorfismen og derfor $\alpha = \alpha_0$. Under automorfismen φ_0 blir α_i'ene syklisk ombyttet: $\varphi_0(\alpha_i) = \varphi_0(\varphi_0^{\,i}\alpha) = \varphi_0^{\,i+1}\alpha = \alpha_{i+1}$ og vi får

$$\varphi_0(\xi,\alpha) = \alpha_1+\xi\alpha_2+\ldots+\xi^{n-2}\alpha_{n-1}+\xi^{n-1}\alpha_0$$

$$= \xi^{-1}(\alpha_0+\xi\alpha_1+\ldots+\xi^{n-1}\alpha_{n-1})$$

$$= \xi^{-1}(\xi,\alpha)$$

Vi ser av dette at $\varphi_0(\xi,\alpha)^n = [\varphi_0(\xi,\alpha)]^n = (\xi^{-1})^n(\xi,\alpha)^n = (\xi,\alpha)^n$. Elementet $(\xi,\alpha)^n$ er altså invariant under φ_0 og dermed under enhver potens av φ_0; d.v.s. under hele den Galoiske gruppen $G(N,F)$. Etter Sats 48 må da $(\xi,\alpha)^n \in F$. Av $\varphi_0^i(\xi,\alpha) = \xi^{-i}(\xi,\alpha)$ følger at det bare er den identiske automorfismen i $G(N,F)$ som lar resolventen (ξ,α) invariant og hovedsatsen i Galois-teorien gir $F((\xi,\alpha)) = N$. Satsen er dermed bevist siden (ξ,α) er rot i polynomet $x^n-(\xi,\alpha)^n$ som hörer til $F[x]$.

32. Hovedsatsen om lösbarhet av algebraiske likninger. Vi trenger först följende

Lemma. Det homomorfe billedet av en opplösbar gruppe er opplösbar.

Bevis: La G være en opplösbar gruppe (se avsnitt 6). Det vil altså si at G har en normalrekke av formen

$$(1) \qquad G \supset G_1 \supset G_2 \quad \ldots \quad \supset G_m = \{e\}$$

hvor alle faktorgruppene G_i/G_{i+1} er abelske. La G' betegner det gitte homomorfe billedet av G, d.v.s. vi har en avbildning φ av G på G' som er en homomorfi. Utfra rekken (1) kan vi nå ved å ta de tilsvarende homomorfe billeder $\varphi G_i = G_i'$ få dannet rekken

$$(2) \qquad G' \supseteq G_1' \supseteq \ldots \supseteq G_m' = \{e'\}$$

Det gjelder å vise at dette er en normalrekke for G' og at alle gruppene G_i'/G'_{i+1} er abelske. For det förste vet vi at alle G_i' er grupper siden det homomorfe billedet av en gruppe er en gruppe. At G'_{i+1} er en invariant undergruppe av G_i' ser vi slik: La $a \in G_i$ og $x \in G_{i+1}$; siden G_{i+1} er invariant i G_i vil $axa^{-1} \in G_{i+1}$. Ved å anvende den gitte homomorfien φ får vi av dette $a'x'a'^{-1} = (axa^{-1})' \in G'_{i+1}$ og da a' og x' kan gjennomlöpe henholdsvis hele G_i' og hele G'_{i+1} följer det at G'_{i+1} er invariant i G_i'. At G_i/G_{i+1} er abelsk betyr at $aG_{i+1}bG_{i+1} = bG_{i+1}\cdot aG_{i+1}$ og ved å anvende φ på begge sider får vi på samme måte som ovenfor at også G_i'/G'_{i+1} er abelsk.

Vi er nå i stand til å bevise den fundamentale

Sats 72. (Hovedsatsen om algebraiske likningers lösbarhet.) La F være en kropp med karakteristikk null og la $f(x) = 0$ være en irreduktibel algebraisk likning over F. Hvis $f(x) = 0$ har en rot som kan uttrykkes ved rottegn o: ligger i en viss radikalutvidelse K_m av F vil hele rotkroppen N til f (og derfor spesielt alle röttene i $f(x) = 0$) også ligge i en passende (större) radikalutvidelse og den Galoiske gruppen G(N,F) til likningen $f(x) = 0$ er en opplösbar gruppe. Omvendt hvis den Galoiske gruppen G(N,F) til $f(x) = 0$ er opplösbar kan $f(x) = 0$ löses ved rotutdragninger på den presiserte måte.

Bemerkning. Ved å kreve at grunnkroppen skal ha karakteristikk null har vi gjort en antagelse som er noe strengere enn nödvendig. Men ved det sikrer vi oss en gang for alle at alle de utvidelser vi skal foreta blir separable og at utvidelsenes grad aldri blir delelig med karakteristikken til F, noe som er nödvendig for anvendelsen av satsene 60 og 71. For en noe mer generell formulering kan vi henvise til [5] s.181.

Bevis: Forutsetningen i förste del av satsen er altså at vi har en radikalutvidelse K_m fremkommet på den angitte måten ved en kjede utvidelser

(3) $$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m$$

slik at $\beta \in K_m$ og $f(\beta) = 0$. Vi antar at vi har $K_{i+1} = K_i(\alpha_{i+1})$ hvor α_{i+1} er rot i likningen $x^{n_i} - a_i = 0$ med $a_i \in K_i$ $(0 \leq i \leq m-1)$. Da blir $K_m = F(\alpha_1, \ldots \alpha_m)$. Vi skal nå vise at vi utfra (3) kan konstruere en ny og "lengre" rekke av utvidelser som har sterkere egenskaper og som tillater oss å trekke konklusjonen i satsen. Vi begynner med å adjungere til F alle $n_0, n_1, \ldots n_{m-1}$'te enhetsrötter. Det klarer seg da å adjungere til de tilsvarende primitive enhetsrötter $\varepsilon_0, \varepsilon_1, \ldots \varepsilon_{m-1}$; for om ε_i er en primitiv n_i'te enhetsrot over F vil $F(\varepsilon_i)$ inneholde alle de n_i'te enhetsröttene over F. Vi får med dette följende kjede av utvidelser

(4) $$F \subseteq F(\varepsilon_0) \subseteq F(\varepsilon_0, \varepsilon_1) \subseteq \cdots \subseteq F(\varepsilon_0, \varepsilon_1, \ldots \varepsilon_{m-1})$$

Her er $F(\varepsilon_0, \ldots \varepsilon_{m-1})$ en normal utvidelse av F siden den er rotkroppen til polynomet $(x^{n_0} - e)(x^{n_1} - e) \ldots (x^{n_{m-1}} - e)$. Vi bygger nå videre på $F(\varepsilon_0, \ldots \varepsilon_{m-1})$ og adjungerer så elementet α_1 og får utvidelsen

(5) $$F(\varepsilon_0, \ldots \varepsilon_{m-1}) = F(\varepsilon_0, \ldots \varepsilon_{m-1}, \alpha_1)$$

som er en normal utvidelse av F siden $F(\varepsilon_o,\dots\varepsilon_{m-1},\alpha_1)$ er rotkroppen til polynomet $(x^{n_o}-a_o)\prod_{i=0}^{m-1}(x^{n_i}-e)$. (Alle rötter i $x^{n_o}-a=0$ er jo av formen $\varepsilon_o^k\alpha_1$.) Vi er nå interessert i stadig å foreta sykliske utvidelser d: utvidelser med sykliske Galois-grupper og det slik at vi ender med en utvidelse som inneholder K_m og er normal over F. Ovenfor har vi allerede oppnådd en normal utvidelse som inneholder K_1. Vi skal bare beskrive den neste serie av adjunksjoner fordi dette skrittet som vil lede til en normal utvidelse som inneholder K_2, har en generell karakter og vil lede til en normal utvidelse som inneholder K_m ved å anvendes m-1 ganger. Vi begynner da selvfölgelig med å adjungere roten α_2 i likningen $x^{n_1}-a_1=0$ til $F(\varepsilon_o,\dots\varepsilon_{m-1},\alpha_1)$; men vi kan ikke være sikker på at den oppnådde utvidelse er normal over F. For å være sikker på å få en normal utvidelse må vi suksessivt adjungere til alle röttene i alle likninger av formen $x^{n_1}-\varphi a_1=0$ hvor $\varphi\in G(F(\varepsilon_o,\dots\varepsilon_{m-1},\alpha_1),F)$. Dette leder oss nemlig til en utvidelse over F som er rotkroppen til polynomet

$$(6)\qquad (x^{n_o}-a_o)\prod_{i=0}^{m-1}(x^{n_i}-e)\prod_{\varphi}(x^{n_1}-\varphi a_1)$$

hvor φ er utstrakt over alle automorfismer i $G(F(\varepsilon_o,\dots\varepsilon_{m-1},\alpha_1),F)=G_1$. At koeffisientene i det polynomet som defineres av det siste produktet i (6) virkelig hörer til F kommer av at de blir symmetriske funksjoner av φa_1'ene ($\varphi\in G_1$) og derfor invariante under enhver $\psi\in G_1$ slik at Sats 48 kan anvendes.

Om vi nå fortsetter på nöyaktig samme måte for $\alpha_3,\alpha_4,\dots\alpha_m$ får vi frem en samlet kjede av utvidelser hvis endeledd kommer til å bli en normal, separabel utvidelse L av F som inneholder alle α_i'ene og dermed K_m og spesielt elementet β som var rot i $f(x)=0$ og inneholdt i K_m. Siden L er normal og $f(x)$ var forutsatt irreduktibel inneholder L hele rotkroppen til $f(x)$. Vi påstår nå at Galois-gruppen $G(L,F)$ er en opplösbar gruppe. Slik som L er dannet er den en radikalutvidelse av grunnkroppen fremkommet ved suksessiv adjunksjon av rötter i rene likninger. La $K_j'\subset K'_{j+1}$ være to kropper som följer umiddelbart på hverandre i denne lange serien av utvidelser. Da er for det förste K'_{j+1} en normal utvidelse av K_j' (men ikke nödvendigvis normal over grunnkroppen !) For de förste m-2 utvidelsene i (4) er dette klart. Senere er utvidelsen fra K_j' til K'_{j+1} alltid av formen $K'_{j+1}=K_j'(\alpha)$ hvor α er rot i en ren likning over K_j' og siden nå

de nödvendige enhetsrötter befinner seg i K_j' vil K'_{j+1} også inneholde alle de konjugerte til α over K_j' (siden disse er av formen $\varepsilon^k\alpha$) og K'_{j+1} blir normal over K_j'. Av dette følger av Sats 69 at $H(K'_{j+1}) = G(L,K'_{j+1})$ er invariant i $H(K_j') = G(L,K_j')$ og Sats 70 gir isomorfien

$$G(K'_{j+1},K_j') \cong H(K_j')/H(K'_{j+1})$$

For å se at $G(L,F)$ er opplösbar gjenstår det derfor bare å vise at gruppen $G(K'_{j+1},K_j')$ alltid er abelsk. For de förste m-2 utvidelser som svarer til (4) följer dette av Sats 60 og for alle de övrige utvidelser följer det av Sats 71 som nå kan brukes fordi de nödvendige enhetsrötter er blitt adjungert. Endelig er rotkroppen N til polynomet $f(x)$ inneholdt i L og vi får en kanonisk homomorfi av $G(L,F)$ på $G(N,F)$ ved å avbilde $\varphi \in G(L,F)$ på restriksjonen av φ til N. Som det homomorfe billedet av den opplösbare gruppen $G(L,F)$ er derfor etter det beviste lemma også $G(N,F)$ opplösbar og förste del av satsen er bevist.

Anta så omvendt at rotkroppen N til likningen $f(x) = 0$ har en opplösbar Galois-gruppe $G(N,F)$. Det betyr at vi har en normalrekke

$$G(N,F) = G_o \supset G_1 \supset \cdots \supset G_m = \{e\}$$

hvor faktorene G_i/G_{i+1} er sykliske. Ved hovedsatsen i Galois-teorien förer dette til en tilsvarende kjede av kropper

$$F \subset K_1 \subset \cdots \subset K_m = N \tag{7}$$

Her kan vi ikke uten videre anvende siste del av Sats 71 idet vi ikke har forutsatt at F skal inneholde de nödvendige enhetsrötter. van der Waerden [5] s.183 sier her bare at en först adjungerer til F alle $n_1, n_2, \cdots n_m$'te enhetsrötter hvor n_i er graden av K_i over K_{i-1} i (7). Men herved får vi jo en grunnkropp $F(\varepsilon_1, \varepsilon_2 \cdots \varepsilon_m)$ (ε_i er n_i'te primitiv enhetsrot) som ikke vanligvis er inneholdt i K_1. Vi har imidlertid följende forslag til ordning av dette: Istedet for (7) betrakter vi följende kjede

$$F \subseteq F(\varepsilon_1) \subseteq F(\varepsilon_1,\varepsilon_2) \subseteq \cdots \subseteq F(\varepsilon_1 \cdots \varepsilon_m) \subseteq K_1(\varepsilon_1, \cdots \varepsilon_m) \subseteq \cdots$$
$$\subseteq K_m(\varepsilon_1 \cdots \varepsilon_m). \tag{8}$$

Vi konstaterer ved samme resonnement som tidligere at hver kropp i kjeden er en normal utvidelse av den foregående og vi påstår at alle disse utvidelsene har sykliske Galois-grupper. Det som må vises er at

$G(K_{i+1}(\varepsilon_1 \cdots \varepsilon_m)\ ;\ K_i(\varepsilon_1 \cdots \varepsilon_m))$ er syklisk. Vi skal gjöre dette ved å vise at $G(K_{i+1}(\varepsilon_1),\ K_i(\varepsilon_1))$ er isomorf med en undergruppe av $G(K_{i+1}, K_i) \cong G_i/G_{i+1}$. Ved å gjenta dette m ganger får vi at $G(K_{i+1}(\varepsilon_1, \cdots \varepsilon_m), K_i(\varepsilon_1 \cdots \varepsilon_m))$ blir isomorf med en undergruppe av den sykliske gruppen G_i/G_{i+1} og derfor selv er syklisk. For å se at $G(K_{i+1}(\varepsilon_1),\ K_i(\varepsilon_1))$ er isomorf med en undergruppe av $G(K_{i+1}, K_i)$ betrakter vi en $\varphi \in G(K_{i+1}(\varepsilon_1),\ K_i(\varepsilon_1))$ og tar dens restriksjon til K_{i+1}. En verifiserer lett at denne restriksjonen definerer en automorfisme $\varphi' \in G(K_{i+1},\ K_i)$ og at avbildningen $\varphi \to \varphi'$ er en isomorfi. - Vi kan nå anvende siste halvdel av Sats 71 på (8) og får at $K_m(\varepsilon_1, \cdots \varepsilon_m)$ er en radikalutvidelse av F som inneholder N. Dette betyr at $f(x) = 0$ kan löses ved rotutdragninger og Sats 72 er dermed fullstendig bevist.

Bemerkning. Som nevnt gjör ikke van der Waerden den betraktningen vi har på slutten av beviset. I Artin [1] s.73 henvises imidlertid på dette punkt til en sats (som han kaller "theorem on natural irrationalities") som er en generalisering av det som ble bevist ovenfor.

33. Ulösbarheten av den generelle n'te gradslikning for $n \geq 5$. Vi beviser först följende

Sats 73. La $F(x_1, \cdots x_n)$ være kroppen av alle rasjonale uttrykk i n bokstaver $x_1 \cdots x_n$. La $\sigma_1 \cdots \sigma_n$ være de elementære symmetriske uttrykk i bokstavene $x_1 \cdots x_n$. Da vil $F(x_1, \cdots x_n)$ være rotkroppen til det separable polynomet $x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n = 0$ over $F(\sigma_1 \cdots \sigma_n)$ og den tilsvarende Galois-gruppen $G(F(x_1 \cdots x_n), F(\sigma_1, \cdots \sigma_n))$ er den symmetriske gruppen over n bokstaver.

Bemerkning. Med den symmetriske gruppen over n bokstaver $\{a_1, \cdots a_n\}$ forstår vi gruppen av alle permutasjoner i mengden $\{a_1, a_2 \cdots a_n\}$.

Bevis: Likningen $x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n = 0$ har de n forskjellige röttene $x_1, \cdots x_n$ og er derfor separabel over $F(\sigma_1, \cdots \sigma_n)$. Videre vil enhver permutasjon i mengden $x_1, \cdots x_n$ bevirke en automorfisme i $F(x_1, \cdots x_n)$ som lar ethvert element i $F(\sigma_1, \cdots \sigma_n)$ invariant siden σ_i er et symmetrisk i x_i'ene - og dette beviser satsen.

Vi minner om (se avsnittet "Problemstilling") at den Galoiske gruppen til den generelle n'te gradslikningen $a_n x^n + \cdots + a_o = 0$ blir den Galoiske gruppen av $a_n x^n + \cdots + a_o = 0$ over den transendente utvidelsen $F(a_o, \cdots a_n)$. Vi har da

Sats 74. Den Galoiske gruppen til den generelle n'te gradslikning er den symmetriske gruppen over n bokstaver.

Bemerkning. I det vi her skal gjöre en sammenlikning med den likningen som opptrer i Sats 73 vil vi forutsette at den generelle n'te gradslikningen har formen $x^n-u_1x^{n-1}+\ldots+(-1)^nu_n = 0$. Denne likningen er - når u'ene oppfattes som uavhengige transendente störrelser ("bokstaver") over grunnkroppen F - like "generell" som den vanlige formen for den generelle n'te gradslikning. Vi har bare foretatt en divisjon og en omdöping av koeffisientene.

Bevis: La rotkroppen til $x^n-u_1x^{n-1}+\ldots+(-1)^nu_n = 0$ være N og la likningens rötter være $v_1,v_2\ldots v_n$. Det gjelder nå först og fremst å konstatere at avbildningen $u_i \longrightarrow \sigma_i$ induserer en kanonisk isomorfi mellom ringene $F[u_1,\ldots u_n]$ og $F[\sigma_1,\ldots\sigma_n]$ hvor den siste ringen refererer seg til situasjonen i Sats 73. Siden $F[u_1\ldots u_n]$ er den vanlige transendente utvidelsen som gir polynomringen i n ubestemte med koeffisienter fra F blir det nok å vise at $F[\sigma_1\ldots\sigma_n]$ også er en slik polynomring i n bokstaver. Det betyr at det ikke må eksistere noen relasjon $f(\sigma_1,\ldots\sigma_n) = 0$ med $f \in F[x]$ uten at f er nullpolynomet. Anta $f(\sigma_1\ldots\sigma_n) = 0$ med $f \in F[x]$. Innförer vi uttrykkene for σ_i'ene får vi $f(\sum x_i, \sum x_ix_j,\ldots) = 0$. Er dette en identitet i x_i'ene gjelder den også ved innsetting av v_i for x_i; d.v.s. $f(\sum v_i, \sum v_iv_j,\ldots) = 0$ og dermed $f(u_1,\ldots u_n) = 0$ som betyr at f må være nullpolynomet. I polynomringen $F[u_1,\ldots u_n]$ eksisterer det nemlig ikke noen relasjon mellom u_i'ene - det er selve definisjonen på at u_i'ene er uavhengige "bokstaver", "transendente störrelser" eller "ubestemte" (eller hva man vil kalle det) over F. Isomorfien $F[u_1,\ldots u_n] \cong F[\sigma_1,\ldots\sigma_n]$ kan nå utvides til en isomorfi mellom de tilsvarende kvotentkroppene: $F(u_1,\ldots u_n) = F(\sigma_1,\ldots\sigma_n)$ og det er tydelig at rotkroppen til likningen $x^n-u_1x^{n-1}+\ldots+(-1)^nu_n = 0$ over $F(u_1,\ldots u_n)$ derfor er isomorf med rotkroppen til $x^n-\sigma_1x^{n-1}+\ldots+(-1)^n\sigma_n = 0$ over $F(\sigma_1\ldots\sigma_n)$. Da denne siste utvidelsen etter Sats 73 har en Galois-gruppe som er isomorf med den symmetriske gruppen over n elementer er satsen bevist.

Sats 75. Den symmetriske gruppen over n elementer danner en ikke-opplösbar gruppe når $n \geq 5$.

Bevis: La G være den symmetriske gruppen over mengden $\{a_1,\ldots a_n\}$ med $n \geq 5$ og la

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m$$

Være en kjede av undergrupper hvor G_i er invariant i G_{i-1} og G_{i-1}/G_i er en syklisk gruppe. Vi skal bevise at G_m for alle m må inneholde alle permutasjoner som lar invariant alle elementene i $\{a_1 \cdots a_n\}$ unntatt tre av dem og bytter disse siste tre elementene syklisk. Dette betyr at G_m aldri kan bli lik $\{I\}$ for noe m hvor I er identitetspermutasjonen - og G kan dermed ikke være opplösbar. Den permutasjonen φ_0 som lar alle a_i invariant unntatt de tre elementene a_r, a_s, a_t som den bytter syklisk d: $\varphi_0(a_r) = a_s$, $\varphi_0(a_s) = a_t$, $\varphi(a_t) = a_r$ vil vi betegne med (r,s,t) og kalle en 3-syklus. Siden $G = G_0$ inneholder alle slike 3-sykluser er det nok å vise at om G_i inneholder alle 3-sykluser så gjör også G_{i+1} det. Hvis permutasjonene φ og ψ begge hörer til G_i vil $\gamma = \varphi^{-1}\psi^{-1}\varphi\psi \in G_{i+1}$. For G_i/G_{i+1} er syklisk og dermed kommutativ slik at om φ' og ψ' betegner billedene av φ og ψ ved den kanoniske homomorfien $G_i \to G_i/G_{i+1}$ vil

$$\gamma' = \varphi'^{-1}\psi'^{-1}\varphi'\psi' = \varphi'^{-1}\psi'^{-1}\psi'\varphi' = I'$$

og det betyr at $\gamma \in G_{i+1}$. Anta nå at G_i inneholder alle 3-sykluser. Spesielt har vi at $\varphi = (rst)$ og $\psi = (tuv) \in G_i$ hvor r,s,t,u,v er 5 av indeksene (fra 1 til n). (Det er her vi bruker betingelsen at $n \geq 5$). Uttrykket $\gamma = \varphi^{-1}\psi^{-1}\varphi\psi$ som vi har bevist hörer til G_{i+1} blir i dette tilfellet

$$\gamma = (rts)(tvu)(rst)(tuv) = (rtu) \in G_{i+1}$$

Siden (rtu) er en vilkårlig 3-syklus er alt bevist. Av satsene 74 og 75 följer nå

Sats 76. Den generelle n'te gradslikning kan for $n \geq 5$ ikke löses ved rotutdragninger.

For $n \leq 4$ er den symmetriske gruppen opplösbar og muligheten for å löse den generelle 2^{nen}, 3^{dje} og 4^{de}-gradslikning ved rotutdragninger följer derfor av Sats 72. Også når det gjelder lösningen av disse likningene gir den Galoiske teorien öket forståelse idet de eksplisitte komposisjonsrekkene en kan stille opp for de symmetriske gruppene $S_n (n \leq 4)$ gir den egentlige grunn for de adjunksjoner en må foreta for å löse disse likningene. Dette står beskrevet på side 186 og utover i [5].

34. Lösbarhet og ulösbarhet av spesielle algebraiske likninger med rasjonale koeffisienter.

Sats 76 beviser også ifölge våre definisjoner (se avsnittet "Problemstilling") ulösbarheten av spesielle n'te gradslikninger - nemlig over en grunnkropp av typen $F(a_0,...a_n)$ (rasjonal funksjonskropp i n ubestemte). Når det gjelder ulösbarhet av spesielle likninger er vi imidlertid först og fremst interessert i ulösbarheten av spesielle likninger med tall-koeffisienter (f.eks. $F = Q$ eller $F = R$ som grunnkropp). Slik ulösbarhet er også mulig å vise ved den teorien vi har utviklet. En kan f.eks. bevise at den ganske bestemte likningen $x^5-x-1=0$ (over Q) er ulösbar fordi den har en Galois-gruppe som er isomorf med den symmetriske gruppen S_5. (Se [5] s.199.) Vi bemerket at Sats 72 förte til at den generelle 2^{nen}, 3^{dje} og 4^{de} gradslikning er lösbare ved rotutdragninger. Men det er ikke fullkomment innlysende (selv om det vanligvis fremstilles slik) at denne lösbarheten for generelle likninger (: likninger over $F(a_0,...a_n)$) også medförer lösbarheten av de spesielle likninger vi får over F når vi for $a_0,...a_n$ innsetter bestemte elementer i F. At denne innsettingen er "tillatt" kan imidlertid begrunnes nærmere ved at denne innsettingsprosessen definerer en viss homomorfi. Grunnlaget for denne betraktningen kan en finne i [3].

Literatur.

[1] E. Artin: Galois theory, Notre Dame Indiana 1948 (annen utgave).

[2] G. Birkhoff & S. MacLane: A survey of modern algebra.

[3] N. Bourbaki: Algebre. Chapitres IV og V.

[4] N. Jacobson: Lectures in abstract algebra.

[5] B.L. van der Waerden: Moderne Algebra I.